RIPSTECH

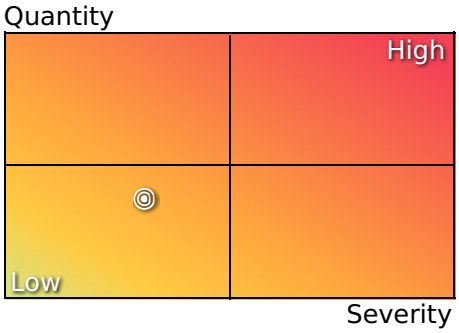
SECURITY ANALYSIS REPORT

Wordpress-popup(Hustle)-v7.0.4
Date: 2020-01-21

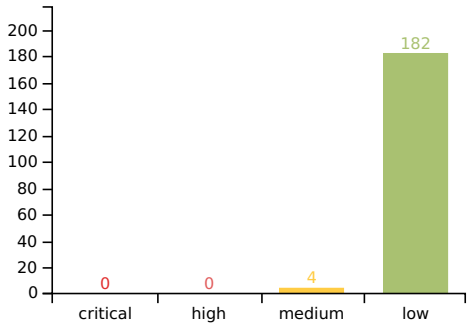
1. Executive Summary

Project Name:	Wordpress-popup(Hustle)-v7.0.4	Analyzed Files:	503
Analysis Start Date:	2020-01-21, 09:14	Analyzed LOC:	92,093
Analysis End Date:	2020-01-21, 09:20	Analyzed Issue Types:	209
Analysis Time:	5m 15s	Detected Issues:	186
Engine Version(s):	php-preparser 3.3.1 php-engine 3.3.4 php-patchgen 3.3.0	Max Issues per Type:	100 / 500

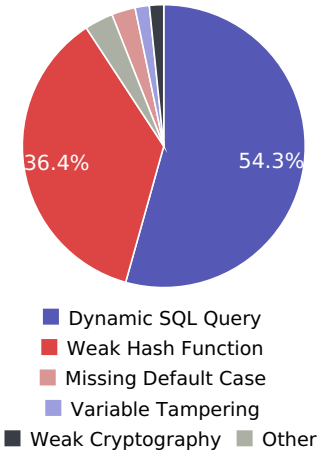
Risk Matrix



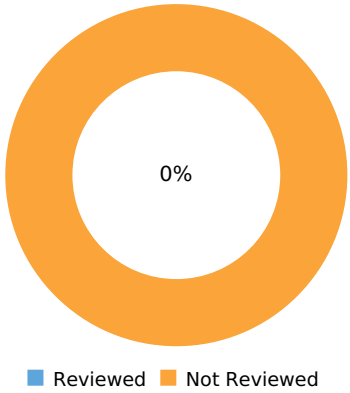
Vulnerabilities by Risk



Top Vulnerability Types



Review Status



2. Issue Breakdown

The detected security issues in this project are categorized as follows.

Severity	Vulnerability Type	CWE [?]	OWASP Top 10 [?]	SANS 25 [?]	PCI DSS [?]	ASVS [?]	Issues
Medium	Variable Tampering	627	A2	Not Ranked	6.5.8		3
Medium	Variable Extraction Error	621		Not Ranked			1
Low	HTTP Parameter Pollution	233	A2	Not Ranked	6.5.4	5.1.1	1
Low	Information Leakage	209	A6	Not Ranked	6.5.5	7.4.1	1
Low	Weak Cryptography	310	A3	Not Ranked	6.5.3		3
Low	Dangerous Feature	242		Not Ranked			3
Low	Dynamic SQL Query	89		Not Ranked			100
Low	Missing Error Handling	390		Not Ranked			1
Low	Missing Default Case	478		Not Ranked			5
Low	Weak Hash Function	328		Not Ranked			67
Low	Expression Always False	572		Not Ranked			1

3. Issue Details

In the following, all security issues detected in the analyzed project are presented in detail. The issues are grouped by vulnerability type and by the detected markup context. A *markup context* represents the position of user-supplied data (*source*) used in a sensitive operation (*sink*). Depending on the markup context, an attacker can alter the operation and different security mechanisms must be applied in order to patch the security issue thoroughly.

3.1. Variable Tampering

ASVS:	
OWASP Top 10:	2017: A2
CWE:	627
PCI DSS:	6.5.8
Severity:	Medium

A variable tampering vulnerability occurs when user input is used to dynamically access variables. An attacker might be able to interfere with the applications logic by manipulating sensitive variables.

A variable tampering vulnerability occurs when user input is used to dynamically access variables. An attacker might be able to interfere with the applications logic by manipulating sensitive variables. If dynamic variable names affected by user input are required, the user input should be checked against a whitelist.

3.1.1. Mass Assignment

ASVS:	4.0.1: 5.1.2
OWASP Top 10:	2017: A2
CWE:	915
SANS 25:	Rank 10
PCI DSS:	6.5.8
Severity:	Medium

The detected vulnerability allows a mass assignment of object properties. This occurs when object properties are dynamically filled with user input. Depending on the properties and their usage this can lead to a critical security issue when, for example, prices in a shopping cart can be overwritten or privileges of a user can be changed.

The detected vulnerability allows a mass assignment of object properties. If dynamically assigning values stemming from user input to properties is necessary, the possible properties should be restricted by a whitelist.

Issue #2274 - wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php: 178

Path:	wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php
Line:	178
Sink:	
Source:	_POST
Taint:	HTTP

Code Summary

A POST parameter is received in line 204 of the file wordpress-popup/lib/wpmu-lib/inc/class-

thelib-array.php in the method TheLib_Array::equip_post().

The user-supplied data is then used to dynamically assign object properties in line 178 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php in the method TheLib_Array::equip(). Please refer to the context and description for further information.

wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php

```
8    class TheLib_Array extends TheLib {
⋮
163  public function equip( &$arr, $fields ) {
⋮
171  $fields = func_get_args();
⋮
175  foreach ( $fields as $field ) {
176  if ( $is_obj ) {
177  if ( ! property_exists( $arr, $field ) ) {
178  $arr->$field = false;
179  $missing += 1;
180  }
181  } else {
182  if ( ! isset( $arr[ $field ] ) ) {
183  $arr[ $field ] = false;
184  $missing += 1;
185  }
186  }
187  }
⋮
190  }
⋮
202  public function equip_post( $fields ) {
⋮
204  return $this->equip( $_POST, $fields );
205  }
⋮
271  }
```

Property Context

The following snippet(s) do not represent actual code but the tainted context.

```
$_POST[$field[.*]]
```

Patch

Whitelist Possible Values

wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php

```
178  // TODO: Fill in the whitelist with names you want to allow
179  if (!in_array($field, ["var1", "var2"], true)) {
180  throw new Exception('Variable name not allowed}');
181  }
182  $arr->{$field} = false;
```

Issue #2275 - wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php: 178

Path: wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php
Line: 178
Sink:

Source: _REQUEST

Taint: HTTP

Code Summary

A GET parameter is received in line 219 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php in the method TheLib_Array::equip_request().

The user-supplied data is then used to dynamically assign object properties in line 178 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php in the method TheLib_Array::equip(). Please refer to the context and description for further information.

wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php

```
8    class TheLib_Array extends TheLib {
⋮
163  public function equip( &$arr, $fields ) {
⋮
171  $fields = func_get_args();
⋮
175  foreach ( $fields as $field ) {
176  if ( $is_obj ) {
177  if ( ! property_exists( $arr, $field ) ) {
178  $arr->$field = false;
179  $missing += 1;
180  }
181  } else {
182  if ( ! isset( $arr[ $field ] ) ) {
183  $arr[ $field ] = false;
184  $missing += 1;
185  }
186  }
187  }
⋮
190  }
⋮
217  public function equip_request( $fields ) {
⋮
219  return $this->equip( $_REQUEST, $fields );
220  }
⋮
271  }
```

Property Context

The following snippet(s) do not represent actual code but the tainted context.

```
$_REQUEST[$field[.*]]
```

Patch

Whitelist Possible Values

wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php

```
178  // TODO: Fill in the whitelist with names you want to allow
179  if (!in_array($field, ["var1", "var2"], true)) {
180  throw new Exception('Variable name not allowed}');
181  }
182  $arr->{$field} = false;
```

Issue #2276 - wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php: 178

Path: wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php

Line: 178
Sink:
Source: _GET
Taint: HTTP

Code Summary

A GET parameter is received in line 234 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php in the method TheLib_Array::equip_get().

The user-supplied data is then used to dynamically assign object properties in line 178 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php in the method TheLib_Array::equip(). Please refer to the context and description for further information.

wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php

```
8    class TheLib_Array extends TheLib {
⋮
163  public function equip( &$arr, $fields ) {
⋮
171  $fields = func_get_args();
⋮
175  foreach ( $fields as $field ) {
176  if ( $is_obj ) {
177  if ( ! property_exists( $arr, $field ) ) {
178  $arr->$field = false;
179  $missing += 1;
180  }
181  } else {
182  if ( ! isset( $arr[ $field ] ) ) {
183  $arr[ $field ] = false;
184  $missing += 1;
185  }
186  }
187  }
⋮
190  }
⋮
232  public function equip_get( $fields ) {
⋮
234  return $this->equip( $_GET, $fields );
235  }
⋮
271  }
```

Property Context

The following snippet(s) do not represent actual code but the tainted context.

```
$_GET[$field[.*]]
```

Patch

Whitelist Possible Values

wordpress-popup/lib/wpmu-lib/inc/class-thelib-array.php

```
178  // TODO: Fill in the whitelist with names you want to allow
179  if (!in_array($field, ["var1", "var2"], true)) {
180  throw new Exception('Variable name not allowed}');
```

```
181 }
182 $arr->{$field} = false;
```

3.2. Variable Extraction Error

CWE: 621
Severity: Medium

The application overwrites variables based on untrusted user input. This can be abused by attackers to initialize or overwrite critical internal variables and to change the control flow of the application or to exploit security-sensitive operations.

Using the extract method on user input should be avoided whenever possible. If it is necessary in a given case, the keys of the input array that gets extracted should be validated to belong to a whitelist beforehand.

Issue #2095 - wordpress-popup/popover.php: 374

Path: wordpress-popup/popover.php
Line: 374
Sink: extract
Source: _POST
Taint: HTTP

Code Summary

The POST parameter 'data[]' is received in line 221 of the file wordpress-popup/inc/provider/hustle-provider-admin-ajax.php in the method Hustle_Provider_Admin_Ajax::settings().

wordpress-popup/inc/provider/hustle-provider-admin-ajax.php

```
6   class Hustle_Provider_Admin_Ajax {
⋮
215 public function settings() {
⋮
219 $data = filter_input( INPUT_POST, 'data', FILTER_DEFAULT );
⋮
221 $data = filter_input( INPUT_POST, 'data', FILTER_DEFAULT, FILTER_REQUIRE_ARRAY );
⋮
223 $sanitized_post_data = Opt_In_Utils::validate_and_sanitize_fields( $data, array( 'slug', 'step', 'current_step' ) );
⋮
257 unset( $sanitized_post_data['slug'] );
⋮
262 $wizard = $provider->get_settings_wizard( $sanitized_post_data, $module_id, $current_step, $step, true );
⋮
269 }
⋮
467 }
```

A code quality issue was detected in line 374 of the file wordpress-popup/popover.php in the method Opt_In::static_render(). Please refer to the context and description for further information.

wordpress-popup/popover.php

```
109 class Opt_In extends Opt_In_Static{
⋮
368 public static function static_render( $file, $params = array(), $return = false ) {
369 $params = array_merge( $params );
```

```
⋮
374  extract( $params, EXTR_OVERWRITE ); // phpcs:ignore
⋮
406  }
⋮
719  }
```

Code Context

The following snippet(s) do not represent actual code but the tainted context.

```
$_POST['data'][$post_datum[.*]]
```

3.3. HTTP Parameter Pollution

ASVS:	4.0.1: 5.1.1
OWASP Top 10:	2017: A2
CWE:	233
PCI DSS:	6.5.4
Severity:	Low

An HTTP Parameter Pollution (HPP) vulnerability occurs when unsanitized user input is used to construct a URL and its query parameters. An attacker can modify the URL and insert additional query string parameters that could overwrite existing ones and thereby change the intended behavior of the request.

To prevent HTTP Parameter Pollution attacks, it is recommended to urlencode() all values that are embedded into query string parameters such that no additional parameters can be added.

Issue #2097 - wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php: 51

Path:	wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php
Line:	51
Sink:	curl_setopt
Source:	_SERVER
Taint:	HTTP

Code Summary

The URI that contains partially unencoded special characters in certain browsers is received in line 50 of the file wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php in the method Hustle_Activecampaign_Api::_request().

The user-supplied data is concatenated into parameter markup in line 50 of the file wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php in the method Hustle_Activecampaign_Api::_request().

The user-supplied data is then used unsanitized in the sensitive operation curl_setopt() in line 51 of the file wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php in the method Hustle_Activecampaign_Api::_request(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php

```
7    class Hustle_Activecampaign_Api {
⋮
```

```
25  private function _request( $verb = "GET", $action, $args = array() ){
26  $url = $this->_url;

⋮
28  $apidata = array(
29  'api_action' => $action,
30  'api_key' => $this->_key,
31  'api_output' => 'serialize',
32  );
⋮
34  $url = add_query_arg( $apidata, $url );

⋮
50  $url = add_query_arg($args, $url);
51  curl_setopt($request, CURLOPT_URL, $url);
⋮
67  }
⋮
256 }
```

Parameter Context

The following snippet(s) do not represent actual code but the tainted context.

```
$_SERVER['REQUEST_URI'] ? = ?api_action= &api_key= &api_output=serialize&
```

3.4. Information Leakage

ASVS:	4.0.1: 7.4.1
OWASP Top 10:	2017: A6
CWE:	209
PCI DSS:	6.5.5
Severity:	Low

An information leakage vulnerability occurs when confidential information about the web server's setup or the application’s inner workings is leaked to the application's user. Although the issue might not be exploitable, it can help an attacker to prepare other attacks.

The affected code might be leftover debug code. In such a case, it should be removed before running the code in production.

3.4.1. Information Leakage (system)

ASVS:	4.0.1: 7.4.1
OWASP Top 10:	2017: A6
CWE:	214
PCI DSS:	6.5.5
Severity:	Low

The affected code leaks information about the system that allows an attacker to learn about used software versions or installation paths.

The affected code might be leftover debug code. In such a case, it should be removed before running the code in production.

Issue #2278 - wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php: 425

Path: wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php

Line: 425
Sink: echo
Taint: HTTP

Code Summary

User-supplied data is concatenated into info markup in line 425 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php in the method TheLib_Debug::trace().

The operation echo() leaks sensitive system information. It is located in line 425 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php in the method TheLib_Debug::trace(). Please refer to the context and description for further information.

wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php

```
8    class TheLib_Debug extends TheLib {
⋮
325  public function trace( $output = true ) {
⋮
330  $trace_str = '';
⋮
333  $block_id = 'wdev-debug-' . md5( rand() );
334  $trace_str .= sprintf(
335  '<span class="wdev-trace-toggle" onclick="toggleBlock(\'%1$s-trace\')">
336  <b>Back-Trace</b>
337  </span>
338  <div class="%1$s-trace" style="display:none">
339  <table class="wdev-trace" width="100%%" cellspacing="0" cellpadding="3" border="1">
340  ',
341  esc_attr( $block_id )
342  );
⋮
345  $trace = debug_backtrace();
⋮
349  for ( $i = 0; $i < $trace_num; $i += 1 ) {
350  $item = $trace[$i];
351  $line_item = $item;
352  $j = $i;
⋮
354  while ( empty( $line_item['line'] ) && $j < $trace_num ) {
355  $line_item = $trace[$j];
356  $j += 1;
357  }
⋮
359  self::$core->array->equip( $line_item, 'file', 'line', 'class', 'type', 'function' );
360  self::$core->array->equip( $item, 'args', 'file', 'line', 'class', 'type', 'function' );
361  if ( 0 === strpos( $item['class'], 'TheLib_' ) ) { continue; }
⋮
363  $line += 1;
364  $args = '';
365  $arg_num = '';
366  $dummy = array();
⋮
368  if ( $i > 0 && is_array( $item['args'] ) && count( $item['args'] ) ) {
369  foreach ( $item['args'] as $arg ) {
370  if ( is_scalar( $arg ) ) {
371  if ( is_bool( $arg ) ) {
372  $dummy[] = ( $arg ? 'true' : 'false' );
373  } elseif ( is_string( $arg ) ) {
374  $dummy[] = '"' . $arg . '"';
375  } else {
```

```
376 $dummy[] = $arg;
377 }
378 } elseif ( is_array( $arg ) ) {
379 $dummy[] = '<i>[Array]</i>';
380 } elseif ( is_object( $arg ) ) {
381 $dummy[] = '<i>[' . get_class( $arg ) . ']</i>';
382 } elseif ( is_null( $arg ) ) {
383 $dummy[] = '<i>NULL</i>';
384 } else {
385 $dummy[] = '<i>[???]</i>';
386 }
387 }
⋮
389 $args = implode( '</font></span><span class="trc-param"><font>', $dummy );
390 $args = '<span class="trc-param"><font>' . $args . '</font></span>';
391 }
⋮
393 if ( $plain_text ) {
394 $file = $line_item['file'];
395 if ( strlen( $file ) > 80 ) {
396 $file = '...' . substr( $line_item['file'], -77 );
397 } else {
398 $file = str_pad( $file, 80, ' ', STR_PAD_RIGHT );
399 }
⋮
401 $trace_str .= sprintf(
402 "\r\n %s. \t %s \t by %s",
403 str_pad( $line, 2, ' ', STR_PAD_LEFT ),
404 $file . ': ' . str_pad( $line_item['line'], 5, ' ', STR_PAD_LEFT ),
405 $item['class'] . $item['type'] . $item['function'] . '(' . strip_tags( $args ) . ')'
406 );
407 } else {
408 $trace_str .= sprintf(
409 "<tr onclick='_m(this)'><td class='trc-num'>%s</td><td class='trc-loc'>%s</td><td class='trc-
    arg'>%s</td></tr>\r\n",
410 $line,
411 $line_item['file'] . ': ' . $line_item['line'],
412 $item['class'] . $item['type'] . $item['function'] . '(' . $args . ')'
413 );
414 }

415 }
⋮
418 $trace_str .= "\r\n-----\r\n";
⋮
425 echo '' . $trace_str;
⋮
429 }
⋮
964 }
```

Info Context

The following snippet(s) do not represent actual code but the tainted context.

```
info
```

3.5. Weak Cryptography

OWASP Top 10:	2017: A3
CWE:	310
PCI DSS:	6.5.3

Severity: Low

3.5.1. Weak Cryptography (unsafe hash comparison)

OWASP Top 10: 2017: A3
PCI DSS: 6.5.3
Severity: Low

Hashes are compared with a timing attack unsafe string comparison operation. It may be possible to use the time of the comparison as a side-channel to extract sensible information about the hashes.

Use the timing attack safe string comparison operation hash_equals() to compare hashes, or the timing attack safe password_verify() to compare a password to a hash.

Issue #2285 - wordpress-popup/vendor/Ctct/WebHooks/CTCTWebhookUtil.php: 99

Path: wordpress-popup/vendor/Ctct/WebHooks/CTCTWebhookUtil.php
Line: 99
Sink:
Taint: HTTP

Code Summary

The operation () is used incorrectly in line 99 of the file wordpress-popup/vendor/Ctct/WebHooks/CTCTWebhookUtil.php in the method ctctwebhooksCTCTWebhookUtil::isValidWebhook(). Please refer to the context and description for further information.

wordpress-popup/vendor/Ctct/WebHooks/CTCTWebhookUtil.php

```
13  class CTCTWebhookUtil
14  {
⋮
91  public function isValidWebhook($xCtctHmacSHA256, $bodyMessage)
92  {
⋮
99  return ($encodedString == $xCtctHmacSHA256)?true:false;
100 }
101 }
```

Info Context

The following snippet(s) do not represent actual code but the tainted context.

```
Timing attacks susceptible hash comparison
```

Patch

Use Safe Compare

wordpress-popup/vendor/Ctct/WebHooks/CTCTWebhookUtil.php

```
99  return (hash_equals($encodedString, $xCtctHmacSHA256))?true:false;
```

3.5.2. Weak Cryptography (cert verification)

ASVS: 4.0.1: 9.1.1

OWASP Top 10: 2017: A3
CWE: 295
PCI DSS: 6.5.4
Severity: Low

The code fails to adequately encrypt network traffic using strong cryptography. This enables man-in-the-middle attackers to intercept and modify the traffic to the requested resource in order to gain control over the application.

A secure protocol such as https should be used in the URL and the verification of the SSL certificate should never be disabled.

Issue #2096 - wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php: 40

Path: wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php
Line: 40
Sink: curl_setopt
Taint: HTTP

Code Summary

The operation curl_setopt() is used incorrectly in line 40 of the file wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php in the method Hustle_Activecampaign_Api::_request(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php

```
7    class Hustle_Activecampaign_Api {
⋮
25   private function _request( $verb = "GET", $action, $args = array() ){
⋮
40   curl_setopt($request, CURLOPT_SSL_VERIFYPEER, false);
⋮
67   }
⋮
256  }
```

Info Context

The following snippet(s) do not represent actual code but the tainted context.

```
Third parameter is FALSE and host is not verified.
```

Patch

Verify Certificate with Curl

wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php

```
40  curl_setopt($request, CURLOPT_SSL_VERIFYPEER, true);
```

Issue #2179 - wordpress-popup/inc/hustle-sshare-model.php: 257

Path: wordpress-popup/inc/hustle-sshare-model.php
Line: 257
Sink: curl_setopt

Taint: HTTP

Code Summary

The operation curl_setopt() is used incorrectly in line 257 of the file wordpress-popup/inc/hustle-sshare-model.php in the method Hustle_SShare_Model::get_networks_data_from_api(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-sshare-model.php

```
3    class Hustle_SShare_Model extends Hustle_Module_Model {
⋮
238  private function get_networks_data_from_api( $current_link, $social_networks = array(), $options = array() ) {
⋮
257  curl_setopt( $curl_handle[ $network ], CURLOPT_SSL_VERIFYPEER, false );
⋮
275  }
⋮
464  }
```

Info Context

The following snippet(s) do not represent actual code but the tainted context.

```
Third parameter is FALSE and host is not verified.
```

Patch

Verify Certificate with Curl

wordpress-popup/inc/hustle-sshare-model.php

```
257  curl_setopt($curl_handle[$network], CURLOPT_SSL_VERIFYPEER, true);
```

3.6. Dangerous Feature

CWE: 242
Severity: Low

The use of an inherently dangerous function or language feature has been detected. The feature is known to introduce security risks and should be avoided whenever possible.

The use of inherently dangerous functions and language features should be avoided whenever possible.

Issue #2098 - wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php: 65

Path: wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php
Line: 65
Sink: unserialize
Taint: HTTP

Code Summary

A code quality issue was detected in line 65 of the file wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php in the method Hustle_Activecampaign_Api::_request(). Please refer to the context and description for further

information.

wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-api.php

```
7    class Hustle_Activecampaign_Api {
⋮
25   private function _request( $verb = "GET", $action, $args = array() ){
⋮
65   return unserialize($response);
⋮
67   }
⋮
256  }
```

Code Context

The following snippet(s) do not represent actual code but the tainted context.

```
unserialize(...)
```

Issue #2197 - wordpress-popup/inc/display-conditions/opt-in-condition-cpt.php: 39

Path: wordpress-popup/inc/display-conditions/opt-in-condition-cpt.php
Line: 39
Sink: unserialize
Taint: HTTP

Code Summary

A code quality issue was detected in line 39 of the file wordpress-popup/inc/display-conditions/opt-in-condition-cpt.php in the method Opt_In_Condition_Cpt::is_allowed(). Please refer to the context and description for further information.

wordpress-popup/inc/display-conditions/opt-in-condition-cpt.php

```
3    class Opt_In_Condition_Cpt extends Opt_In_Condition_Abstract {
4    public function is_allowed( Hustle_Model $optin ){
⋮
39   $subscriptions = unserialize($user_meta['ms_subscriptions'][0]);
⋮
92   }
⋮
120  }
```

Code Context

The following snippet(s) do not represent actual code but the tainted context.

```
unserialize(...)
```

Issue #2198 - wordpress-popup/inc/display-conditions/opt-in-condition-cpt.php: 73

Path: wordpress-popup/inc/display-conditions/opt-in-condition-cpt.php
Line: 73
Sink: unserialize
Taint: HTTP

Code Summary

A code quality issue was detected in line 73 of the file wordpress-popup/inc/display-conditions/opt-in-condition-cpt.php in the method Opt_In_Condition_Cpt::is_allowed(). Please refer to the context and description for further information.

wordpress-popup/inc/display-conditions/opt-in-condition-cpt.php

```
3    class Opt_In_Condition_Cpt extends Opt_In_Condition_Abstract {
4    public function is_allowed( Hustle_Model $optin ){
⋮
73   $subscriptions = unserialize($user_meta['ms_subscriptions'][0]);
⋮
92   }
⋮
120  }
```

Code Context

The following snippet(s) do not represent actual code but the tainted context.

```
unserialize(...)
```

3.7. Dynamic SQL Query

CWE: 89
Severity: Low

A SQL query is constructed dynamically by concatenation. This can lead to SQL injection attacks.

It is recommended to use prepared statements for all SQL queries. The prepared statement itself should only use placeholders for data and never concatenate data directly into the query.

Issue #2093 - wordpress-popup/inc/hustle-module-collection.php: 388

Path: wordpress-popup/inc/hustle-module-collection.php
Line: 388
Sink: execute
Source: _POST
Taint: HTTP

Code Summary

A code quality issue was detected in line 388 of the file wordpress-popup/inc/hustle-module-collection.php in the method Hustle_Module_Collection::get_active_providers_module(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-module-collection.php

```
8    class Hustle_Module_Collection extends Hustle_Collection {
⋮
383  public static function get_active_providers_module( $slug ) {
⋮
388  $query = $wpdb->prepare(
389  "SELECT `module_id`
390  FROM {$modules_meta_table}
391  WHERE `meta_value`
392  LIKE %s
393  AND `meta_key` = 'integrations_settings'",
394  "%". $slug . "%"
```

```
395 );
⋮
398 }
⋮
400 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `module_id` FROM self WHERE `meta_value` LIKE % $_POST['data'][$post_datum[.*]] % AND `meta_key` =
'integrations_settings'
```

Issue #2094 - wordpress-popup/inc/hustle-model.php: 523

Path: wordpress-popup/inc/hustle-model.php
Line: 523
Sink: execute
Source: _POST
Taint: HTTP

Code Summary

A code quality issue was detected in line 523 of the file wordpress-popup/inc/hustle-model.php in the method Hustle_Model::get_meta(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-model.php

```
13    abstract class Hustle_Model extends Hustle_Data {
⋮
512   public function get_meta( $meta_key, $default = null, $get_cached = true ){
⋮
523   $value = $this->_wpdb->get_var( $this->_wpdb->prepare( "SELECT `meta_value` FROM " . Hustle_Db::module
      s_meta_table() . " WHERE `meta_key`=%s AND `module_id`=%d", $meta_key, (int) $this->id ) );
⋮
530   }
⋮
1222  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `meta_value` FROM self WHERE `meta_key`= $_POST['data'][$post_datum[.*]] self AND `module_id`=1
```

Issue #2099 - wordpress-popup/inc/hustle-module-collection.php: 181

Path: wordpress-popup/inc/hustle-module-collection.php
Line: 181
Sink: get_var
Taint: HTTP

Code Summary

A code quality issue was detected in line 181 of the file wordpress-popup/inc/hustle-module-collection.php in the method Hustle_Module_Collection::get_all(). Please refer to the context and

description for further information.

wordpress-popup/inc/hustle-module-collection.php

```
8    class Hustle_Module_Collection extends Hustle_Collection {
⋮
26   public function get_all( $active = true, $args = array(), $limit = -1 ) {
⋮
53   $module_type_condition = '';
⋮
55   $v = implode( ',', array_map( array( $this, '_wrap_string' ), $types ) );
56   $module_type_condition .= 'AND m.`module_type` IN ( ' . $v .' ) ';
⋮
58   $module_type_condition .= ( isset($args['except_types']) ) ? $this->prepare_except_module_types_condition( $a
     rgs['except_types'] ) : "";
⋮
62   $join = '';
⋮
73   $join .= 'LEFT JOIN '.Hustle_Db::modules_meta_table().' AS cf ON cf.`module_id` = m.`module_id` ';
74   $join .= self::$_db->prepare(
75   'AND cf.`meta_key` = %s ',
76   $args['meta']['key']
77   );
78   $module_type_condition .= 'AND cf.`meta_value` IS NULL ';
⋮
81   $join .= 'JOIN '.Hustle_Db::modules_meta_table().' AS cf ON cf.`module_id` = m.`module_id` ';
82   $join .= self::$_db->prepare(
83   'AND cf.`meta_key` = %s AND cf.`meta_value` = %s ',

84   $args['meta']['key'],
85   $args['meta']['value']
86   );
⋮
101  $join .= 'JOIN '.Hustle_Db::modules_meta_table().' AS cf1 ON cf1.`module_id` = m.`module_id` AND cf1.`meta_k
     ey` = "edit_roles" ';
102  $join .= self::$_db->prepare(
103  'AND ( cf1.`meta_value` LIKE %s ) ',
104  '%"' . $filter_role . '"%'
105  );
⋮
116  $module_type_condition .= self::$_db->prepare( 'AND m.`module_name` LIKE %s ', '%' . $args['filter']['q'] . '%' );
⋮
121  $query = 'SELECT ';
⋮
128  $query .= 'COUNT( distinct m.`module_id` )';
⋮
130  $query .= 'm.`module_id` ';
⋮
132  $query .= 'FROM ' . Hustle_Db::modules_table() . ' AS m '.$join.'WHERE 1 ';
⋮
143  $query .= self::$_db->prepare(
144  'AND m.`blog_id` IN ( 0, %d ) ',
145  $main_id
146  );
⋮
151  $query .= self::$_db->prepare( "AND m.`active`= %d ", (int) $active );
⋮
157  $query .= self::$_db->prepare( " AND m.`module_mode`= %s ", $module_mode );

⋮
159  $query .= $module_type_condition .' ';
⋮
164  $query .= 'ORDER BY ';
⋮
172  $query .= self::$_db->prepare( 'm.%s, ', $args['filter']['sort'] );
⋮
```

```
174  $query .= 'm.`module_name` ';
⋮
176  $query .= $limit.' '.$offset;
⋮
181  return self::$_db->get_var( $query );
⋮
198  }
⋮
400  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT COUNT( distinct m.`module_id` )FROM self AS m LEFT JOIN self AS cf ON cf.`module_id` = m.`module_id` JOIN self AS cf1 ON cf1.`module_id` = m.`module_id` AND cf1.`meta_key` = "edit_roles" WHERE 1 AND m.`module_type` IN ( 1 ) AND `module_type` != ' 'AND cf.`meta_value` IS NULL ORDER BY m.`module_name`
```

Issue #2109 - wordpress-popup/inc/hustle-tracking-model.php: 89

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 89
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 89 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::save_tracking(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
59   public function save_tracking( $module_id, $action, $module_type, $page_id, $module_sub_type = null, $date_cr
     eated = null, $ip = null ) {
⋮
64   $ip_query = ' AND `ip` IS NULL';
⋮
69   $ip_query = ' AND `ip` = %s';
⋮
78   $sql = "SELECT `tracking_id` FROM {$this->table_name} WHERE `module_id` = %d AND `page_id` = %d {$ip_
     query} AND `action` = %s AND `module_type` = %s AND `date_created` BETWEEN ";
⋮
80   $sql .= ' utc_date() AND utc_timestamp()';
⋮
82   $sql .= sprintf(
83   "'%s' AND '%s 23:59:59'",
84   substr( $date_created, 0, 10 ),
85   substr( $date_created, 0, 10 )
86   );
⋮
89   $prepared_sql = $wpdb->prepare( $sql, $module_id, $page_id, $ip, $action, $module_type ); // WPCS: unprepare
     d SQL ok. false positive
⋮
100  }
⋮
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `tracking_id` FROM WHERE `module_id` = %d AND `page_id` = %d AND `ip` = %s AND `action` = %s AND
`module_type` = %s AND `date_created` BETWEEN utc_date() AND utc_timestamp()
```

Issue #2111 - wordpress-popup/inc/hustle-tracking-model.php: 91

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 91
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 91 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::save_tracking(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
59   public function save_tracking( $module_id, $action, $module_type, $page_id, $module_sub_type = null, $date_cr
     eated = null, $ip = null ) {
⋮
64   $ip_query = ' AND `ip` IS NULL';
⋮
69   $ip_query = ' AND `ip` = %s';
⋮
78   $sql = "SELECT `tracking_id` FROM {$this->table_name} WHERE `module_id` = %d AND `page_id` = %d {$ip_
     query} AND `action` = %s AND `module_type` = %s AND `date_created` BETWEEN ";
⋮
80   $sql .= ' utc_date() AND utc_timestamp()';
⋮
82   $sql .= sprintf(
83   "'%s' AND '%s 23:59:59'",
84   substr( $date_created, 0, 10 ),
85   substr( $date_created, 0, 10 )
86   );
⋮
89   $prepared_sql = $wpdb->prepare( $sql, $module_id, $page_id, $ip, $action, $module_type ); // WPCS: unprepare
     d SQL ok. false positive
⋮
91   $prepared_sql = $wpdb->prepare( $sql, $module_id, $page_id, $action, $module_type ); // WPCS: unprepared S
     QL ok. false positive
⋮
100  }
⋮
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `tracking_id` FROM WHERE `module_id` = %d AND `page_id` = %d AND `ip` = %s AND `action` = %s AND
`module_type` = %s AND `date_created` BETWEEN utc_date() AND utc_timestamp()
```

Issue #2118 - wordpress-popup/inc/hustle-module-model.php: 881

Path: wordpress-popup/inc/hustle-module-model.php

Line: 881
Sink: execute
Source: _POST
Taint: HTTP

Code Summary

A code quality issue was detected in line 881 of the file wordpress-popup/inc/hustle-module-model.php in the method Hustle_Module_Model::get_module_type_by_module_id(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-module-model.php

```
9     class Hustle_Module_Model extends Hustle_Model {
⋮
879   public function get_module_type_by_module_id( $module_id ) {
⋮
881   $query = $this->_wpdb->prepare( "
882   SELECT module_type FROM `" . Hustle_Db::modules_table() . "`
883   WHERE `module_id`=%s",
884   $module_id
885   );
⋮
888   }
⋮
1178  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT module_type FROM `self` WHERE `module_id`= $_POST['id']['0']
```

Issue #2120 - wordpress-popup/inc/hustle-tracking-model.php: 275

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 275
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 275 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::_generate_date_query(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9     class Hustle_Tracking_Model {
⋮
271   private function _generate_date_query( $wpdb, $starting_date = null, $ending_date = null, $prefix = '', $clause
      = 'AND' ) {
⋮
273   $date_format = '%%Y-%%m-%%d';
⋮
      $date_query = $wpdb->prepare( "$clause DATE_FORMAT($prefix`date_created`, '$date_format') >= %s AND D
275   ATE_FORMAT($prefix`date_created`, '$date_format') <= %s", $starting_date, $ending_date ); // WPCS: unprepar
      ed SQL OK.
⋮
```

```
284 }
⋮
757 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DATE_FORMAT( `date_created`, '%%Y-%%m-%%d') >= %s AND DATE_FORMAT( `date_created`, '%%Y-%%m-%%d')
<= %s
```

Issue #2121 - wordpress-popup/inc/hustle-tracking-model.php: 278

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 278
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 278 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::_generate_date_query(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9     class Hustle_Tracking_Model {
⋮
271   private function _generate_date_query( $wpdb, $starting_date = null, $ending_date = null, $prefix = '', $clause
      = 'AND' ) {
⋮
273   $date_format = '%%Y-%%m-%%d';
⋮
      $date_query = $wpdb->prepare( "$clause DATE_FORMAT($prefix`date_created`, '$date_format') >= %s AND D
275   ATE_FORMAT($prefix`date_created`, '$date_format') <= %s", $starting_date, $ending_date ); // WPCS: unprepar
      ed SQL OK.
⋮
278   $date_query = $wpdb->prepare( "$clause DATE_FORMAT($prefix`date_created`, '$date_format') >= %s",
      $starting_date ); // WPCS: unprepared SQL OK.
⋮
284   }
⋮
757   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DATE_FORMAT( `date_created`, '%%Y-%%m-%%d') >= %s
```

Issue #2122 - wordpress-popup/inc/hustle-tracking-model.php: 280

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 280
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 280 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::_generate_date_query(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
271  private function _generate_date_query( $wpdb, $starting_date = null, $ending_date = null, $prefix = '', $clause = 'AND' ) {
⋮
273  $date_format = '%%Y-%%m-%%d';
⋮
275  $date_query = $wpdb->prepare( "$clause DATE_FORMAT($prefix`date_created`, '$date_format') >= %s AND DATE_FORMAT($prefix`date_created`, '$date_format') <= %s", $starting_date, $ending_date ); // WPCS: unprepared SQL OK.
⋮
278  $date_query = $wpdb->prepare( "$clause DATE_FORMAT($prefix`date_created`, '$date_format') >= %s", $starting_date ); // WPCS: unprepared SQL OK.
⋮
280  $date_query = $wpdb->prepare( "$clause DATE_FORMAT($prefix`date_created`, '$date_format') <= %s", $starting_date ); // WPCS: unprepared SQL OK.
⋮
284  }
⋮
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DATE_FORMAT( `date_created`, '%%Y-%%m-%%d') <= %s
```

Issue #2138 - wordpress-popup/inc/hustle-model.php: 139

Path:	wordpress-popup/inc/hustle-model.php
Line:	139
Sink:	execute
Source:	_GET
Taint:	HTTP

Code Summary

A code quality issue was detected in line 139 of the file wordpress-popup/inc/hustle-model.php in the method Hustle_Model::get_by_shortcode(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-model.php

```
13   abstract class Hustle_Model extends Hustle_Data {
⋮
126  public function get_by_shortcode( $shortcode_id, $enforce_type = true ){
⋮
139  $sql = $this->_wpdb->prepare(
140  "SELECT * FROM `" . Hustle_Db::modules_table() . "` as modules
141  JOIN `{$prefix}hustle_modules_meta` as meta
142  ON modules.`module_id`=meta.`module_id`
143  WHERE `meta_key`='shortcode_id'
144  AND (`module_type` = 'embedded' OR `module_type` = 'social_sharing')
145  AND `meta_value`=%s",
146  trim( $shortcode_id)
```

```
147   );
⋮
166   }
⋮
1222  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT * FROM `self` as modules JOIN `hustle_modules_meta` as meta ON modules.`module_id`=meta.`module_id`
WHERE `meta_key`='shortcode_id' AND (`module_type` = 'embedded' OR `module_type` = 'social_sharing') AND
`meta_value`= $_GET['shortcode_id']['0']
```

Issue #2140 - wordpress-popup/inc/hustle-modules-common-admin-ajax.php: 801

Path: wordpress-popup/inc/hustle-modules-common-admin-ajax.php
Line: 801
Sink: execute
Source: _POST
Taint: HTTP

Code Summary

A code quality issue was detected in line 801 of the file wordpress-popup/inc/hustle-modules-common-admin-ajax.php in the method Hustle_Modules_Common_Admin_Ajax::get_new_condition_ids(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-modules-common-admin-ajax.php

```
10   class Hustle_Modules_Common_Admin_Ajax {
⋮
782  public function get_new_condition_ids() {
783  $post_type = filter_input( INPUT_POST, 'postType', FILTER_SANITIZE_STRING );
⋮
800  global $wpdb;
801  $result = $wpdb->get_results( $wpdb->prepare( "SELECT ID as id, post_title as text FROM {$wpdb->posts} "
802  . "WHERE post_type = %s AND post_status = 'publish' AND post_title LIKE %s LIMIT " . intval( $limit ), $post_type
     , '%'. $search . '%' ) );
⋮
820  }
⋮
822  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT ID as id, post_title as text FROM WHERE post_type = $_POST['postType'] AND post_status = 'publish' AND
post_title LIKE LIMIT 123
```

Issue #2149 - wordpress-popup/inc/hustle-entry-model.php: 602

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 602
Sink: execute
Source: _POST

Taint: HTTP

Code Summary

A code quality issue was detected in line 602 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entries(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
568   public static function delete_by_entries( $module_id, $entries, $db = false ) {
⋮
593   $prepared_placeholders = implode( ', ', array_fill( 0, count( $entries ), '%s' ) );
⋮
602   $sql = $db->prepare( "DELETE FROM {$table_meta_name} WHERE `entry_id` IN ($prepared_placeholders)", $
      entries );
⋮
615   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DELETE FROM self WHERE `entry_id` IN ( $_POST['ids'] )
```

Issue #2157 - wordpress-popup/inc/hustle-deletion.php: 209

Path: wordpress-popup/inc/hustle-deletion.php
Line: 209
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 209 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_module_views(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8     class Hustle_Deletion {
⋮
207   public static function hustle_clear_module_views() {
208   global $wpdb;
209   $wpdb->query( "TRUNCATE {$wpdb->prefix}hustle_tracking" );
210   }
⋮
228   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
TRUNCATE hustle_tracking
```

Issue #2160 - wordpress-popup/inc/hustle-deletion.php: 163

Path: wordpress-popup/inc/hustle-deletion.php
Line: 163
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 163 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_module_submissions(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
146  public static function hustle_clear_module_submissions() {
⋮
163  $wpdb->query( "TRUNCATE {$wpdb->prefix}hustle_entries" );
⋮
200  }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
TRUNCATE hustle_entries
```

Issue #2161 - wordpress-popup/inc/hustle-deletion.php: 165

Path: wordpress-popup/inc/hustle-deletion.php
Line: 165
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 165 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_module_submissions(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
146  public static function hustle_clear_module_submissions() {
⋮
165  $wpdb->query( "TRUNCATE {$wpdb->prefix}hustle_entries_meta" );
⋮
200  }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
TRUNCATE hustle_entries_meta
```

Issue #2162 - wordpress-popup/inc/hustle-deletion.php: 182

Path: wordpress-popup/inc/hustle-deletion.php
Line: 182
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 182 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_module_submissions(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
146  public static function hustle_clear_module_submissions() {
⋮
182  $alter_entries = $wpdb->prepare(
183  "ALTER TABLE {$wpdb->prefix}hustle_entries
184  AUTO_INCREMENT = %d",
185  ++$max_entry_id
186  );
⋮
200  }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
ALTER TABLE hustle_entries AUTO_INCREMENT = %d
```

Issue #2163 - wordpress-popup/inc/hustle-deletion.php: 188

Path: wordpress-popup/inc/hustle-deletion.php
Line: 188
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 188 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_module_submissions(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
146  public static function hustle_clear_module_submissions() {
⋮
```

```
188 $alter_meta = $wpdb->prepare(
189 "ALTER TABLE {$wpdb->prefix}hustle_entries_meta
190 AUTO_INCREMENT = %d",
191 ++$max_entry_meta_id
192 );
⋮
200 }
⋮
228 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
ALTER TABLE hustle_entries_meta AUTO_INCREMENT = %d
```

Issue #2164 - wordpress-popup/inc/hustle-deletion.php: 193

Path: wordpress-popup/inc/hustle-deletion.php
Line: 193
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 193 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_module_submissions(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8   class Hustle_Deletion {
⋮
146 public static function hustle_clear_module_submissions() {
⋮
182 $alter_entries = $wpdb->prepare(
183 "ALTER TABLE {$wpdb->prefix}hustle_entries
184 AUTO_INCREMENT = %d",
185 ++$max_entry_id
186 );
⋮
193 $wpdb->query( $alter_entries );// phpcs:ignore
⋮
200 }
⋮
228 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
ALTER TABLE hustle_entries AUTO_INCREMENT = %d
```

Issue #2165 - wordpress-popup/inc/hustle-deletion.php: 194

Path: wordpress-popup/inc/hustle-deletion.php
Line: 194
Sink: execute

Taint: HTTP

Code Summary

A code quality issue was detected in line 194 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_module_submissions(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
146  public static function hustle_clear_module_submissions() {
⋮
188  $alter_meta = $wpdb->prepare(
189  "ALTER TABLE {$wpdb->prefix}hustle_entries_meta
190  AUTO_INCREMENT = %d",
191  ++$max_entry_meta_id
192  );
⋮
194  $wpdb->query( $alter_meta );// phpcs:ignore
⋮
200  }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
ALTER TABLE hustle_entries_meta AUTO_INCREMENT = %d
```

Issue #2168 - wordpress-popup/inc/hustle-deletion.php: 122

Path: wordpress-popup/inc/hustle-deletion.php
Line: 122
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 122 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_modules(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
89   public static function hustle_clear_modules() {
⋮
122  $alter_modules = $wpdb->prepare(
123  "ALTER TABLE {$wpdb->prefix}hustle_modules
124  AUTO_INCREMENT = %d",
125  ++$max_module_id
126  );
⋮
139  }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
ALTER TABLE hustle_modules AUTO_INCREMENT = %d
```

Issue #2169 - wordpress-popup/inc/hustle-deletion.php: 127

Path: wordpress-popup/inc/hustle-deletion.php
Line: 127
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 127 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_modules(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8     class Hustle_Deletion {
⋮
89    public static function hustle_clear_modules() {
⋮
127   $alter_meta = $wpdb->prepare(
128   "ALTER TABLE {$wpdb->prefix}hustle_modules_meta
129   AUTO_INCREMENT = %d",
130   ++$max_module_meta_id
131   );
⋮
139   }
⋮
228   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
ALTER TABLE hustle_modules_meta AUTO_INCREMENT = %d
```

Issue #2170 - wordpress-popup/inc/hustle-deletion.php: 133

Path: wordpress-popup/inc/hustle-deletion.php
Line: 133
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 133 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_modules(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8     class Hustle_Deletion {
⋮
```

```
89   public static function hustle_clear_modules() {
⋮
133  $wpdb->query( "TRUNCATE {$wpdb->prefix}hustle_modules" );
⋮
139  }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
TRUNCATE hustle_modules
```

Issue #2171 - wordpress-popup/inc/hustle-deletion.php: 134

Path: wordpress-popup/inc/hustle-deletion.php
Line: 134
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 134 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_modules(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
89   public static function hustle_clear_modules() {
⋮
122  $alter_modules = $wpdb->prepare(
123  "ALTER TABLE {$wpdb->prefix}hustle_modules
124  AUTO_INCREMENT = %d",

125  ++$max_module_id
126  );
⋮
134  $wpdb->query( $alter_modules );// phpcs:ignore
⋮
139  }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
ALTER TABLE hustle_modules AUTO_INCREMENT = %d
```

Issue #2172 - wordpress-popup/inc/hustle-deletion.php: 136

Path: wordpress-popup/inc/hustle-deletion.php
Line: 136
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 136 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_modules(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8     class Hustle_Deletion {
⋮
89    public static function hustle_clear_modules() {
⋮
136   $wpdb->query( "TRUNCATE {$wpdb->prefix}hustle_modules_meta" );
⋮
139   }
⋮
228   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
TRUNCATE hustle_modules_meta
```

Issue #2173 - wordpress-popup/inc/hustle-deletion.php: 137

Path: wordpress-popup/inc/hustle-deletion.php
Line: 137
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 137 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_modules(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8     class Hustle_Deletion {
⋮
89    public static function hustle_clear_modules() {
⋮
127   $alter_meta = $wpdb->prepare(
128   "ALTER TABLE {$wpdb->prefix}hustle_modules_meta
129   AUTO_INCREMENT = %d",
130   ++$max_module_meta_id
131   );
⋮
137   $wpdb->query( $alter_meta );// phpcs:ignore
⋮
139   }
⋮
228   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
ALTER TABLE hustle_modules_meta AUTO_INCREMENT = %d
```

Issue #2176 - wordpress-popup/inc/hustle-entry-model.php: 905

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 905
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 905 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::is_email_subscribed_to_module_id(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
891   public static function is_email_subscribed_to_module_id( $module_id, $email ) {
892   global $wpdb;
⋮
894   $entries_table = Hustle_Db::entries_table();
895   $entries_meta_table = Hustle_Db::entries_meta_table();
896   $query =
897   "SELECT COUNT(*)
898   FROM {$entries_table} e
899   INNER JOIN {$entries_meta_table} m
900   ON e.entry_id = m.entry_id
901   AND e.module_id = %d
902   AND m.meta_key = 'email'
903   AND m.meta_value = %s";
⋮
905   $query = $wpdb->prepare( $query, $module_id, $email ); // phpcs:ignore
      WordPress.DB.PreparedSQL.NotPrepared
⋮
911   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT COUNT(*) FROM self e INNER JOIN self m ON e.entry_id = m.entry_id AND e.module_id = %d AND m.meta_key
= 'email' AND m.meta_value = %s
```

Issue #2177 - wordpress-popup/inc/hustle-entry-model.php: 936

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 936
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 936 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::get_email_subscribed_to_module_id(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
922   public static function get_email_subscribed_to_module_id( $module_id, $email ) {
923   global $wpdb;
⋮
925   $entries_table = Hustle_Db::entries_table();
926   $entries_meta_table = Hustle_Db::entries_meta_table();
927   $query =
928   "SELECT e.entry_id
929   FROM {$entries_table} e
930   INNER JOIN {$entries_meta_table} m
931   ON e.entry_id = m.entry_id
932   AND e.module_id = %d
933   AND m.meta_key = 'email'
934   AND m.meta_value = %s";
⋮
936   $query = $wpdb->prepare( $query, $module_id, $email ); // phpcs:ignore
      WordPress.DB.PreparedSQL.NotPrepared
⋮
942   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT e.entry_id FROM self e INNER JOIN self m ON e.entry_id = m.entry_id AND e.module_id = %d AND m.meta_key
= 'email' AND m.meta_value = %s
```

Issue #2178 - wordpress-popup/inc/hustle-tracking-model.php: 89

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 89
Sink: execute
Source: _POST
Taint: HTTP

Code Summary

A code quality issue was detected in line 89 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::save_tracking(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9     class Hustle_Tracking_Model {
⋮
59    public function save_tracking( $module_id, $action, $module_type, $page_id, $module_sub_type = null, $date_cr
      eated = null, $ip = null ) {
⋮
76    $module_type = $module_type . '_' . $module_sub_type;
⋮
89    $prepared_sql = $wpdb->prepare( $sql, $module_id, $page_id, $ip, $action, $module_type ); // WPCS: unprepare
      d SQL ok. false positive
⋮
100   }
⋮
757   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `tracking_id` FROM .* WHERE `module_id` = 1 AND `page_id` = 1 AND `ip` = _ $_POST['data']['form']
['hustle_sub_type'] AND `action` = AND `module_type` = AND `date_created` BETWEEN utc_date() AND
utc_timestamp()
```

Issue #2180 - wordpress-popup/inc/hustle-module-model.php: 881

Path: wordpress-popup/inc/hustle-module-model.php
Line: 881
Sink: execute
Source: _POST
Taint: HTTP

Code Summary

A code quality issue was detected in line 881 of the file wordpress-popup/inc/hustle-module-model.php in the method Hustle_Module_Model::get_module_type_by_module_id(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-module-model.php

```
9     class Hustle_Module_Model extends Hustle_Model {
⋮
879   public function get_module_type_by_module_id( $module_id ) {
⋮
881   $query = $this->_wpdb->prepare( "
882   SELECT module_type FROM `" . Hustle_Db::modules_table() . "`
883   WHERE `module_id`=%s",
884   $module_id
885   );
⋮
888   }
⋮
1178  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT module_type FROM `self` WHERE `module_id`= $_POST['moduleId']['0']
```

Issue #2181 - wordpress-popup/inc/hustle-entry-model.php: 959

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 959
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 959 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::get_modules_id_by_email_in_local_list(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
952   public function get_modules_id_by_email_in_local_list( $email ) {
953   global $wpdb;
954   $query = sprintf(
955   'SELECT DISTINCT `module_id` FROM %s e INNER JOIN %s m ON e.entry_id = m.entry_id AND m.meta_key = \'e
      mail\' AND m.meta_value = %%s',
956   Hustle_Db::entries_table(),
957   Hustle_Db::entries_meta_table()
958   );
959   $query = $wpdb->prepare( $query, $email ); // phpcs:ignore WordPress.DB.PreparedSQL.NotPrepared
⋮
961   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT DISTINCT `module_id` FROM self e INNER JOIN self m ON e.entry_id = m.entry_id AND m.meta_key = 'email'
AND m.meta_value =
```

Issue #2187 - wordpress-popup/inc/hustle-deletion.php: 219

Path: wordpress-popup/inc/hustle-deletion.php
Line: 219
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 219 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_drop_custom_tables(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8     class Hustle_Deletion {
⋮
217   public static function hustle_drop_custom_tables() {
218   global $wpdb;
219   $wpdb->query( "DROP TABLE IF EXISTS {$wpdb->prefix}hustle_entries" );
⋮
226   }
⋮
228   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DROP TABLE IF EXISTS hustle_entries
```

Issue #2188 - wordpress-popup/inc/hustle-deletion.php: 220

Path: wordpress-popup/inc/hustle-deletion.php
Line: 220

Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 220 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_drop_custom_tables(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
217  public static function hustle_drop_custom_tables() {
218  global $wpdb;
⋮
220  $wpdb->query( "DROP TABLE IF EXISTS {$wpdb->prefix}hustle_entries_meta" );
⋮
226  }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DROP TABLE IF EXISTS hustle_entries_meta
```

Issue #2189 - wordpress-popup/inc/hustle-deletion.php: 221

Path: wordpress-popup/inc/hustle-deletion.php
Line: 221
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 221 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_drop_custom_tables(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
217  public static function hustle_drop_custom_tables() {
218  global $wpdb;
⋮
221  $wpdb->query( "DROP TABLE IF EXISTS {$wpdb->prefix}hustle_modules" );
⋮
226  }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DROP TABLE IF EXISTS hustle_modules
```

Issue #2190 - wordpress-popup/inc/hustle-deletion.php: 222

Path: wordpress-popup/inc/hustle-deletion.php
Line: 222
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 222 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_drop_custom_tables(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
217  public static function hustle_drop_custom_tables() {
218  global $wpdb;
⋮
222  $wpdb->query( "DROP TABLE IF EXISTS {$wpdb->prefix}hustle_modules_meta" );
⋮
226  }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DROP TABLE IF EXISTS hustle_modules_meta
```

Issue #2191 - wordpress-popup/inc/hustle-deletion.php: 223

Path: wordpress-popup/inc/hustle-deletion.php
Line: 223
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 223 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_drop_custom_tables(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
217  public static function hustle_drop_custom_tables() {
218  global $wpdb;
⋮
223  $wpdb->query( "DROP TABLE IF EXISTS {$wpdb->prefix}hustle_tracking" );
⋮
226  }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DROP TABLE IF EXISTS hustle_tracking
```

Issue #2192 - wordpress-popup/inc/hustle-deletion.php: 224

Path: wordpress-popup/inc/hustle-deletion.php
Line: 224
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 224 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_drop_custom_tables(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8     class Hustle_Deletion {
⋮
217   public static function hustle_drop_custom_tables() {
218   global $wpdb;
⋮
224   $wpdb->query( "DROP TABLE IF EXISTS {$wpdb->prefix}optin_meta" );
⋮
226   }
⋮
228   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DROP TABLE IF EXISTS optin_meta
```

Issue #2193 - wordpress-popup/inc/hustle-deletion.php: 225

Path: wordpress-popup/inc/hustle-deletion.php
Line: 225
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 225 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_drop_custom_tables(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8     class Hustle_Deletion {
⋮
217   public static function hustle_drop_custom_tables() {
218   global $wpdb;
⋮
```

```
225 $wpdb->query( "DROP TABLE IF EXISTS {$wpdb->prefix}optins" );
226 }
⋮
228 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DROP TABLE IF EXISTS optins
```

Issue #2202 - wordpress-popup/inc/hustle-entry-model.php: 1015

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 1015
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 1015 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::remove_local_subscription_by_email_and_module_id(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9    class Hustle_Entry_Model {
⋮
1008 public function remove_local_subscription_by_email_and_module_id( $email, $module_id ) {
1009 global $wpdb;
1010 $query = sprintf(
1011 'SELECT DISTINCT e.`entry_id` FROM %s e INNER JOIN %s m ON e.`entry_id` = m.`entry_id` AND m.`meta_key` = \'email\' AND m.`meta_value` = %%s WHERE e.`module_id` = %%d',
1012 Hustle_Db::entries_table(),
1013 Hustle_Db::entries_meta_table()
1014 );
1015 $query = $wpdb->prepare( $query, $email, $module_id ); // phpcs:ignore WordPress.DB.PreparedSQL.NotPrepared
⋮
1023 }
⋮
1130 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT DISTINCT e.`entry_id` FROM self e INNER JOIN self m ON e.`entry_id` = m.`entry_id` AND m.`meta_key` = 'email' AND m.`meta_value` =
```

Issue #2208 - wordpress-popup/inc/hustle-module-collection.php: 286

Path: wordpress-popup/inc/hustle-module-collection.php
Line: 286
Sink: execute
Taint: HTTP

Code Summary

A code quality issue was detected in line 286 of the file wordpress-popup/inc/hustle-module-collection.php in the method Hustle_Module_Collection::get_embed_id_names(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-module-collection.php

```
8     class Hustle_Module_Collection extends Hustle_Collection {
⋮
277   public function get_embed_id_names( $module_types = array() ) {
278   $types = '';
⋮
280   $temp_array = array();
281   foreach( $module_types as $type ) {
282   array_push( $temp_array, '`module_type` = "'. $type .'"' );
283   }
284   $types = ' AND ( '. implode( ' OR ', $temp_array ) . ' )';
⋮
286   return self::$_db->get_results( self::$_db->prepare( "SELECT `module_id`, `module_name` FROM " . Hustle_Db::
      modules_table() ." WHERE `active`=%d" . $types, 1 ), OBJECT );
287   }
⋮
400   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `module_id`, `module_name` FROM self WHERE `active`=%d AND ( `module_type` = " " )
```

Issue #2210 - wordpress-popup/inc/hustle-module-model.php: 881

Path: wordpress-popup/inc/hustle-module-model.php
Line: 881
Sink: execute
Source: _GET
Taint: HTTP

Code Summary

A code quality issue was detected in line 881 of the file wordpress-popup/inc/hustle-module-model.php in the method Hustle_Module_Model::get_module_type_by_module_id(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-module-model.php

```
9     class Hustle_Module_Model extends Hustle_Model {
⋮
879   public function get_module_type_by_module_id( $module_id ) {
⋮
881   $query = $this->_wpdb->prepare( "
882   SELECT module_type FROM `" . Hustle_Db::modules_table() . "`
883   WHERE `module_id`=%s",
884   $module_id
885   );
⋮
888   }
⋮
1178  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT module_type FROM `self` WHERE `module_id`= $_GET['id']['0']
```

3.7.1. Dynamic SQL Query (Table)

CWE: 89
Severity: Low

A SQL query is constructed with a dynamically concatenated table specification. This can lead to SQL injection attacks.

It is not possible to use prepared statements to secure dynamic table names. It is highly recommended to use a whitelist for all possible table names.

Issue #2089 - wordpress-popup/inc/hustle-model.php: 60

Path: wordpress-popup/inc/hustle-model.php
Line: 60
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 60 of the file wordpress-popup/inc/hustle-model.php in the method Hustle_Model::get().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 60 of the file wordpress-popup/inc/hustle-model.php in the method Hustle_Model::get(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-model.php

```
13    abstract class Hustle_Model extends Hustle_Data {
⋮
55    public function get( $id ){
⋮
60    $data = $this->_wpdb->get_row( $this->_wpdb->prepare( "SELECT * FROM " . Hustle_Db::modules_table() . "
      WHERE `module_id`=%d", $this->id ), OBJECT );
⋮
69    }
⋮
1222  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT * FROM self WHERE `module_id`=%d
```

Issue #2090 - wordpress-popup/inc/hustle-model.php: 523

Path: wordpress-popup/inc/hustle-model.php
Line: 523
Sink: execute

Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 523 of the file wordpress-popup/inc/hustle-model.php in the method Hustle_Model::get_meta().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 523 of the file wordpress-popup/inc/hustle-model.php in the method Hustle_Model::get_meta(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-model.php

```
13    abstract class Hustle_Model extends Hustle_Data {
⋮
512   public function get_meta( $meta_key, $default = null, $get_cached = true ){
⋮
523   $value = $this->_wpdb->get_var( $this->_wpdb->prepare( "SELECT `meta_value` FROM " . Hustle_Db::modules_meta_table() . " WHERE `meta_key`=%s AND `module_id`=%d", $meta_key, (int) $this->id ) );
⋮
530   }
⋮
1222  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `meta_value` FROM self WHERE `meta_key`=%s AND `module_id`=%d
```

Issue #2091 - wordpress-popup/inc/hustle-model.php: 498

Path: wordpress-popup/inc/hustle-model.php
Line: 498
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 498 of the file wordpress-popup/inc/hustle-model.php in the method Hustle_Model::has_meta().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 498 of the file wordpress-popup/inc/hustle-model.php in the method Hustle_Model::has_meta(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-model.php

```
13    abstract class Hustle_Model extends Hustle_Data {
⋮
497   public function has_meta( $meta_key ){
498   return (bool)$this->_wpdb->get_row( $this->_wpdb->prepare( "SELECT * FROM " . Hustle_Db::modules_meta_table() . " WHERE `meta_key`=%s AND `module_id`=%d", $meta_key, (int) $this->id ) );
499   }
⋮
1222  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT * FROM self WHERE `meta_key`=%s AND `module_id`=%d
```

Issue #2092 - wordpress-popup/inc/hustle-module-collection.php: 388

Path: wordpress-popup/inc/hustle-module-collection.php
Line: 388
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 389 of the file wordpress-popup/inc/hustle-module-collection.php in the method Hustle_Module_Collection::get_active_providers_module().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 388 of the file wordpress-popup/inc/hustle-module-collection.php in the method Hustle_Module_Collection::get_active_providers_module(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-module-collection.php

```
8    class Hustle_Module_Collection extends Hustle_Collection {
⋮
383  public static function get_active_providers_module( $slug ) {
384  global $wpdb;
385  $modules_meta_table = Hustle_Db::modules_meta_table();
⋮
388  $query = $wpdb->prepare(
389  "SELECT `module_id`
390  FROM {$modules_meta_table}
391  WHERE `meta_value`
392  LIKE %s
393  AND `meta_key` = 'integrations_settings'",
394  "%". $slug . "%"
395  );
⋮
398  }
⋮
400  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `module_id` FROM self WHERE `meta_value` LIKE %s AND `meta_key` = 'integrations_settings'
```

Issue #2100 - wordpress-popup/inc/hustle-module-model.php: 881

Path: wordpress-popup/inc/hustle-module-model.php
Line: 881
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 881 of the file wordpress-popup/inc/hustle-module-model.php in the method Hustle_Module_Model::get_module_type_by_module_id().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 881 of the file wordpress-popup/inc/hustle-module-model.php in the method Hustle_Module_Model::get_module_type_by_module_id(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-module-model.php

```
9     class Hustle_Module_Model extends Hustle_Model {
⋮
879   public function get_module_type_by_module_id( $module_id ) {
⋮
881   $query = $this->_wpdb->prepare( "
882   SELECT module_type FROM `" . Hustle_Db::modules_table() . "`
883   WHERE `module_id`=%s",
884   $module_id
885   );
⋮
888   }
⋮
1178  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT module_type FROM ` self` WHERE `module_id`=%s
```

Issue #2104 - wordpress-popup/inc/hustle-module-collection.php: 355

Path: wordpress-popup/inc/hustle-module-collection.php
Line: 355
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 355 of the file wordpress-popup/inc/hustle-module-collection.php in the method Hustle_Module_Collection::get_30_modules_ids_by_blog().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 355 of the file wordpress-popup/inc/hustle-module-collection.php in the method Hustle_Module_Collection::get_30_modules_ids_by_blog(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-module-collection.php

```
8     class Hustle_Module_Collection extends Hustle_Collection {
⋮
353   public function get_30_modules_ids_by_blog( $blog_id ) {
354   $modules_table = self::$_db->base_prefix . Hustle_Db::TABLE_HUSTLE_MODULES;
355   return self::$_db->get_col( self::$_db->prepare( "SELECT `module_id` FROM " . $modules_table ." WHERE `blog_
      id`=%d ORDER BY `module_id` ASC", $blog_id ) );
356   }
⋮
400   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `module_id` FROM hustle_db WHERE `blog_id`=%d ORDER BY `module_id` ASC
```

Issue #2105 - wordpress-popup/inc/hustle-migration.php: 1369

Path: wordpress-popup/inc/hustle-migration.php
Line: 1369
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 1370 of the file wordpress-popup/inc/hustle-migration.php in the method Hustle_Migration::get_tracking_submissions_count().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 1369 of the file wordpress-popup/inc/hustle-migration.php in the method Hustle_Migration::get_tracking_submissions_count(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-migration.php

```
8     class Hustle_Migration {
⋮
1346  private static function get_tracking_submissions_count( $wpdb = false, $modules_id ) {
⋮
1354  $modules_id_query = $wpdb->prepare(
1355  "`module_id` IN ({$modules_id_placeholders})",
1356  $modules_id
1357  );
⋮
1362  $meta_keys_query = $wpdb->prepare(
1363  "`meta_key` IN ({$meta_keys_placeholders})",
1364  self::$tracking_meta_keys
1365  );
⋮
1369  $query = $wpdb->prepare(
1370  "SELECT COUNT(*)
1371  FROM `{$wpdb->base_prefix}hustle_modules_meta`
1372  WHERE ({$modules_id_query}
1373  AND {$meta_keys_query})
1374  OR `meta_key` LIKE %s",
1375  '%page_shares'
1376  );
⋮
1380  }
⋮
1534  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT COUNT(*) FROM ` hustle_modules_meta` WHERE ( AND ) OR `meta_key` LIKE %s
```

Issue #2106 - wordpress-popup/inc/hustle-migration.php: 1326

Path: wordpress-popup/inc/hustle-migration.php
Line: 1326
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 1327 of the file wordpress-popup/inc/hustle-migration.php in the method Hustle_Migration::get_paged_metas().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 1326 of the file wordpress-popup/inc/hustle-migration.php in the method Hustle_Migration::get_paged_metas(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-migration.php

```
8     class Hustle_Migration {
⋮
1307  private function get_paged_metas( $modules_id, $current_meta, $limit = 10, $wpdb = false ) {
⋮
1314  $meta_key_query = $wpdb->prepare(
1315  "`meta_key` IN ({$meta_keys_placeholders})", // phpcs:ignore
1316  self::$tracking_meta_keys
1317  );
⋮
1320  $modules_id_query = $wpdb->prepare(
1321  "`module_id` IN ({$modules_id_placeholders})", // phpcs:ignore
1322  $modules_id
1323  );
⋮
1326  $query = $wpdb->prepare(
1327  "SELECT *
1328  FROM `". $wpdb->base_prefix ."hustle_modules_meta`
1329  WHERE `meta_id` > %d
1330  AND (({$modules_id_query}
1331  AND {$meta_key_query})
1332  OR `meta_key` LIKE %s)
1333  ORDER BY `meta_id` ASC
1334  LIMIT %d",
1335  $current_meta,
1336  '%page_shares',
1337  $limit
1338  );
⋮
1344  }
⋮
1534  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT * FROM ` hustle_modules_meta` WHERE `meta_id` > %d AND (( AND ) OR `meta_key` LIKE %s) ORDER BY `meta_id` ASC LIMIT %d
```

Issue #2107 - wordpress-popup/inc/hustle-migration.php: 1510

Path: wordpress-popup/inc/hustle-migration.php
Line: 1510

Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 1511 of the file wordpress-popup/inc/hustle-migration.php in the method Hustle_Migration::get_module_type_by_module_id().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 1510 of the file wordpress-popup/inc/hustle-migration.php in the method Hustle_Migration::get_module_type_by_module_id(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-migration.php

```
8     class Hustle_Migration {
⋮
1505  private function get_module_type_by_module_id( $module_id ) {
1506  global $wpdb;
⋮
1510  $module_type = $wpdb->get_var( $wpdb->prepare(
1511  "SELECT `module_type`
1512  FROM " . Hustle_Db::modules_table() .
1513  " WHERE `module_id`=%d",
1514  $module_id
1515  ) );
⋮
1519  }
⋮
1534  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `module_type` FROM self WHERE `module_id`=%d
```

Issue #2108 - wordpress-popup/inc/hustle-tracking-model.php: 89

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 89
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 80 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::save_tracking().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 89 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::save_tracking(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9     class Hustle_Tracking_Model {
⋮
```

```
59  public function save_tracking( $module_id, $action, $module_type, $page_id, $module_sub_type = null, $date_cr
    eated = null, $ip = null ) {
⋮
64  $ip_query = ' AND `ip` IS NULL';
⋮
69  $ip_query = ' AND `ip` = %s';
⋮
78  $sql = "SELECT `tracking_id` FROM {$this->table_name} WHERE `module_id` = %d AND `page_id` = %d {$ip_
    query} AND `action` = %s AND `module_type` = %s AND `date_created` BETWEEN ";
⋮
80  $sql .= ' utc_date() AND utc_timestamp()';
⋮
82  $sql .= sprintf(
83  "'%s' AND '%s 23:59:59'",
84  substr( $date_created, 0, 10 ),
85  substr( $date_created, 0, 10 )
86  );
⋮
89  $prepared_sql = $wpdb->prepare( $sql, $module_id, $page_id, $ip, $action, $module_type ); // WPCS: unprepare
    d SQL ok. false positive
⋮
100 }
⋮
757 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `tracking_id` FROM WHERE `module_id` = %d AND `page_id` = %d AND `ip` = %s AND `action` = %s AND
`module_type` = %s AND `date_created` BETWEEN utc_date() AND utc_timestamp()
```

Issue #2110 - wordpress-popup/inc/hustle-tracking-model.php: 91

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 91
Sink: execute
Taint: HTTP

Code Summary

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 91 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::save_tracking(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9   class Hustle_Tracking_Model {
⋮
59  public function save_tracking( $module_id, $action, $module_type, $page_id, $module_sub_type = null, $date_cr
    eated = null, $ip = null ) {
⋮
64  $ip_query = ' AND `ip` IS NULL';
⋮
69  $ip_query = ' AND `ip` = %s';
⋮
78  $sql = "SELECT `tracking_id` FROM {$this->table_name} WHERE `module_id` = %d AND `page_id` = %d {$ip_
    query} AND `action` = %s AND `module_type` = %s AND `date_created` BETWEEN ";
⋮
80  $sql .= ' utc_date() AND utc_timestamp()';
⋮
```

```
82  $sql .= sprintf(
83  "'%s' AND '%s 23:59:59'",
84  substr( $date_created, 0, 10 ),

85  substr( $date_created, 0, 10 )
86  );
⋮
89  $prepared_sql = $wpdb->prepare( $sql, $module_id, $page_id, $ip, $action, $module_type ); // WPCS: unprepare
    d SQL ok. false positive
⋮
91  $prepared_sql = $wpdb->prepare( $sql, $module_id, $page_id, $action, $module_type ); // WPCS: unprepared S
    QL ok. false positive
⋮
100 }
⋮
757 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `tracking_id` FROM WHERE `module_id` = %d AND `page_id` = %d AND `ip` = %s AND `action` = %s AND
`module_type` = %s AND `date_created` BETWEEN utc_date() AND utc_timestamp()
```

Issue #2112 - wordpress-popup/inc/hustle-tracking-model.php: 181

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 181
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 182 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::_update().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 181 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::_update(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9   class Hustle_Tracking_Model {
⋮
175 private function _update( $id, $db = false ) {
⋮
180 $date = Opt_In_Utils::get_current_date();
181 $db->query( $db->prepare(
182 "UPDATE {$this->table_name} SET `counter` = `counter`+1, `date_updated` = %s WHERE `tracking_id` = %d"
    ,
183 $date,
184 $id
185 ));
186 }
⋮
757 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
UPDATE SET `counter` = `counter`+1, `date_updated` = %s WHERE `tracking_id` = %d
```

Issue #2113 - wordpress-popup/inc/hustle-entry-model.php: 127

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 127
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 126 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::get().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 127 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::get(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
109   public function get( $entry_id ) {
⋮
126   $sql = "SELECT `entry_type`, `module_id`, `date_created` FROM {$this->table_name} WHERE `entry_id` = %d";
127   $entry = $wpdb->get_row( $wpdb->prepare( $sql, $entry_id ) ); // WPCS: unprepared SQL ok. false positive
⋮
140   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `entry_type`, `module_id`, `date_created` FROM WHERE `entry_id` = %d
```

Issue #2114 - wordpress-popup/inc/hustle-entry-model.php: 236

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 236
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 235 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::load_meta().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 236 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::load_meta(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
229   public function load_meta( $db = false ) {
⋮
234   $this->meta_data = array();
235   $sql = "SELECT `meta_id`, `meta_key`, `meta_value` FROM {$this->table_meta_name} WHERE `entry_id` =
      %d";
236   $results = $db->get_results( $db->prepare( $sql, $this->entry_id ) );
⋮
243   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `meta_id`, `meta_key`, `meta_value` FROM WHERE `entry_id` = %d
```

Issue #2115 - wordpress-popup/inc/hustle-module-collection.php: 297

Path: wordpress-popup/inc/hustle-module-collection.php
Line: 297
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 298 of the file wordpress-popup/inc/hustle-module-collection.php in the method Hustle_Module_Collection::get_hustle_30_modules().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 297 of the file wordpress-popup/inc/hustle-module-collection.php in the method Hustle_Module_Collection::get_hustle_30_modules(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-module-collection.php

```
8     class Hustle_Module_Collection extends Hustle_Collection {
⋮
295   public function get_hustle_30_modules( $blog_id = null ) {
296   $db = self::$_db;
297   $sql = $db->prepare(
298   "SELECT * FROM `". $db->base_prefix ."hustle_modules` WHERE `blog_id` > 0 AND `blog_id` = %d",
299   get_current_blog_id()
300   );
⋮
344   }
⋮
400   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT * FROM ` hustle_modules` WHERE `blog_id` > 0 AND `blog_id` = %d
```

Issue #2116 - wordpress-popup/inc/hustle-module-collection.php: 324

Path: wordpress-popup/inc/hustle-module-collection.php
Line: 324
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 325 of the file wordpress-popup/inc/hustle-module-collection.php in the method Hustle_Module_Collection::get_hustle_30_modules().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 324 of the file wordpress-popup/inc/hustle-module-collection.php in the method Hustle_Module_Collection::get_hustle_30_modules(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-module-collection.php

```
8    class Hustle_Module_Collection extends Hustle_Collection {
⋮
295  public function get_hustle_30_modules( $blog_id = null ) {
⋮
324  $sql = $db->prepare(
325  "SELECT `meta_value`, `meta_key`
326  FROM `{$db->base_prefix}hustle_modules_meta`
327  WHERE `module_id` = %d",
328  $module_id );
⋮
344  }
⋮
400  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `meta_value`, `meta_key` FROM ` hustle_modules_meta` WHERE `module_id` = %d
```

Issue #2119 - wordpress-popup/inc/hustle-tracking-model.php: 370

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 370
Sink: get_var
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 366 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_latest_conversion_date().

The user-supplied data is then used unsanitized in the sensitive operation get_var() in line 370 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_latest_conversion_date(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
347  public function get_latest_conversion_date( $module_type = 'popup' ) {
⋮
366  $sql = "SELECT `date_updated` FROM {$this->table_name} {$where_query} AND `action` IN ( 'conversion', 'optin_conversion', 'cta_conversion' ) ORDER BY `date_updated` DESC";
⋮
368  $sql = "SELECT `date_updated` FROM {$this->table_name} WHERE `action` IN ( 'conversion', 'optin_conversion', 'cta_conversion' ) ORDER BY `date_updated` DESC";
⋮
370  $date = $wpdb->get_var( $sql ); // WPCS: unprepared SQL ok. false positive
⋮
372  }
⋮
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `date_updated` FROM AND `action` IN ( 'conversion', 'optin_conversion', 'cta_conversion' ) ORDER BY `date_updated` DESC
```

Issue #2123 - wordpress-popup/inc/hustle-tracking-model.php: 254

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 254
Sink: get_var
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 253 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::_count().

The user-supplied data is then used unsanitized in the sensitive operation get_var() in line 254 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::_count(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
235  private function _count( $action, $module_id = null, $module_subtype = null, $starting_date = null, $ending_date = null ) {
⋮
252  $date_query = $this->_generate_date_query( $wpdb, $starting_date, $ending_date );
253  $sql = "SELECT SUM(`counter`) FROM {$this->table_name} {$where_query} $date_query";
254  $counts = $wpdb->get_var( $sql ); // WPCS: unprepared SQL ok. false positive
⋮
259  }
⋮
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT SUM(`counter`) FROM
```

Issue #2124 - wordpress-popup/inc/hustle-tracking-model.php: 559

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 559
Sink: get_var
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 560 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_most_conversions_module_id().

The user-supplied data is then used unsanitized in the sensitive operation get_var() in line 559 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_most_conversions_module_id(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
556  public function get_most_conversions_module_id() {
557  global $wpdb;
⋮
559  $value = intval( $wpdb->get_var( // WPCS: unprepared SQL OK.
560  "SELECT `module_id` FROM " . $this->table_name . " WHERE `action` IN ( 'conversion', 'optin_conversion', 'cta_c
     onversion' ) GROUP BY `module_id` ORDER BY sum(`counter`) DESC LIMIT 1"
561  ) );
⋮
564  }
⋮
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `module_id` FROM WHERE `action` IN ( 'conversion', 'optin_conversion', 'cta_conversion' ) GROUP BY
`module_id` ORDER BY sum(`counter`) DESC LIMIT 1
```

Issue #2125 - wordpress-popup/inc/hustle-tracking-model.php: 579

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 579
Sink: get_var
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 575 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_today_conversions().

The user-supplied data is then used unsanitized in the sensitive operation get_var() in line 579 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_today_conversions(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
573  public function get_today_conversions() {
574  global $wpdb;
575  $sql = sprintf(
576  'SELECT COUNT(*) FROM `%s` WHERE `action` = "conversion" AND `date_created` > DATE_SUB( NOW(), INTERVAL 24 hour )',
577  $this->table_name
578  );
579  $value = intval( $wpdb->get_var( $sql ) );
⋮
581  }
⋮
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT COUNT(*) FROM ` ` WHERE `action` = "conversion" AND `date_created` > DATE_SUB( NOW(), INTERVAL 24 hour )
```

Issue #2126 - wordpress-popup/inc/hustle-tracking-model.php: 596

Path:	wordpress-popup/inc/hustle-tracking-model.php
Line:	596
Sink:	get_var
Taint:	HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 592 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_last_week_conversions().

The user-supplied data is then used unsanitized in the sensitive operation get_var() in line 596 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_last_week_conversions(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
590  public function get_last_week_conversions() {
591  global $wpdb;
592  $sql = sprintf(
593  'SELECT COUNT(*) FROM `%s` WHERE `action` = "conversion" AND `date_created` > DATE_SUB( NOW(), INTERVAL 7 DAY )',
594  $this->table_name
595  );
596  $value = intval( $wpdb->get_var( $sql ) );
⋮
598  }
⋮
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT COUNT(*) FROM ` ` WHERE `action` = "conversion" AND `date_created` > DATE_SUB( NOW(), INTERVAL 7
DAY )
```

Issue #2127 - wordpress-popup/inc/hustle-tracking-model.php: 613

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 613
Sink: get_var
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 609 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_last_month_conversions().

The user-supplied data is then used unsanitized in the sensitive operation get_var() in line 613 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_last_month_conversions(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
607  public function get_last_month_conversions() {
608  global $wpdb;
609  $sql = sprintf(
610  'SELECT COUNT(*) FROM `%s` WHERE `action` = "conversion" AND `date_created` > DATE_SUB( NOW(), INTER
     VAL 1 MONTH )',
611  $this->table_name
612  );
613  $value = intval( $wpdb->get_var( $sql ) );
⋮
615  }
⋮
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT COUNT(*) FROM ` ` WHERE `action` = "conversion" AND `date_created` > DATE_SUB( NOW(), INTERVAL 1
MONTH )
```

Issue #2128 - wordpress-popup/inc/hustle-tracking-model.php: 458

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 458
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 459 of the file wordpress-popup/inc/hustle-tracking-model.php in the method

Hustle_Tracking_Model::get_ssharing_per_page_conversion_count().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 458 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_ssharing_per_page_conversion_count(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
452  public function get_ssharing_per_page_conversion_count( $limit ) {
⋮
454  global $wpdb;
⋮
456  $table_name = $this->table_name;
⋮
458  $query = $wpdb->prepare(
459  "SELECT SUM(`counter`) AS tracked_count, `page_id` AS page_id
460  FROM {$table_name}
461  WHERE `action` = '_page_shares'
462  OR ( `module_type` LIKE %s AND `action` = 'conversion' )
463  GROUP BY `page_id`
464  ORDER BY `counter` DESC
465  LIMIT %d",
466  Hustle_Module_Model::SOCIAL_SHARING_MODULE .'%',
467  $limit
468  );
⋮
471  }
⋮
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT SUM(`counter`) AS tracked_count, `page_id` AS page_id FROM WHERE `action` = '_page_shares' OR (
`module_type` LIKE %s AND `action` = 'conversion' ) GROUP BY `page_id` ORDER BY `counter` DESC LIMIT %d
```

Issue #2129 - wordpress-popup/inc/hustle-entry-model.php: 514

Path:	wordpress-popup/inc/hustle-entry-model.php
Line:	514
Sink:	get_var
Taint:	HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 514 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::global_count_entries().

The user-supplied data is then used unsanitized in the sensitive operation get_var() in line 514 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::global_count_entries(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
503   public static function global_count_entries() {
⋮
513   $table_name = Hustle_Db::entries_table();
514   $global_count = (int)$wpdb->get_var( "SELECT count(`entry_id`) FROM {$table_name}" ); //WPCS: unprepared
      SQL ok. false positive
⋮
519   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT count(`entry_id`) FROM self
```

Issue #2130 - wordpress-popup/inc/hustle-tracking-model.php: 398

Path:	wordpress-popup/inc/hustle-tracking-model.php
Line:	398
Sink:	execute
Taint:	HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 397 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_latest_conversion_date_by_module_id().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 398 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_latest_conversion_date_by_module_id(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9     class Hustle_Tracking_Model {
⋮
384   public function get_latest_conversion_date_by_module_id( $module_id, $sub_type = '', $cta_or_optin = 'all_conv
      ersion' ) {
⋮
397   $sql = "SELECT `date_updated` FROM {$this->table_name} WHERE `module_id` = %d {$and_action}{$and_su
      btype} ORDER BY `date_updated` DESC";
398   $date = $wpdb->get_var( $wpdb->prepare( $sql, $module_id ) ); // WPCS: unprepared SQL ok. false positive
⋮
400   }
⋮
757   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `date_updated` FROM WHERE `module_id` = %d ORDER BY `date_updated` DESC
```

Issue #2131 - wordpress-popup/inc/hustle-tracking-model.php: 217

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 217
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 217 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::has_old_tracking_data().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 217 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::has_old_tracking_data(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
215  public function has_old_tracking_data( $module_id ) {
216  global $wpdb;
     $result = $wpdb->get_var( $wpdb->prepare( "SELECT COUNT( tracking_id ) FROM {$this->table_name} WHERE
217  module_id = %d AND action = 'conversion'", $module_id ) ); //phpcs:ignore
     WordPress.DB.PreparedSQL.NotPrepared
⋮
220  }
⋮
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT COUNT( tracking_id ) FROM WHERE module_id = %d AND action = 'conversion'
```

Issue #2132 - wordpress-popup/inc/hustle-tracking-model.php: 333

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 333
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 324 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_form_latest_tracking_data_count_grouped_by_day().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 333 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_form_latest_tracking_data_count_grouped_by_day(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
```

```
296  public function get_form_latest_tracking_data_count_grouped_by_day( $module_id, $date_created, $action, $mo
     dule_type = null, $module_sub_type = null ) {
⋮
298  $table_name = $this->table_name;
⋮
323  $date_query = $this->_generate_date_query( $wpdb, $date_created );
324  $sql = "SELECT SUM(`counter`) AS tracked_count,
325  DATE(e.date_created) AS date_created
326  FROM {$table_name} e
327  WHERE e.module_id = %d
328  {$and_action}
329  {$sub_type_query}
330  {$date_query}
331  GROUP BY DATE(e.date_created)
332  ORDER BY e.date_created DESC";
333  $sql = $wpdb->prepare( $sql, // phpcs:ignore WordPress.DB.PreparedSQL.NotPrepared
334  $module_id );
⋮
337  }
⋮
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT SUM(`counter`) AS tracked_count, DATE(e.date_created) AS date_created FROM e WHERE e.module_id = %d
GROUP BY DATE(e.date_created) ORDER BY e.date_created DESC
```

Issue #2133 - wordpress-popup/inc/hustle-module-model.php: 861

Path: wordpress-popup/inc/hustle-module-model.php
Line: 861
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 861 of the file wordpress-popup/inc/hustle-module-model.php in the method Hustle_Module_Model::get_module_id_by_shortcode_id().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 861 of the file wordpress-popup/inc/hustle-module-model.php in the method Hustle_Module_Model::get_module_id_by_shortcode_id(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-module-model.php

```
9    class Hustle_Module_Model extends Hustle_Model {
⋮
859  public function get_module_id_by_shortcode_id( $shortcode_id ) {
⋮
861  $module_id = $this->_wpdb->get_var( $this->_wpdb->prepare( "
862  SELECT module_id FROM `" . Hustle_Db::modules_meta_table() . "`
863  WHERE `meta_key`='shortcode_id'
864  AND `meta_value`=%s", $shortcode_id
865  ));
⋮
868  }
```

```
⋮
1178 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT module_id FROM ` self` WHERE `meta_key`='shortcode_id' AND `meta_value`=%s
```

Issue #2134 - wordpress-popup/inc/hustle-entry-model.php: 662

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 662
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 663 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_entries().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 662 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_entries(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
657   public static function delete_entries( $module_id ) {
658   global $wpdb;
⋮
660   $entires_table = Hustle_Db::entries_table();
⋮
662   $entires = $wpdb->get_col( $wpdb->prepare(
663   "SELECT `entry_id` FROM {$entires_table} WHERE `module_id` = %d", //phpcs:ignore
664   $module_id
665   ) );
⋮
695   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `entry_id` FROM self WHERE `module_id` = %d
```

Issue #2135 - wordpress-popup/inc/hustle-entry-model.php: 668

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 668
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 669 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_entries().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 668 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_entries(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
657   public static function delete_entries( $module_id ) {
658   global $wpdb;

⋮
662   $entires = $wpdb->get_col( $wpdb->prepare(
663   "SELECT `entry_id` FROM {$entires_table} WHERE `module_id` = %d", //phpcs:ignore
664   $module_id
665   ) );
⋮
668   $wpdb->query(
669   "DELETE FROM {$entires_meta_table} WHERE `entry_id` IN ('" . implode( "','", $entires ) . "')" //phpcs:ignore
670   );
⋮
695   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DELETE FROM self WHERE `entry_id` IN ('1')
```

Issue #2136 - wordpress-popup/inc/hustle-model.php: 139

Path: wordpress-popup/inc/hustle-model.php
Line: 139
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 140 of the file wordpress-popup/inc/hustle-model.php in the method Hustle_Model::get_by_shortcode().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 139 of the file wordpress-popup/inc/hustle-model.php in the method Hustle_Model::get_by_shortcode(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-model.php

```
13    abstract class Hustle_Model extends Hustle_Data {
⋮
126   public function get_by_shortcode( $shortcode_id, $enforce_type = true ){
⋮
135   $prefix = $this->_wpdb->prefix;
⋮
139   $sql = $this->_wpdb->prepare(
```

```
140   "SELECT * FROM `" . Hustle_Db::modules_table() . "` as modules
141   JOIN `{$prefix}hustle_modules_meta` as meta
142   ON modules.`module_id`=meta.`module_id`

143   WHERE `meta_key`='shortcode_id'
144   AND (`module_type` = 'embedded' OR `module_type` = 'social_sharing')
145   AND `meta_value`=%s",
146   trim( $shortcode_id)
147   );
⋮
166   }
⋮
1222  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT * FROM ` self` as modules JOIN ` hustle_modules_meta` as meta ON modules.`module_id`=meta.`module_id`
WHERE `meta_key`='shortcode_id' AND (`module_type` = 'embedded' OR `module_type` = 'social_sharing') AND
`meta_value`=%s
```

Issue #2137 - wordpress-popup/inc/hustle-model.php: 150

Path: wordpress-popup/inc/hustle-model.php
Line: 150
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 151 of the file wordpress-popup/inc/hustle-model.php in the method Hustle_Model::get_by_shortcode().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 150 of the file wordpress-popup/inc/hustle-model.php in the method Hustle_Model::get_by_shortcode(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-model.php

```
13    abstract class Hustle_Model extends Hustle_Data {
⋮
126   public function get_by_shortcode( $shortcode_id, $enforce_type = true ){
⋮
135   $prefix = $this->_wpdb->prefix;
⋮
150   $sql = $this->_wpdb->prepare(
151   "SELECT * FROM `" . Hustle_Db::modules_table() . "` as modules
152   JOIN `{$prefix}hustle_modules_meta` as meta
153   ON modules.`module_id`=meta.`module_id`
154   WHERE `meta_key`='shortcode_id'
155   AND `meta_value`=%s",
156   trim( $shortcode_id )
157   );
⋮
166   }
⋮
1222  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT * FROM ` self` as modules JOIN ` hustle_modules_meta` as meta ON modules.`module_id`=meta.`module_id`
WHERE `meta_key`='shortcode_id' AND `meta_value`=%s
```

Issue #2139 - wordpress-popup/inc/hustle-modules-common-admin-ajax.php: 801

Path: wordpress-popup/inc/hustle-modules-common-admin-ajax.php
Line: 801
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 801 of the file wordpress-popup/inc/hustle-modules-common-admin-ajax.php in the method Hustle_Modules_Common_Admin_Ajax::get_new_condition_ids().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 801 of the file wordpress-popup/inc/hustle-modules-common-admin-ajax.php in the method Hustle_Modules_Common_Admin_Ajax::get_new_condition_ids(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-modules-common-admin-ajax.php

```
10   class Hustle_Modules_Common_Admin_Ajax {
⋮
782  public function get_new_condition_ids() {
⋮
800  global $wpdb;
801  $result = $wpdb->get_results( $wpdb->prepare( "SELECT ID as id, post_title as text FROM {$wpdb->posts} "
802  . "WHERE post_type = %s AND post_status = 'publish' AND post_title LIKE %s LIMIT " . intval( $limit ), $post_type
     , '%'. $search . '%' ) );
⋮
820  }
⋮
822  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT ID as id, post_title as text FROM WHERE post_type = %s AND post_status = 'publish' AND post_title LIKE %s
LIMIT 123
```

Issue #2141 - wordpress-popup/inc/hustle-entry-model.php: 645

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 645
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 644 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entry().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 645

of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entry(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
626   public static function delete_by_entry( $module_id, $entry_id, $db = false ) {
⋮
634   $table_meta_name = Hustle_Db::entries_meta_table();
⋮
644   $sql = "DELETE FROM {$table_meta_name} WHERE `entry_id` = %d";
645   $db->query( $db->prepare( $sql, $entry_id ) );
⋮
655   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DELETE FROM self WHERE `entry_id` = %d
```

Issue #2142 - wordpress-popup/inc/hustle-entry-model.php: 645

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 645
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 644 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entry().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 645 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entry(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
626   public static function delete_by_entry( $module_id, $entry_id, $db = false ) {
⋮
644   $sql = "DELETE FROM {$table_meta_name} WHERE `entry_id` = %d";
645   $db->query( $db->prepare( $sql, $entry_id ) );
⋮
655   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DELETE FROM self WHERE `entry_id` = %d
```

Issue #2143 - wordpress-popup/inc/hustle-entry-model.php: 648

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 648
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 647 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entry().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 648 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entry(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
626   public static function delete_by_entry( $module_id, $entry_id, $db = false ) {
⋮
633   $table_name = Hustle_Db::entries_table();
⋮
647   $sql = "DELETE FROM {$table_name} WHERE `entry_id` = %d";
648   $db->query( $db->prepare( $sql, $entry_id ) );
⋮
655   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DELETE FROM self WHERE `entry_id` = %d
```

Issue #2144 - wordpress-popup/inc/hustle-entry-model.php: 648

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 648
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 647 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entry().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 648 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entry(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
```

```
⋮
626   public static function delete_by_entry( $module_id, $entry_id, $db = false ) {
⋮
647   $sql = "DELETE FROM {$table_name} WHERE `entry_id` = %d";
648   $db->query( $db->prepare( $sql, $entry_id ) );
⋮
655   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DELETE FROM self WHERE `entry_id` = %d
```

Issue #2145 - wordpress-popup/inc/hustle-entry-model.php: 602

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 602
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 602 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entries().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 602 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entries(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
568   public static function delete_by_entries( $module_id, $entries, $db = false ) {
⋮
582   $table_meta_name = Hustle_Db::entries_meta_table();
⋮
593   $prepared_placeholders = implode( ', ', array_fill( 0, count( $entries ), '%s' ) );
⋮
602   $sql = $db->prepare( "DELETE FROM {$table_meta_name} WHERE `entry_id` IN ($prepared_placeholders)", $
      entries );
⋮
615   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DELETE FROM self WHERE `entry_id` IN (%s)
```

Issue #2146 - wordpress-popup/inc/hustle-entry-model.php: 603

Path: wordpress-popup/inc/hustle-entry-model.php

Line: 603
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 602 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entries().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 603 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entries(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
568   public static function delete_by_entries( $module_id, $entries, $db = false ) {
⋮
582   $table_meta_name = Hustle_Db::entries_meta_table();
⋮
593   $prepared_placeholders = implode( ', ', array_fill( 0, count( $entries ), '%s' ) );
⋮
602   $sql = $db->prepare( "DELETE FROM {$table_meta_name} WHERE `entry_id` IN ($prepared_placeholders)", $
      entries );
603   $db->query( $sql );
⋮
615   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DELETE FROM self WHERE `entry_id` IN (%s)
```

Issue #2147 - wordpress-popup/inc/hustle-entry-model.php: 605

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 605
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 605 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entries().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 605 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entries(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
```

```
⋮
568  public static function delete_by_entries( $module_id, $entries, $db = false ) {
⋮
581  $table_name = Hustle_Db::entries_table();
⋮
593  $prepared_placeholders = implode( ', ', array_fill( 0, count( $entries ), '%s' ) );
⋮
605  $sql = $db->prepare( "DELETE FROM {$table_name} WHERE `entry_id` IN ($prepared_placeholders)", $entries
     );
⋮
615  }
⋮
1130 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DELETE FROM self WHERE `entry_id` IN (%s)
```

Issue #2148 - wordpress-popup/inc/hustle-entry-model.php: 606

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 606
Sink: execute
Taint: HTTP

Code Summary

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 606 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_by_entries(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9    class Hustle_Entry_Model {
⋮
568  public static function delete_by_entries( $module_id, $entries, $db = false ) {
⋮
581  $table_name = Hustle_Db::entries_table();
⋮
593  $prepared_placeholders = implode( ', ', array_fill( 0, count( $entries ), '%s' ) );
⋮
602  $sql = $db->prepare( "DELETE FROM {$table_meta_name} WHERE `entry_id` IN ($prepared_placeholders)", $
     entries );
⋮
     $sql = $db->prepare( "DELETE FROM {$table_name} WHERE `entry_id` IN ($prepared_placeholders)", $entries
605  );

606  $db->query( $sql );
⋮
615  }
⋮
1130 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DELETE FROM self WHERE `entry_id` IN (%s)
```

Issue #2150 - wordpress-popup/inc/hustle-entry-model.php: 485

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 485
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 484 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::count_entries().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 485 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::count_entries(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
471   public static function count_entries( $module_id, $db = false ) {
⋮
483   $table_name = Hustle_Db::entries_table();
484   $sql = "SELECT count(`entry_id`) FROM {$table_name} WHERE `module_id` = %d";
485   $entries = $db->get_var( $db->prepare( $sql, $module_id ) );
⋮
494   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT count(`entry_id`) FROM self WHERE `module_id` = %d
```

Issue #2151 - wordpress-popup/inc/hustle-entry-model.php: 436

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 436
Sink: get_var
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 427 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::query_entries().

The user-supplied data is then used unsanitized in the sensitive operation get_var() in line 436 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::query_entries(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
```

```
350  public static function query_entries( $args, &$count ) {
⋮
381  $entries_meta_table_name = Hustle_Db::entries_meta_table();
⋮
386  $where = 'WHERE 1=1';
⋮
388  $where .= $wpdb->prepare( ' AND metas.meta_key NOT LIKE %s', $wpdb->esc_like( 'hustle_provider_' ) . '%' );
⋮
391  $where .= $wpdb->prepare( ' AND entries.module_id = %d', $args['module_id'] );
⋮
398  $where .= $wpdb->prepare( ' AND ( entries.date_created >= %s AND entries.date_created <= %s )', $date_cr
     eated[0], $date_created[1] );
⋮
403  $where .= $wpdb->prepare( ' AND metas.meta_value LIKE %s', '%' . $wpdb->esc_like( $args['search_email'] ) .
     '%' );
⋮
426  $sql_count
427  = "SELECT count(DISTINCT entries.entry_id) as total_entries
428  FROM
429  {$entries_table_name} AS entries
430  INNER JOIN {$entries_meta_table_name} AS metas
431  ON (entries.entry_id = metas.entry_id)
432  {$where}
433  ";
⋮
435  $sql_count = apply_filters( 'hustle_query_entries_sql_count', $sql_count, $args );
436  $count = intval( $wpdb->get_var( $sql_count ) ); // WPCS: unprepared SQL ok. false positive
⋮
461  }
⋮
1130 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT count(DISTINCT entries.entry_id) as total_entries FROM self AS entries INNER JOIN self AS metas ON
(entries.entry_id = metas.entry_id) WHERE 1=11
```

Issue #2152 - wordpress-popup/inc/hustle-entry-model.php: 453

Path:	wordpress-popup/inc/hustle-entry-model.php
Line:	453
Sink:	get_results
Taint:	HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 441 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::query_entries().

The user-supplied data is then used unsanitized in the sensitive operation get_results() in line 453 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::query_entries(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9    class Hustle_Entry_Model {
⋮
350  public static function query_entries( $args, &$count ) {
```

```
⋮
407    $group_by = 'GROUP BY entries.entry_id';
408    $group_by = apply_filters( 'hustle_query_entries_group_by', $group_by, $args );
⋮
422    $limit = $wpdb->prepare( 'LIMIT %d, %d', $args['offset'], $args['per_page'] );
423    $limit = apply_filters( 'hustle_query_entries_limit', $limit, $args );

⋮
440    $sql
441    = "SELECT entries.entry_id AS entry_id
442    FROM
443    {$entries_table_name} AS entries
444    INNER JOIN {$entries_meta_table_name} AS metas
445    ON (entries.entry_id = metas.entry_id)
446    {$where}
447    {$group_by}
448    {$order_by} {$order}
449    {$limit}
450    ";
⋮
452    $sql = apply_filters( 'hustle_query_entries_sql', $sql, $args );
453    $results = $wpdb->get_results( $sql ); // WPCS: unprepared SQL ok. false positive
⋮
461    }
⋮
1130   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT entries.entry_id AS entry_id FROM self AS entries INNER JOIN self AS metas ON (entries.entry_id =
metas.entry_id) WHERE 1=11 GROUP BY entries.entry_id ORDER BY DESC 1
```

Issue #2153 - wordpress-popup/inc/hustle-entry-model.php: 546

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 546
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 545 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::get_entries().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 546 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::get_entries(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9      class Hustle_Entry_Model {
⋮
541    public static function get_entries( $module_id ) {
542    global $wpdb;
⋮
544    $table_name = Hustle_Db::entries_table();
545    $sql = "SELECT `entry_id` FROM {$table_name} WHERE `module_id` = %d ORDER BY `entry_id` DESC";
```

```
546   $results = $wpdb->get_results( $wpdb->prepare( $sql, $module_id ) ); // WPCS: unprepared SQL ok. false positive
⋮
555   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `entry_id` FROM self WHERE `module_id` = %d ORDER BY `entry_id` DESC
```

Issue #2154 - wordpress-popup/inc/hustle-tracking-model.php: 628

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 628
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 624 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::set_null_on_all_ips().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 628 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::set_null_on_all_ips(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9     class Hustle_Tracking_Model {
⋮
622   public function set_null_on_all_ips() {
623   global $wpdb;
624   $query = sprintf(
625   'UPDATE `%s` SET `ip` = NULL WHERE `ip` IS NOT NULL',
626   $this->table_name
627   );
628   $wpdb->query( $query );
629   }
⋮
757   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
UPDATE ` ` SET `ip` = NULL WHERE `ip` IS NOT NULL
```

Issue #2155 - wordpress-popup/inc/hustle-tracking-model.php: 668

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 668
Sink: execute
Taint: HTTP

Code Summary

Code Summary

User-supplied data is concatenated into sql markup in line 666 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::set_null_on_selected_ips().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 668 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::set_null_on_selected_ips(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9     class Hustle_Tracking_Model {
⋮
638   public function set_null_on_selected_ips( $ips ) {
⋮
656   $query = sprintf( 'UPDATE `%s` SET `ip` = NULL WHERE ', $this->table_name );
⋮
658   $query .= sprintf(
659   '`ip` IN ( %s ) ', implode( ', ', array_map( array( $this, 'wrap_ip' ), $in ) )
660   );
⋮
662   $query .= 'OR ';
⋮
666   $query .= implode( ' OR ', $ranges );
⋮
668   $wpdb->query( $query );
669   }
⋮
757   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
UPDATE ` ` SET `ip` = NULL WHERE `ip` IN ( 1 ) OR ( INET_ATON( `ip` ) BETWEEN d AND d )
```

Issue #2156 - wordpress-popup/inc/hustle-entry-model.php: 1127

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 1127
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 1126 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_selected_ips().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 1127 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::delete_selected_ips(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
1092  public function delete_selected_ips( $ips ) {
```

```
⋮
1097  $in = array();
⋮
1107  $in[] = $one;
⋮
1110  $query = sprintf(
1111  'DELETE FROM `%s` WHERE `meta_key` = \'hustle_ip\' AND ( ',
1112  Hustle_Db::entries_meta_table()
1113  );
⋮
1115  $formatted_in_array = array_map( function( $a ) {
1116  return sprintf( '\'%s\'', $a );
1117  }, $in );
1118  $query .= sprintf( '`meta_value` IN ( %s ) ', implode( ', ', $formatted_in_array ) );
⋮
1120  $query .= 'OR ';
⋮
1124  $query .= implode( ' OR ', $ranges );
⋮
1126  $query .= ' )';
1127  $wpdb->query( $query );
1128  }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DELETE FROM ` self` WHERE `meta_key` = 'hustle_ip' AND ( `meta_value` IN ( ''Array'' ) OR ( INET_ATON(
`meta_value` ) BETWEEN d AND d ) )
```

Issue #2158 - wordpress-popup/inc/hustle-deletion.php: 151

Path: wordpress-popup/inc/hustle-deletion.php
Line: 151
Sink: get_var
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 150 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_module_submissions().

The user-supplied data is then used unsanitized in the sensitive operation get_var() in line 151 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_module_submissions(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8     class Hustle_Deletion {
⋮
146   public static function hustle_clear_module_submissions() {
147   global $wpdb;
⋮
150   $max_entry_id_query = "SELECT MAX(`entry_id`) FROM {$wpdb->prefix}hustle_entries";
151   $max_entry_id = $wpdb->get_var( $max_entry_id_query ); // phpcs:ignore
⋮
200   }
```

```
⋮
228 }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT MAX(`entry_id`) FROM hustle_entries
```

Issue #2159 - wordpress-popup/inc/hustle-deletion.php: 155

Path: wordpress-popup/inc/hustle-deletion.php
Line: 155
Sink: get_var
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 154 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_module_submissions().

The user-supplied data is then used unsanitized in the sensitive operation get_var() in line 155 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_module_submissions(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8     class Hustle_Deletion {
⋮
146   public static function hustle_clear_module_submissions() {

147   global $wpdb;
⋮
154   $max_entry_meta_id_query = "SELECT MAX(`meta_id`) FROM {$wpdb->prefix}hustle_entries_meta";
155   $max_entry_meta_id = $wpdb->get_var( $max_entry_meta_id_query ); // phpcs:ignore
⋮
200   }
⋮
228   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT MAX(`meta_id`) FROM hustle_entries_meta
```

Issue #2166 - wordpress-popup/inc/hustle-deletion.php: 94

Path: wordpress-popup/inc/hustle-deletion.php
Line: 94
Sink: get_var
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 93 of the file wordpress-

popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_modules().

The user-supplied data is then used unsanitized in the sensitive operation get_var() in line 94 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_modules(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
89   public static function hustle_clear_modules() {
90   global $wpdb;
⋮
93   $max_module_id_query = "SELECT MAX(`module_id`) FROM {$wpdb->prefix}hustle_modules";
94   $max_module_id = (int) $wpdb->get_var( $max_module_id_query ); // phpcs:ignore
⋮
139  }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT MAX(`module_id`) FROM hustle_modules
```

Issue #2167 - wordpress-popup/inc/hustle-deletion.php: 98

Path: wordpress-popup/inc/hustle-deletion.php
Line: 98
Sink: get_var
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 97 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_modules().

The user-supplied data is then used unsanitized in the sensitive operation get_var() in line 98 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_clear_modules(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
89   public static function hustle_clear_modules() {
90   global $wpdb;
⋮
97   $max_module_meta_id_query = "SELECT MAX(`meta_id`) FROM {$wpdb->prefix}hustle_modules_meta";
98   $max_module_meta_id = (int) $wpdb->get_var( $max_module_meta_id_query ); // phpcs:ignore
⋮
139  }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT MAX(`meta_id`) FROM hustle_modules_meta
```

Issue #2174 - wordpress-popup/inc/opt-in-utils.php: 361

Path: wordpress-popup/inc/opt-in-utils.php
Line: 361
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 361 of the file wordpress-popup/inc/opt-in-utils.php in the method Opt_In_Utils::update_hustle_edit_module_capability().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 361 of the file wordpress-popup/inc/opt-in-utils.php in the method Opt_In_Utils::update_hustle_edit_module_capability(). Please refer to the context and description for further information.

wordpress-popup/inc/opt-in-utils.php

```
10    class Opt_In_Utils {
⋮
349   public static function update_hustle_edit_module_capability( $roles = null ) {
⋮
352   $table = Hustle_Db::modules_meta_table();
⋮
361   $result = $wpdb->get_var( $wpdb->prepare( "SELECT module_id FROM `{$table}` WHERE `meta_key`='edit_r
      oles' AND meta_value LIKE %s LIMIT 1", '%"' . $role_key . '"%' ) ); // WPCS: unprepared SQL OK. False positive.
⋮
374   }
⋮
1324  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT module_id FROM ` self` WHERE `meta_key`='edit_roles' AND meta_value LIKE %s LIMIT 1
```

Issue #2182 - wordpress-popup/inc/hustle-entry-model.php: 1042

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 1042
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 1037 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::get_older_entry_ids().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 1042 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::get_older_entry_ids(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
1034  public static function get_older_entry_ids( $date_created ) {
1035  global $wpdb;
1036  $entries_table = Hustle_Db::entries_table();
1037  $query = "SELECT e.entry_id AS entry_id
1038  FROM {$entries_table} e
1039  WHERE e.date_created < %s";
⋮
1042  $query = $wpdb->prepare( $query, $date_created );
⋮
1046  }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT e.entry_id AS entry_id FROM self e WHERE e.date_created < %s
```

Issue #2183 - wordpress-popup/inc/hustle-tracking-model.php: 709

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 709
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 704 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_older_tracking_ids().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 709 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_older_tracking_ids(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9     class Hustle_Tracking_Model {
⋮
701   public static function get_older_tracking_ids( $date_created ) {
702   global $wpdb;
703   $tracking_table = Hustle_Db::tracking_table();
704   $query = "SELECT e.tracking_id AS tracking_id
705   FROM {$tracking_table} e
706   WHERE e.date_created < %s";
⋮
709   $query = $wpdb->prepare( $query, $date_created );
⋮
713   }
⋮
757   }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT e.tracking_id AS tracking_id FROM self e WHERE e.date_created < %s
```

Issue #2184 - wordpress-popup/inc/hustle-tracking-model.php: 732

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 732
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 727 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_ip_from_tracking_id().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 732 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::get_ip_from_tracking_id(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
724  public static function get_ip_from_tracking_id( $tracking_id ){
725  global $wpdb;
726  $tracking_table = Hustle_Db::tracking_table();
727  $query = "SELECT e.ip AS ip
728  FROM {$tracking_table} e
729  WHERE e.tracking_id < %s";
⋮
732  $query = $wpdb->prepare( $query, $tracking_id );
⋮
736  }
⋮
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT e.ip AS ip FROM self e WHERE e.tracking_id < %s
```

Issue #2185 - wordpress-popup/inc/hustle-tracking-model.php: 751

Path: wordpress-popup/inc/hustle-tracking-model.php
Line: 751
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 752 of the file wordpress-popup/inc/hustle-tracking-model.php in the method Hustle_Tracking_Model::anonymise_tracked_id().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 751 of the file wordpress-popup/inc/hustle-tracking-model.php in the method

Hustle_Tracking_Model::anonymise_tracked_id(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-tracking-model.php

```
9    class Hustle_Tracking_Model {
⋮
748  public static function anonymise_tracked_id( $tracking_id, $ip ){
749  global $wpdb;
750  $tracking_table = Hustle_Db::tracking_table();
751  $wpdb->query( $wpdb->prepare(
752  "UPDATE {$tracking_table} SET `ip` = %s WHERE `tracking_id` = %d",
753  $ip,
754  $tracking_id
755  ));
756  }
757  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
UPDATE self SET `ip` = %s WHERE `tracking_id` = %d
```

Issue #2186 - wordpress-popup/inc/hustle-deletion.php: 18

Path: wordpress-popup/inc/hustle-deletion.php
Line: 18
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 18 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_reset_notifications().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 18 of the file wordpress-popup/inc/hustle-deletion.php in the method Hustle_Deletion::hustle_reset_notifications(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-deletion.php

```
8    class Hustle_Deletion {
⋮
15   public static function hustle_reset_notifications() {
16   global $wpdb;
⋮
18   $wpdb->query( "DELETE FROM {$wpdb->usermeta} WHERE `meta_key` = 'hustle_dismissed_notifications'" );
19   }
⋮
228  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
DELETE FROM WHERE `meta_key` = 'hustle_dismissed_notifications'
```

Issue #2196 - wordpress-popup/inc/hustle-entry-model.php: 791

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 791
Sink: get_var
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 789 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::get_total_entries_count().

The user-supplied data is then used unsanitized in the sensitive operation get_var() in line 791 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::get_total_entries_count(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
784   public static function get_total_entries_count() {
⋮
786   global $wpdb;
787   $table_name = Hustle_Db::entries_table();
⋮
789   $sql = "SELECT COUNT(`entry_id`) FROM {$table_name}";
⋮
791   return $wpdb->get_var( $sql );
792   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT COUNT(`entry_id`) FROM self
```

Issue #2199 - wordpress-popup/inc/hustle-entry-model.php: 825

Path: wordpress-popup/inc/hustle-entry-model.php
Line: 825
Sink: execute
Taint: HTTP

Code Summary

User-supplied data is concatenated into sql markup in line 824 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::get_latest_entry().

The user-supplied data is then used unsanitized in the sensitive operation execute() in line 825 of the file wordpress-popup/inc/hustle-entry-model.php in the method Hustle_Entry_Model::get_latest_entry(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-entry-model.php

```
9     class Hustle_Entry_Model {
⋮
```

```
813   public static function get_latest_entry( $entry_type = 'popup' ) {
⋮
822   $table_name = Hustle_Db::entries_table();
⋮
824   $sql = "SELECT `entry_id` FROM {$table_name} WHERE `entry_type` = %s ORDER BY `date_created` DESC";
825   $sql = $wpdb->prepare( $sql, $entry_type ); // WPCS: unprepared SQL ok. false positive
⋮
836   }
⋮
1130  }
```

SQL Context

The following snippet(s) do not represent actual code but the tainted context.

```
SELECT `entry_id` FROM self WHERE `entry_type` = %s ORDER BY `date_created` DESC
```

3.8. Missing Error Handling

CWE: 390
Severity: Low

The application checks for an error, but no error handling code is present.

All errors should be handled by the application to avoid undefined states, crashes, or exposure of sensitive information.

Issue #2175 - wordpress-popup/inc/provider/hustle-provider-form-hooks-abstract.php: 136

Path: wordpress-popup/inc/provider/hustle-provider-form-hooks-abstract.php
Line: 136
Sink: if
Taint: HTTP

Code Summary

A code quality issue was detected in line 136 of the file wordpress-popup/inc/provider/hustle-provider-form-hooks-abstract.php in the method Hustle_Provider_Form_Hooks_Abstract::on_form_submit(). Please refer to the context and description for further information.

wordpress-popup/inc/provider/hustle-provider-form-hooks-abstract.php

```
16   abstract class Hustle_Provider_Form_Hooks_Abstract {
⋮
101  public function on_form_submit( $submitted_data, $allow_subscribed ) {
⋮
136  if( ! $allow_subscribed ){ //phpcs:ignore
137  /**
138  * Use your provider validation to check
139  * for duplicate entries and put a stop here.
140  * You can add a message on the`$is_success`
141  * variable to display your own custom message
142  */
143  }
⋮
181  }
⋮
513  }
```

Code Context

The following snippet(s) do not represent actual code but the tainted context.

```
Empty conditional block.
```

3.9. Missing Default Case

CWE: 478
Severity: Low

The switch statement has no default case. This can lead to logical errors when the defined cases do not handle all possibilities. Thus, further code can lead to errors or vulnerabilities.

Each switch statement should have a default case to handle the situation where no case was matched.

Issue #2102 - wordpress-popup/lib/wpmu-lib/inc/class-thelib-html.php: 1507

Path: wordpress-popup/lib/wpmu-lib/inc/class-thelib-html.php
Line: 1507
Sink: switch
Taint: HTTP

Code Summary

A code quality issue was detected in line 1507 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-html.php in the method TheLib_Html::select_options(). Please refer to the context and description for further information.

wordpress-popup/lib/wpmu-lib/inc/class-thelib-html.php

```
8     class TheLib_Html extends TheLib {
⋮
1481  private function select_options( $list, $value = '', $type = 'default' ) {
⋮
1507  switch ( $type ) {
1508  case 'default':
1509  $attr .= selected( $is_selected, true, false );
1510  $options .= sprintf(
1511  '<option value="%1$s" %2$s>%3$s</option>',
1512  esc_attr( $key ),
1513  $attr,
1514  $option
1515  );
1516  break;
⋮
1518  case 'taglist':
1519  $attr .= ($is_selected ? 'disabled="disabled"' : '');
1520  $options .= sprintf(
1521  '<option value="%1$s" %2$s>%3$s</option>',
1522  esc_attr( $key ),
1523  $attr,
1524  $option
1525  );
1526  break;
1527  }
⋮
1532  }
```

```
⋮
1756 }
```

Code Context

The following snippet(s) do not represent actual code but the tainted context.

```
Missing default block in switch.
```

Issue #2103 - wordpress-popup/lib/wpmu-lib/inc/class-thelib-html.php: 521

Path: wordpress-popup/lib/wpmu-lib/inc/class-thelib-html.php
Line: 521
Sink: switch
Taint: HTTP

Code Summary

A code quality issue was detected in line 521 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-html.php in the method TheLib_Html::element(). Please refer to the context and description for further information.

wordpress-popup/lib/wpmu-lib/inc/class-thelib-html.php

```
8     class TheLib_Html extends TheLib {
⋮
380   public function element( $field_args, $return = false ) {
⋮
521   switch ( $type ) {
522   case self::INPUT_TYPE_HIDDEN:
523   $this->element_hidden(
524   $id,
525   $name,
526   $value,
527   $class
528   );
529   break;
⋮
531   case self::INPUT_TYPE_TEXT:
532   case self::INPUT_TYPE_PASSWORD:
533   case self::INPUT_TYPE_NUMBER:
534   case self::INPUT_TYPE_EMAIL:
535   case self::INPUT_TYPE_URL:
536   case self::INPUT_TYPE_TIME:
537   case self::INPUT_TYPE_SEARCH:
538   case self::INPUT_TYPE_FILE:
539   $this->element_input(
540   $labels,
541   $type,
542   $class,
543   $id,
544   $name,
545   $value,
546   $read_only . $max_attr . $attr_placeholder . $ajax_data . $data_attr . $disabled,
547   $wrapper_class
548   );
549   break;
⋮
551   case self::INPUT_TYPE_DATEPICKER:
552   $this->element_datepicker(
553   $labels,
554   $class,
```

```
555     $id,
556     $name,
557     $value,
558     $max_attr . $attr_placeholder . $ajax_data . $data_attr . $disabled,
559     $wrapper_class
560     );
561     break;
⋮
563     case self::INPUT_TYPE_TEXT_AREA:
564     $this->element_textarea(
565     $labels,
566     $class,
567     $id,
568     $name,
569     $value,
570     $read_only . $attr_placeholder . $ajax_data . $data_attr . $disabled,
571     $wrapper_class
572     );
573     break;
⋮
575     case self::INPUT_TYPE_SELECT:
576     $this->element_select(
577     $labels,
578     $class,
579     $id,
580     $name,
581     $value,
582     $multiple . $read_only . $attr_data_placeholder . $ajax_data . $data_attr . $disabled,
583     $field_options,
584     $wrapper_class
585     );
586     break;
⋮
588     case self::INPUT_TYPE_RADIO:
589     $this->element_radio(
590     $labels,
591     $class,
592     $id,
593     $name,
594     $value,
595     $ajax_data,
596     $field_options,
597     $wrapper_class
598     );
599     break;
⋮
601     case self::INPUT_TYPE_CHECKBOX:
602     $this->element_checkbox(
603     $labels,
604     $class,
605     $id,
606     $name,
607     $value,
608     $ajax_data . $data_attr . $disabled,
609     $field_options,
610     $config
611     );
612     break;
⋮
614     case self::INPUT_TYPE_WP_EDITOR:
615     $this->element_wp_editor(
616     $labels,
617     $id? $id:$name,
618     $value,
619     $field_options
```

```
620     );
621     break;
⋮
623     case self::INPUT_TYPE_BUTTON:
624     case self::INPUT_TYPE_SUBMIT:
625     if ( empty( $button_type ) ) {
626     $button_type = $type;
627     }
⋮
629     if ( $button_type === self::INPUT_TYPE_SUBMIT ) {
630     $class .= ' wpmui-submit button-primary';
631     }
⋮
633     $this->element_button(
634     $labels,
635     $type,
636     $class,
637     $id,
638     $name,
639     $value,
640     $button_value,
641     $ajax_data . $data_attr . $disabled
642     );
643     break;
⋮
645     case self::INPUT_TYPE_IMAGE:
646     $this->element_image(
647     $labels,
648     $class,
649     $id,
650     $name,
651     $value,
652     $alt,
653     $ajax_data . $data_attr . $disabled
654     );
655     break;
⋮
657     case self::INPUT_TYPE_RADIO_SLIDER:
658     $this->element_radioslider(
659     $labels,
660     $class,
661     $id,
662     $name,
663     $value,
664     $url,
665     $read_only,
666     $ajax_data . $data_attr,
667     $field_options,
668     $wrapper_class
669     );
670     break;
⋮
672     case self::INPUT_TYPE_TAG_SELECT:
673     $this->element_tagselect(
674     $labels,
675     $class,
676     $id,
677     $name,
678     $value,
679     $field_options,
680     $multiple . $read_only . $attr_data_placeholder . $data_attr . $disabled,
681     $ajax_data,
682     $empty_text,
683     $button_text,
```

```
684 $title_selected,
685 $wrapper_class
686 );
687 break;
⋮
689 case self::INPUT_TYPE_WP_PAGES:
690 $this->element_wp_pages(
691 $labels,
692 $class,
693 $id,
694 $name,
695 $value,
696 $multiple . $read_only . $attr_data_placeholder . $ajax_data . $data_attr . $disabled,
697 $field_options,
698 $wrapper_class
699 );
700 break;
⋮
702 case self::TYPE_HTML_LINK:
703 $this->element_link(
704 $labels,
705 $class,
706 $id,
707 $value,
708 $url,
709 $ajax_data . $data_attr,
710 $target
711 );
712 break;
⋮
714 case self::TYPE_HTML_SEPARATOR:
715 $this->element_separator(
716 ($value !== 'vertical' ? 'horizontal' : 'vertical')
717 );
718 break;
⋮
720 case self::TYPE_HTML_TEXT:
721 $this->element_wrapper(
722 $labels,
723 $class,
724 $id,
725 $value,
726 'span',
727 $wrapper_class
728 );
729 break;
⋮
731 case self::TYPE_HTML_TABLE:
732 $this->element_table(
733 $labels,
734 $class,
735 $id,
736 $value,
737 $field_options,
738 $wrapper_class
739 );
740 break;
⋮
742 /**
743 * wp-color-picker
744 *
745 * @since 3.0.5
746 */
747 case self::INPUT_TYPE_WP_COLOR_PICKER:
748 $this->element_color_picker(
```

```
749   $labels,
750   $class,
751   $id,
752   $name,
753   $value,
754   $max_attr . $attr_placeholder . $ajax_data . $data_attr . $disabled,
755   $wrapper_class
756   );
757   break;
⋮
759   /**
760   * wp_media
761   *
762   * @since 3.0.5
763   */
764   case self::INPUT_TYPE_WP_MEDIA:
765   $this->element_wp_media(
766   $labels,
767   $class,
768   $id,
769   $name,
770   $value,
771   $max_attr . $attr_placeholder . $ajax_data . $data_attr,
772   $wrapper_class
773   );
774   break;
⋮
776   }
⋮
780   }
⋮
1756  }
```

Code Context

The following snippet(s) do not represent actual code but the tainted context.

```
Missing default block in switch.
```

Issue #2194 - wordpress-popup/views/admin/commons/pagination.php: 44

Path: wordpress-popup/views/admin/commons/pagination.php
Line: 44
Sink: switch
Taint: HTTP

Code Summary

A code quality issue was detected in line 44 of the file wordpress-popup/views/admin/commons/pagination.php in the function hustle_pagination_one(). Please refer to the context and description for further information.

wordpress-popup/views/admin/commons/pagination.php

```
41  function hustle_pagination_one( $url, $content = '', $enabled = true, $class = '' ) {
⋮
44  switch ( $content ) {
⋮
46  case 'sui-icon-arrow-skip-end' :
47  case 'sui-icon-arrow-skip-start' :
48  case 'sui-icon-chevron-left' :
```

```
49  case 'sui-icon-chevron-right' :
50  $content = sprintf(
51  '<i class="%s" aria-hidden="true"></i>',
52  $content
53  );
54  break;
55  }
⋮
64  }
```

Code Context

The following snippet(s) do not represent actual code but the tainted context.

```
Missing default block in switch.
```

Issue #2255 - wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-settings.php: 665

Path:	wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-settings.php
Line:	665
Sink:	switch
Taint:	HTTP

Code Summary

A code quality issue was detected in line 665 of the file wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-settings.php in the method Hustle_Mailchimp_Form_Settings::get_group_interest_options(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-settings.php

```
9     class Hustle_Mailchimp_Form_Settings extends Hustle_Provider_Form_Settings_Abstract {
⋮
645   private function get_group_interest_options( $_type, $interests, $interest_id, $placeholder = '' ) {
⋮
665   switch ( $_type ) {
⋮
667   case 'dropdown' :
668   $field_type = 'select';
669   $class = 'sui-select';
670   break;
⋮
672   case 'checkboxes' :
673   $choose_prompt = __( 'Default Interest(s)', 'wordpress-popup' );
674   $input_name = 'group_interest[]';
675   $class = 'sui-checkbox-sm sui-checkbox-stacked';
676   break;
⋮
678   case 'radio' :
679   $field_type = 'radios';
680   $class = 'sui-radio-sm sui-radio-stacked';
681   $choose_prompt = sprintf(
682   __( 'Default Interest %1$s(clear selection)%2$s', 'wordpress-popup' ),
683   '<a href="#" class="hustle-provider-clear-radio-options" style="margin-left: 5px;" data-name="group_interest"
      >',
684   '</a>'
685   );
686   break;
⋮
```

```
688 case 'hidden' :
689 $class = 'sui-select';
690 $choose_prompt = __( 'Default Interest', 'wordpress-popup' );
691 break;
692 }
⋮
744 }
⋮
831 } // Class end.
```

Code Context

The following snippet(s) do not represent actual code but the tainted context.

```
Missing default block in switch.
```

Issue #2280 - wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php: 456

Path: wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php
Line: 456
Sink: switch
Taint: HTTP

Code Summary

A code quality issue was detected in line 456 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php in the method TheLib_Debug::_dump_var(). Please refer to the context and description for further information.

wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php

```
8   class TheLib_Debug extends TheLib {
⋮
441 protected function _dump_var( $data, $item_key = null, $default_depth = 3, $level = array( null ), $args = array
    () ) {
⋮
456 switch ( $type ) {
457 case 'String':
458 $type_length = strlen( $data );
459 $type_data = '"' . htmlentities( $data ) . '"';
460 break;
⋮
462 case 'Double':
463 case 'Float':
464 $type = 'Float';
465 $type_length = strlen( $data );
466 $type_data = htmlentities( $data );
467 break;
⋮
469 case 'Integer':
470 $type_length = strlen( $data );
471 $type_data = htmlentities( $data );
472 break;
⋮
474 case 'Boolean':
475 $type_length = strlen( $data );
476 $type_data = $data ? 'TRUE' : 'FALSE';
477 break;
⋮
479 case 'NULL':
480 $type_length = 0;
```

```
481  $type_data = 'NULL';
482  break;
⋮
484  case 'Array':
485  $type_length = count( $data );
486  break;
⋮
488  case 'Object':
489  $full_dump = true;
490  break;
491  }
⋮
585  }
⋮
964  }
```

Code Context

The following snippet(s) do not represent actual code but the tainted context.

```
Missing default block in switch.
```

3.10. Weak Hash Function

OWASP Top 10:	
CWE:	328
Severity:	Low

The code uses a hash function that is cryptographically insecure. An attacker may be able to craft different values that produce the same hash, or to find preimages for some or all values in the output space of the hash function. This can be dangerous if the hash function is used in a security context, e.g., for authentication purposes.

A secure hash algorithm should be used. The availability of algorithms depends on the used PHP version. Secure hash algorithms that may be available include SHA-256, SHA-384, and SHA-512, all of which belong to the SHA-2 family of hash functions, as well as SHA3-224, SHA3-256, SHA3-384, and SHA3-512, which belong to the SHA-3 family of hash functions.

Issue #2101 - wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-api.php: 80

Path:	wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-api.php
Line:	80
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 80 of the file wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-api.php in the method Hustle_SendinBlue_Api::boot(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-api.php

```
12  class Hustle_SendinBlue_Api {
⋮
78  public static function boot( $api_key ) {
⋮
80  $instance_key = md5( $api_key );
```

```
⋮
87    }
⋮
387   }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-api.php

```
80  $instance_key = hash('sha3-256', $api_key);
```

Issue #2117 - wordpress-popup/inc/hustle-migration.php: 922

Path: wordpress-popup/inc/hustle-migration.php
Line: 922
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 922 of the file wordpress-popup/inc/hustle-migration.php in the method Hustle_Migration::parse_visibility_meta(). Please refer to the context and description for further information.

wordpress-popup/inc/hustle-migration.php

```
8       class Hustle_Migration {
⋮
914     private function parse_visibility_meta( $module, $old_module ) {
⋮
922     $group_id = substr( md5( wp_rand() ), 0, 10 );
⋮
1032    }
⋮
1534    }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/hustle-migration.php

```
922  $group_id = substr( hash('sha3-256', wp_rand()), 0, 10 );
```

Issue #2213 - wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php: 289

Path:	wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php
Line:	289
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 289 of the file wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php in the method Hustle_ActiveCampaign_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php

```
9     class Hustle_ActiveCampaign_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
288   protected function get_subscriber( $api, $data ) {
289   if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data['email'] ) ] ) ){
⋮
294   }
⋮
317   }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php

```
289   if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data['email']) ] ) ){
```

Issue #2214 - wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php: 290

Path:	wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php
Line:	290
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 290 of the file wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php in the method Hustle_ActiveCampaign_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php

```
9    class Hustle_ActiveCampaign_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
288  protected function get_subscriber( $api, $data ) {
⋮
290  $this->_subscriber[ md5( $data['email'] ) ] = $api->email_exist( $data['email'], $data['list'] );
⋮
294  }
⋮
317  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php

```
290  $this->_subscriber[ hash('sha3-256', $data['email']) ] = $api->email_exist( $data['email'], $data['list'] );
```

Issue #2215 - wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php: 293

Path:	wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php
Line:	293
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 293 of the file wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php in the method Hustle_ActiveCampaign_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php

```
9    class Hustle_ActiveCampaign_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
288  protected function get_subscriber( $api, $data ) {
⋮
293  return $this->_subscriber[ md5( $data['email'] ) ];
294  }
⋮
317  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/activecampaign/hustle-activecampaign-form-hooks.php

```
293 return $this->_subscriber[ hash('sha3-256', $data['email']) ];
```

Issue #2216 - wordpress-popup/inc/providers/aweber/lib/class-aweber-oauth.php: 155

Path: wordpress-popup/inc/providers/aweber/lib/class-aweber-oauth.php
Line: 155
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 155 of the file wordpress-popup/inc/providers/aweber/lib/class-aweber-oauth.php in the method Hustle_Addon_Aweber_Oauth::generate_oauth_nonce(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/aweber/lib/class-aweber-oauth.php

```
7   class Hustle_Addon_Aweber_Oauth {
⋮
150 public static function generate_oauth_nonce( $timestamp = 0 ) {
⋮
155 $oauth_nonce = md5( $timestamp . '-' . wp_rand( 10000, 99999 ) . '-' . uniqid() );
⋮
169 }
170 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/aweber/lib/class-aweber-oauth.php

```
155 $oauth_nonce = hash('sha3-256', $timestamp . '-' . wp_rand(10000, 99999) . '-' . uniqid());
```

Issue #2217 - wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php: 354

Path: wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php
Line: 354
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 354 of the file wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php in the method

Hustle_Aweber_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php

```
9    class Hustle_Aweber_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
353  protected function get_subscriber( $api, $data ) {
354  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data['email'] ) ] ) ){
⋮
358  }
⋮
360  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php

```
354  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data['email']) ] ) ){
```

Issue #2218 - wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php: 355

Path:	wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php
Line:	355
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 355 of the file wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php in the method Hustle_Aweber_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php

```
9    class Hustle_Aweber_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
353  protected function get_subscriber( $api, $data ) {
⋮
355  $this->_subscriber[ md5( $data['email'] ) ] = $api->find_account_list_subscriber( $data['account_id'], $data['list
     _id'], array( 'email' => $data['email'] ) );
⋮
358  }
⋮
360  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php

```
355 $this->_subscriber[ hash('sha3-256', $data['email']) ] = $api->find_account_list_subscriber( $data['account_id'],
    $data['list_id'], array( 'email' => $data['email'] ) );
```

Issue #2219 - wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php: 357

Path: wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php
Line: 357
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 357 of the file wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php in the method Hustle_Aweber_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php

```
9   class Hustle_Aweber_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
353 protected function get_subscriber( $api, $data ) {
⋮
357 return $this->_subscriber[ md5( $data['email'] ) ];
358 }
⋮
360 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/aweber/hustle-aweber-form-hooks.php

```
357 return $this->_subscriber[ hash('sha3-256', $data['email']) ];
```

Issue #2220 - wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php: 68

Path: wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php
Line: 68
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 68 of the file wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php in the method Hustle_Campaignmonitor_API::boot(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php

```
6    class Hustle_Campaignmonitor_API {
⋮
67   public static function boot( $api_key ) {
68   if ( ! isset( self::$_instances[ md5( $api_key ) ] ) ) {
⋮
73   }
⋮
524  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php

```
68 if ( ! isset( self::$_instances[ hash('sha3-256', $api_key) ] ) ) {
```

Issue #2221 - wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php: 69

Path:	wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php
Line:	69
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 69 of the file wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php in the method Hustle_Campaignmonitor_API::boot(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php

```
6    class Hustle_Campaignmonitor_API {
⋮
67   public static function boot( $api_key ) {
⋮
69   self::$_instances[ md5( $api_key ) ] = new static( $api_key );
⋮
73   }
⋮
524  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php

```
69  self::$_instances[ hash('sha3-256', $api_key) ] = new static( $api_key );
```

Issue #2222 - wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php: 72

Path:	wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php
Line:	72
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 72 of the file wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php in the method Hustle_Campaignmonitor_API::boot(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php

```
6     class Hustle_Campaignmonitor_API {
⋮
67    public static function boot( $api_key ) {
⋮
72    return self::$_instances[ md5( $api_key ) ];
73    }
⋮
524   }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-api.php

```
72  return self::$_instances[ hash('sha3-256', $api_key) ];
```

Issue #2223 - wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php: 277

Path:	wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php
Line:	277
Sink:	md5

Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 277 of the file wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php in the method Hustle_Campaignmonitor_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php

```
9    class Hustle_Campaignmonitor_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
276  protected function get_subscriber( $api, $data ) {
277  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data['email'] ) ] ) ){
⋮
282  }
⋮
284  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php

```
277  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data['email']) ] ) ){
```

Issue #2224 - wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php: 278

Path: wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php
Line: 278
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 278 of the file wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php in the method Hustle_Campaignmonitor_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php

```
9    class Hustle_Campaignmonitor_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
276  protected function get_subscriber( $api, $data ) {
⋮
278  $this->_subscriber[ md5( $data['email'] ) ] = $api->get_subscriber( $data['list'], $data['email'] );
```

```
⋮
282 }
⋮
284 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php

```
278 $this->_subscriber[ hash('sha3-256', $data['email']) ] = $api->get_subscriber( $data['list'], $data['email'] );
```

Issue #2225 - wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php: 281

Path:	wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php
Line:	281
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 281 of the file wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php in the method Hustle_Campaignmonitor_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php

```
9   class Hustle_Campaignmonitor_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
276 protected function get_subscriber( $api, $data ) {
⋮
281 return $this->_subscriber[ md5( $data['email'] ) ];
282 }
⋮
284 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/campaignmonitor/hustle-campaignmonitor-form-hooks.php

```
281 return $this->_subscriber[ hash('sha3-256', $data['email']) ];
```

Issue #2226 - wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php: 258

Path:	wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php
Line:	258
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 258 of the file wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php in the method Hustle_ConstantContact_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php

```
9   class Hustle_ConstantContact_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
257 protected function get_subscriber( $api, $data ) {
258 if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data['email'] ) ] ) ){
⋮
263 }
⋮
265 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php

```
258 if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data['email']) ] ) ){
```

Issue #2227 - wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php: 260

Path:	wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php
Line:	260
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 260 of the file wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php in the method Hustle_ConstantContact_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php

```
9    class Hustle_ConstantContact_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
257  protected function get_subscriber( $api, $data ) {
⋮
260  $this->_subscriber[ md5( $data['email'] ) ] = $api->contact_exist( $existing_contact, $data['list_id'] );
⋮
263  }
⋮
265  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php

```
260  $this->_subscriber[ hash('sha3-256', $data['email']) ] = $api->contact_exist( $existing_contact, $data['list_id'] );
```

Issue #2228 - wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php: 262

Path:	wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php
Line:	262
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 262 of the file wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php in the method Hustle_ConstantContact_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php

```
9    class Hustle_ConstantContact_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
257  protected function get_subscriber( $api, $data ) {
⋮
262  return $this->_subscriber[ md5( $data['email'] ) ];
263  }
⋮
265  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/constantcontact/hustle-constantcontact-form-hooks.php

```
262 return $this->_subscriber[ hash('sha3-256', $data['email']) ];
```

Issue #2229 - wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php: 299

Path: wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php
Line: 299
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 299 of the file wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php in the method Hustle_ConvertKit_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php

```
9   class Hustle_ConvertKit_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
298 protected function get_subscriber( $api, $data ) {
299 if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data['email'] ) ] ) ){
⋮
303 }
304 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php

```
299 if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data['email']) ] ) ){
```

Issue #2230 - wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php: 300

Path: wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php
Line: 300

Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 300 of the file wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php in the method Hustle_ConvertKit_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php

```
9    class Hustle_ConvertKit_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
298  protected function get_subscriber( $api, $data ) {
⋮
300  $this->_subscriber[ md5( $data['email'] ) ] = $api->is_form_subscriber( $data['email'], $data['list_id'] );
⋮
303  }
304  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php

```
300  $this->_subscriber[ hash('sha3-256', $data['email']) ] = $api->is_form_subscriber( $data['email'], $data['list_id'] );
```

Issue #2231 - wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php: 302

Path: wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php
Line: 302
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 302 of the file wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php in the method Hustle_ConvertKit_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php

```
9    class Hustle_ConvertKit_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
298  protected function get_subscriber( $api, $data ) {
⋮
302  return $this->_subscriber[ md5( $data['email'] ) ];
303  }
304  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/convertkit/hustle-convertkit-form-hooks.php

```
302 return $this->_subscriber[ hash('sha3-256', $data['email']) ];
```

Issue #2232 - wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php: 250

Path: wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php
Line: 250
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 250 of the file wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php in the method Hustle_E_Newsletter_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php

```
9   class Hustle_E_Newsletter_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
249 protected function get_subscriber( $api, $data ) {
250 if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data ) ] ) ){
⋮
254 }
⋮
256 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php

```
250 if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data) ] ) ){
```

Issue #2233 - wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php: 251

Path: wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php
Line: 251

Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 251 of the file wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php in the method Hustle_E_Newsletter_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php

```
9    class Hustle_E_Newsletter_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
249  protected function get_subscriber( $api, $data ) {
⋮
251  $this->_subscriber[ md5( $data ) ] = $api->is_member( $data ) ;
⋮
254  }
⋮
256  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php

```
251  $this->_subscriber[ hash('sha3-256', $data) ] = $api->is_member( $data ) ;
```

Issue #2234 - wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php: 253

Path: wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php
Line: 253
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 253 of the file wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php in the method Hustle_E_Newsletter_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php

```
9    class Hustle_E_Newsletter_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
249  protected function get_subscriber( $api, $data ) {
⋮
253  return $this->_subscriber[ md5( $data ) ];
254  }
```

```
⋮
256 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/e_newsletter/hustle-e-newsletter-form-hooks.php

```
253 return $this->_subscriber[ hash('sha3-256', $data) ];
```

Issue #2235 - wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php: 294

Path: wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php
Line: 294
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 294 of the file wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php in the method Hustle_Get_Response_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php

```
9   class Hustle_Get_Response_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
293 protected function get_subscriber( $api, $data ) {
294 if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data ) ] ) ){
⋮
298 }
299 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php

```
294 if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data) ] ) ){
```

Issue #2236 - wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php: 295

Path: wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php
Line: 295
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 295 of the file wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php in the method Hustle_Get_Response_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php

```
9    class Hustle_Get_Response_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
293  protected function get_subscriber( $api, $data ) {
⋮
295  $this->_subscriber[ md5( $data ) ] = $api->get_contact( $data );
⋮
298  }
299  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php

```
295  $this->_subscriber[ hash('sha3-256', $data) ] = $api->get_contact( $data );
```

Issue #2237 - wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php: 297

Path: wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php
Line: 297
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 297 of the file wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php in the method Hustle_Get_Response_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php

```
9    class Hustle_Get_Response_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
293  protected function get_subscriber( $api, $data ) {
⋮
297  return $this->_subscriber[ md5( $data ) ];
```

```
298 }
299 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/getresponse/hustle-get-response-form-hooks.php

```
297 return $this->_subscriber[ hash('sha3-256', $data) ];
```

Issue #2238 - wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php: 295

Path: wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php
Line: 295
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 295 of the file wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php in the method Hustle_HubSpot_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php

```
9   class Hustle_HubSpot_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
293 protected function get_subscriber( $api, $data ){
⋮
295 if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data ) ] ) ){
⋮
300 }
⋮
302 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php

```
295 if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data) ] ) ){
```

Issue #2239 - wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php: 296

Path: wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php
Line: 296
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 296 of the file wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php in the method Hustle_HubSpot_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php

```
9    class Hustle_HubSpot_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
293  protected function get_subscriber( $api, $data ){
⋮
296  $this->_subscriber[ md5( $data ) ] = $api->email_exists( $data );
⋮
300  }
⋮
302  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php

```
296  $this->_subscriber[ hash('sha3-256', $data) ] = $api->email_exists( $data );
```

Issue #2240 - wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php: 299

Path: wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php
Line: 299
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 299 of the file wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php in the method Hustle_HubSpot_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php

```
9    class Hustle_HubSpot_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
293  protected function get_subscriber( $api, $data ){
⋮
```

```
299 return $this->_subscriber[ md5( $data ) ];
300 }
⋮
302 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/hubspot/hustle-hubspot-form-hooks.php

```
299 return $this->_subscriber[ hash('sha3-256', $data) ];
```

Issue #2241 - wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php: 314

Path: wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php
Line: 314
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 314 of the file wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php in the method Hustle_Icontact_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php

```
9   class Hustle_Icontact_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
312 protected function get_subscriber( $api, $data ){
⋮
314 if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data['email'] ) ] ) ){
⋮
319 }
320 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php

```
314 if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data['email']) ] ) ){
```

Issue #2242 - wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php: 315

Path: wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php
Line: 315
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 315 of the file wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php in the method Hustle_Icontact_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php

```
9    class Hustle_Icontact_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
312  protected function get_subscriber( $api, $data ){
⋮
315  $this->_subscriber[ md5( $data['email'] ) ] = $api->_is_subscribed( $data['api'], $data['list_id'], $data['email'] );
⋮
319  }
320  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php

```
315  $this->_subscriber[ hash('sha3-256', $data['email']) ] = $api->_is_subscribed( $data['api'], $data['list_id'], $data
     ['email'] );
```

Issue #2243 - wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php: 318

Path: wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php
Line: 318
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 318 of the file wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php in the method Hustle_Icontact_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php

```
9    class Hustle_Icontact_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
312  protected function get_subscriber( $api, $data ){
⋮
318  return $this->_subscriber[ md5( $data['email'] ) ];
319  }
320  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/icontact/hustle-icontact-form-hooks.php

```
318  return $this->_subscriber[ hash('sha3-256', $data['email']) ];
```

Issue #2244 - wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php: 323

Path:	wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php
Line:	323
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 323 of the file wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php in the method Hustle_InfusionSoft_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php

```
9    class Hustle_InfusionSoft_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
321  protected function get_subscriber( $api, $data ){
⋮
323  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data ) ] ) ){
⋮
328  }
329  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php

```
323 if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data) ] ) ){
```

Issue #2245 - wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php: 324

Path: wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php
Line: 324
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 324 of the file wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php in the method Hustle_InfusionSoft_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php

```
9   class Hustle_InfusionSoft_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
321 protected function get_subscriber( $api, $data ){
⋮
324 $this->_subscriber[ md5( $data ) ] = $api->email_exist( $data );
⋮
328 }
329 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php

```
324 $this->_subscriber[ hash('sha3-256', $data) ] = $api->email_exist( $data );
```

Issue #2246 - wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php: 327

Path: wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php
Line: 327
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 327 of the file wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php in the method Hustle_InfusionSoft_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php

```
9    class Hustle_InfusionSoft_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
321  protected function get_subscriber( $api, $data ){
⋮
327  return $this->_subscriber[ md5( $data ) ];
328  }
329  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/infusionsoft/hustle-infusion-soft-form-hooks.php

```
327  return $this->_subscriber[ hash('sha3-256', $data) ];
```

Issue #2247 - wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-api.php: 76

Path: wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-api.php
Line: 76
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 76 of the file wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-api.php in the method Hustle_Mad_Mimi_Api::boot(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-api.php

```
7    class Hustle_Mad_Mimi_Api {
⋮
74   public static function boot( $user_name, $api_key ) {
⋮
76   $instance_key = md5( $api_key );
⋮
83   }
⋮
341  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-api.php

```
76  $instance_key = hash('sha3-256', $api_key);
```

Issue #2248 - wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php: 304

Path: wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php
Line: 304
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 304 of the file wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php in the method Hustle_Mad_Mimi_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php

```
9    class Hustle_Mad_Mimi_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
303  protected function get_subscriber( $api, $data ) {
304  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data ) ] ) ){
⋮
309  }
310  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php

```
304  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data) ] ) ){
```

Issue #2249 - wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php: 305

Path: wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php
Line: 305
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 305 of the file wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php in the method Hustle_Mad_Mimi_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php

```
9    class Hustle_Mad_Mimi_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
303  protected function get_subscriber( $api, $data ) {
⋮
305  $this->_subscriber[ md5( $data ) ] = $api->get_subscriber( array( 'query' => $data ) );
⋮
309  }
310  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php

```
305  $this->_subscriber[ hash('sha3-256', $data) ] = $api->get_subscriber( array( 'query' => $data ) );
```

Issue #2250 - wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php: 308

Path: wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php
Line: 308
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 308 of the file wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php in the method Hustle_Mad_Mimi_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php

```
9    class Hustle_Mad_Mimi_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
303  protected function get_subscriber( $api, $data ) {
⋮
308  return $this->_subscriber[ md5( $data ) ];
309  }
310  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/madmimi/hustle-mad-mimi-form-hooks.php

```
308  return $this->_subscriber[ hash('sha3-256', $data) ];
```

Issue #2251 - wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php: 212

Path: wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php
Line: 212
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 212 of the file wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php in the method Hustle_Mailchimp_Api::check_email(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php

```
7    class Hustle_Mailchimp_Api {
⋮
211  public function check_email( $list_id, $email ) {
212  $md5_email = md5( strtolower( $email ) );
⋮
216  }
⋮
341  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php

```
212  $md5_email = hash('sha3-256', strtolower($email));
```

Issue #2252 - wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php: 228

Path: wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php
Line: 228
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 228 of the file wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php in the method Hustle_Mailchimp_Api::delete_email(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php

```
7    class Hustle_Mailchimp_Api {
```

```
⋮
227 public function delete_email( $list_id, $email ) {
228 $md5_email = md5( strtolower( $email ) );
⋮
231 }
⋮
341 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php

```
228 $md5_email = hash('sha3-256', strtolower($email));
```

Issue #2253 - wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php: 328

Path: wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php
Line: 328
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 328 of the file wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php in the method Hustle_Mailchimp_Api::update_subscription_patch(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php

```
7   class Hustle_Mailchimp_Api {
⋮
327 public function update_subscription_patch( $list_id, $email, $data ) {
328 $md5_email = md5( strtolower( $email ) );
⋮

339 }
⋮
341 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php

```
328 $md5_email = hash('sha3-256', strtolower($email));
```

Issue #2254 - wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php: 303

Path: wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php
Line: 303
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 303 of the file wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php in the method Hustle_Mailchimp_Api::update_subscription(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php

```
7   class Hustle_Mailchimp_Api {
⋮
302 public function update_subscription( $list_id, $email, $data ) {
303 $md5_email = md5( strtolower( $email ) );
⋮
316 }
⋮
341 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-api.php

```
303 $md5_email = hash('sha3-256', strtolower($email));
```

Issue #2256 - wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php: 465

Path: wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php
Line: 465
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 465 of the file wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php in the method Hustle_Mailchimp_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php

```
9    class Hustle_Mailchimp_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
464  protected function get_subscriber( $api, $data ) {
465  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data['email'] ) ] ) ){
⋮
470  }
⋮
515  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php

```
465  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data['email']) ] ) ){
```

Issue #2257 - wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php: 466

Path: wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php
Line: 466
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 466 of the file wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php in the method Hustle_Mailchimp_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php

```
9    class Hustle_Mailchimp_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
464  protected function get_subscriber( $api, $data ) {
⋮
466  $this->_subscriber[ md5( $data['email'] ) ] = $api->check_email( $data['list_id'], $data['email'] );
⋮
470  }
⋮
515  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php

```
466 $this->_subscriber[ hash('sha3-256', $data['email']) ] = $api->check_email( $data['list_id'], $data['email'] );
```

Issue #2258 - wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php: 469

Path: wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php
Line: 469
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 469 of the file wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php in the method Hustle_Mailchimp_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php

```
9   class Hustle_Mailchimp_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
464 protected function get_subscriber( $api, $data ) {
⋮
469 return $this->_subscriber[ md5( $data['email'] ) ];
470 }
⋮
515 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mailchimp/hustle-mailchimp-form-hooks.php

```
469 return $this->_subscriber[ hash('sha3-256', $data['email']) ];
```

Issue #2259 - wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php: 287

Path: wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php
Line: 287
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 287 of the file wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php in the method Hustle_MailerLite_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php

```
9    class Hustle_MailerLite_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
286  protected function get_subscriber( $api, $data ) {
287  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data['email'] ) ] ) ){
⋮
292  }
⋮
294  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php

```
287  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data['email']) ] ) ){
```

Issue #2260 - wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php: 288

Path: wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php
Line: 288
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 288 of the file wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php in the method Hustle_MailerLite_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php

```
9    class Hustle_MailerLite_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
286  protected function get_subscriber( $api, $data ) {
⋮
288  $this->_subscriber[ md5( $data['email'] ) ] = $api->_email_exists( $data['list_id'], $data['email'], $data['api'] );
⋮
292  }
⋮
294  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php

```
288 $this->_subscriber[ hash('sha3-256', $data['email']) ] = $api->_email_exists( $data['list_id'], $data['email'], $dat
    a['api'] );
```

Issue #2261 - wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php: 291

Path: wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php
Line: 291
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 291 of the file wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php in the method Hustle_MailerLite_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php

```
9   class Hustle_MailerLite_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
286 protected function get_subscriber( $api, $data ) {
⋮
291 return $this->_subscriber[ md5( $data['email'] ) ];
292 }
⋮
294 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mailerlite/hustle-mailerlite-form-hooks.php

```
291 return $this->_subscriber[ hash('sha3-256', $data['email']) ];
```

Issue #2262 - wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php: 290

Path: wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php
Line: 290
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 290 of the file wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php in the method Hustle_Mautic_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php

```
9    class Hustle_Mautic_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
289  protected function get_subscriber( $api, $data ) {
290  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data ) ] ) ){
⋮
295  }
296  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php

```
290  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data) ] ) ){
```

Issue #2263 - wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php: 291

Path: wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php
Line: 291
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 291 of the file wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php in the method Hustle_Mautic_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php

```
9    class Hustle_Mautic_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
289  protected function get_subscriber( $api, $data ) {
⋮
291  $this->_subscriber[ md5( $data ) ] = $api->email_exist( $data );
⋮
295  }
296  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php

```
291 $this->_subscriber[ hash('sha3-256', $data) ] = $api->email_exist( $data );
```

Issue #2264 - wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php: 294

Path: wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php
Line: 294
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 294 of the file wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php in the method Hustle_Mautic_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php

```
9   class Hustle_Mautic_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
289 protected function get_subscriber( $api, $data ) {
⋮
294 return $this->_subscriber[ md5( $data ) ];
295 }
296 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mautic/hustle-mautic-form-hooks.php

```
294 return $this->_subscriber[ hash('sha3-256', $data) ];
```

Issue #2265 - wordpress-popup/inc/providers/mautic/hustle-mautic-api.php: 88

Path: wordpress-popup/inc/providers/mautic/hustle-mautic-api.php
Line: 88
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 88 of the file wordpress-popup/inc/providers/mautic/hustle-mautic-api.php in the method Hustle_Mautic_Api::get_instance(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mautic/hustle-mautic-api.php

```
11 class Hustle_Mautic_Api {
```

```
⋮
82  public static function get_instance( $base_url = '', $username, $password = '' ) {
⋮
88  if ( ! isset( self::$_instances[ md5( $username ) ] ) ) {
⋮
92  }
⋮
433 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mautic/hustle-mautic-api.php

```
88  if ( ! isset( self::$_instances[ hash('sha3-256', $username) ] ) ) {
```

Issue #2266 - wordpress-popup/inc/providers/mautic/hustle-mautic-api.php: 89

Path: wordpress-popup/inc/providers/mautic/hustle-mautic-api.php
Line: 89
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 89 of the file wordpress-popup/inc/providers/mautic/hustle-mautic-api.php in the method Hustle_Mautic_Api::get_instance(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mautic/hustle-mautic-api.php

```
11  class Hustle_Mautic_Api {
⋮
82  public static function get_instance( $base_url = '', $username, $password = '' ) {
⋮
89  self::$_instances[ md5( $username ) ] = new self( $base_url, $username, $password );
⋮
92  }
⋮
433 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mautic/hustle-mautic-api.php

```
89  self::$_instances[ hash('sha3-256', $username) ] = new self( $base_url, $username, $password );
```

Issue #2267 - wordpress-popup/inc/providers/mautic/hustle-mautic-api.php: 91

Path: wordpress-popup/inc/providers/mautic/hustle-mautic-api.php
Line: 91
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 91 of the file wordpress-popup/inc/providers/mautic/hustle-mautic-api.php in the method Hustle_Mautic_Api::get_instance(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/mautic/hustle-mautic-api.php

```
11  class Hustle_Mautic_Api {
⋮
82  public static function get_instance( $base_url = '', $username, $password = '' ) {
⋮
91  return self::$_instances[ md5( $username ) ];
92  }
⋮
433 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/mautic/hustle-mautic-api.php

```
91  return self::$_instances[ hash('sha3-256', $username) ];
```

Issue #2268 - wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php: 272

Path: wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php
Line: 272
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 272 of the file wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php in the method Hustle_Sendgrid_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php

```
9    class Hustle_Sendgrid_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
271  protected function get_subscriber( $api, $data ) {
272  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data['email'] ) ] ) ){
⋮
277  }
⋮
279  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php

```
272  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data['email']) ] ) ){
```

Issue #2269 - wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php: 273

Path:	wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php
Line:	273
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 273 of the file wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php in the method Hustle_Sendgrid_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php

```
9    class Hustle_Sendgrid_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
271  protected function get_subscriber( $api, $data ) {
⋮
273  $this->_subscriber[ md5( $data['email'] ) ] = $api->email_exists( $data['email'], $data['list_id'] );
⋮
277  }
⋮
279  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php

```
273 $this->_subscriber[ hash('sha3-256', $data['email']) ] = $api->email_exists( $data['email'], $data['list_id'] );
```

Issue #2270 - wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php: 276

Path: wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php
Line: 276
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 276 of the file wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php in the method Hustle_Sendgrid_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php

```
9   class Hustle_Sendgrid_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
271 protected function get_subscriber( $api, $data ) {
⋮
276 return $this->_subscriber[ md5( $data['email'] ) ];
277 }
⋮
279 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/sendgrid/hustle-sendgrid-form-hooks.php

```
276 return $this->_subscriber[ hash('sha3-256', $data['email']) ];
```

Issue #2271 - wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php: 297

Path: wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php
Line: 297
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 297 of the file wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php in the method Hustle_SendinBlue_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php

```
9    class Hustle_SendinBlue_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
296  protected function get_subscriber( $api, $data ) {
297  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ md5( $data ) ] ) ){
⋮
302  }
⋮
304  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php

```
297  if( empty ( $this->_subscriber ) && ! isset( $this->_subscriber[ hash('sha3-256', $data) ] ) ){
```

Issue #2272 - wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php: 298

Path: wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php
Line: 298
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 298 of the file wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php in the method Hustle_SendinBlue_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php

```
9    class Hustle_SendinBlue_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
296  protected function get_subscriber( $api, $data ) {
⋮
298  $this->_subscriber[ md5( $data ) ] = $api->get_contact( $data );
⋮
302  }
⋮
304  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php

```
298 $this->_subscriber[ hash('sha3-256', $data) ] = $api->get_contact( $data );
```

Issue #2273 - wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php: 301

Path: wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php
Line: 301
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 301 of the file wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php in the method Hustle_SendinBlue_Form_Hooks::get_subscriber(). Please refer to the context and description for further information.

wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php

```
9   class Hustle_SendinBlue_Form_Hooks extends Hustle_Provider_Form_Hooks_Abstract {
⋮
296 protected function get_subscriber( $api, $data ) {
⋮
301 return $this->_subscriber[ md5( $data ) ];
302 }
⋮
304 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/inc/providers/sendinblue/hustle-sendinblue-form-hooks.php

```
301 return $this->_subscriber[ hash('sha3-256', $data) ];
```

Issue #2277 - wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php: 333

Path: wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php
Line: 333
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 333 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php in the method TheLib_Debug::trace(). Please refer to the context and description for further information.

wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php

```
8    class TheLib_Debug extends TheLib {
⋮
325  public function trace( $output = true ) {
⋮
333  $block_id = 'wdev-debug-' . md5( rand() );
⋮
429  }
⋮
964  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php

```
333  $block_id = 'wdev-debug-' . hash('sha3-256', rand());
```

Issue #2279 - wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php: 277

Path: wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php
Line: 277
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 277 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php in the method TheLib_Debug::dump(). Please refer to the context and description for further information.

wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php

```
8    class TheLib_Debug extends TheLib {
⋮
270  public function dump( $first_arg ) {
⋮
277  $block_id = 'wdev-debug-' . md5( rand() );
⋮
313  }
⋮
964  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php

```
277 $block_id = 'wdev-debug-' . hash('sha3-256', rand());
```

Issue #2281 - wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php: 513

Path: wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php
Line: 513
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 513 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php in the method TheLib_Debug::_dump_var(). Please refer to the context and description for further information.

wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php

```
8   class TheLib_Debug extends TheLib {
⋮
441 protected function _dump_var( $data, $item_key = null, $default_depth = 3, $level = array( null ), $args = array
    () ) {
⋮
513 $id = substr( md5( rand() . ':' . $key . ':' . count( $level ) ), 0, 8 );
⋮
585 }
⋮
964 }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php

```
513 $id = substr( hash('sha3-256', rand() . ':' . $key . ':' . count($level)), 0, 8 );
```

Issue #2282 - wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php: 918

Path: wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php
Line: 918
Sink: md5
Taint: HTTP

Code Summary

A weak hash function in the operation md5() is used in line 918 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php in the method TheLib_Debug::marker_html(). Please refer to the context and description for further information.

wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php

```
8   class TheLib_Debug extends TheLib {
⋮
```

```
917  public function marker_html( $label = null, $styles = array() ) {
918  $hash = md5( rand( 1000, 9999 ) . time() );
⋮
963  }
964  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php

```
918  $hash = hash('sha3-256', rand(1000, 9999) . time());
```

Issue #2283 - wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php: 923

Path:	wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php
Line:	923
Sink:	md5
Taint:	HTTP

Code Summary

A weak hash function in the operation md5() is used in line 923 of the file wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php in the method TheLib_Debug::marker_html(). Please refer to the context and description for further information.

wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php

```
8    class TheLib_Debug extends TheLib {
⋮
917  public function marker_html( $label = null, $styles = array() ) {
⋮
923  $hash = md5( $label );
⋮
963  }
964  }
```

Algorithm Context

The following snippet(s) do not represent actual code but the tainted context.

```
weak hash algorithm: MD5
```

Patch

Replace Weak Hash with Strong Hash

wordpress-popup/lib/wpmu-lib/inc/class-thelib-debug.php

```
923  $hash = hash('sha3-256', $label);
```

3.11. Expression Always False

CWE: 572
Severity: Low

The application uses an expression that evaluates always to false. This is possibly leftover debug code in the application that should be removed when used in production.

The condition does not do anything and should be removed.

Issue #2195 - wordpress-popup/views/admin/commons/sui-wizard/tab-visibility/conditions.php: 38

Path: wordpress-popup/views/admin/commons/sui-wizard/tab-visibility/conditions.php
Line: 38
Sink:
Taint: HTTP

Code Summary

A code quality issue was detected in line 38 of the file wordpress-popup/views/admin/commons/sui-wizard/tab-visibility/conditions.php. Please refer to the context and description for further information.

wordpress-popup/views/admin/commons/sui-wizard/tab-visibility/conditions.php

```
38  <?php if ( false ) : // To be added. ?>
```

Code Context

The following snippet(s) do not represent actual code but the tainted context.

```
Constraint always false
```