```
kano@kali  /mnt/hgfs/SharedSpace/temp  wpscan --url http://10.129.64.192
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.10
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.129.64.192/ [10.129.64.192]
[+] Started: Sat Dec 19 21:41:27 2020

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.129.64.192/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress readme found: http://10.129.64.192/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.129.64.192/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.129.64.192/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8 identified (Insecure, released on 2017-06-08).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.129.64.192/index.php/feed/, <generator>https://wordpress.org/?v=4.8</gen
erator>
 |  - http://10.129.64.192/index.php/comments/feed/, <generator>https://wordpress.org/?v
=4.8</generator>
 |
 | [!] 49 vulnerabilities identified:
 |
 | [!] Title: WordPress 2.3.0-4.8.1 - $wpdb->prepare() potential SQL Injection
```

```
 |     Fixed in: 4.8.2
 |     References:
 |      - https://wpscan.com/vulnerability/8905
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14723
 |      - https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-re
lease/
 |      - https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c0705a5
48128e48
 |      - https://github.com/WordPress/WordPress/commit/fc930d3daed1c3acef010d04acc2c5de
93cd18ec
 |
 | [!] Title: WordPress 2.9.2-4.8.1 - Open Redirect
 |     Fixed in: 4.8.2
 |     References:
 |      - https://wpscan.com/vulnerability/8910
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14725
 |      - https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-re
lease/
 |      - https://core.trac.wordpress.org/changeset/41398
 |
 | [!] Title: WordPress 3.0-4.8.1 - Path Traversal in Unzipping
 |     Fixed in: 4.8.2
 |     References:
 |      - https://wpscan.com/vulnerability/8911
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14719
 |      - https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-re
lease/
 |      - https://core.trac.wordpress.org/changeset/41457
 |      - https://hackerone.com/reports/205481
 |
 | [!] Title: WordPress 4.4-4.8.1 - Path Traversal in Customizer
 |     Fixed in: 4.8.2
 |     References:
 |      - https://wpscan.com/vulnerability/8912
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14722
 |      - https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-re
lease/
 |      - https://core.trac.wordpress.org/changeset/41397
 |
 | [!] Title: WordPress 4.4-4.8.1 - Cross-Site Scripting (XSS) in oEmbed
 |     Fixed in: 4.8.2
 |     References:
 |      - https://wpscan.com/vulnerability/8913
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14724
 |      - https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-re
lease/
 |      - https://core.trac.wordpress.org/changeset/41448
 |
 | [!] Title: WordPress 4.2.3-4.8.1 - Authenticated Cross-Site Scripting (XSS) in Visual
Editor
 |     Fixed in: 4.8.2
 |     References:
 |      - https://wpscan.com/vulnerability/8914
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14726
 |      - https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-re
lease/
 |      - https://core.trac.wordpress.org/changeset/41395
 |      - https://blog.sucuri.net/2017/09/stored-cross-site-scripting-vulnerability-in-w
ordpress-4-8-1.html
 |
```

```
 | [!] Title: WordPress 2.3-4.8.3 - Host Header Injection in Password Reset
 |     References:
 |      - https://wpscan.com/vulnerability/8807
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8295
 |      - https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Password-Reset-0day-CVE-2017-8295.html
 |      - https://blog.dewhurstsecurity.com/2017/05/04/exploitbox-wordpress-security-advisories.html
 |      - https://core.trac.wordpress.org/ticket/25239
 |
 | [!] Title: WordPress <= 4.8.2 - $wpdb->prepare() Weakness
 |     Fixed in: 4.8.3
 |     References:
 |      - https://wpscan.com/vulnerability/8941
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-16510
 |      - https://wordpress.org/news/2017/10/wordpress-4-8-3-security-release/
 |      - https://github.com/WordPress/WordPress/commit/a2693fd8602e3263b5925b9d799ddd577202167d
 |      - https://twitter.com/ircmaxell/status/923662170092638208
 |      - https://blog.ircmaxell.com/2017/10/disclosure-wordpress-wpdb-sql-injection-technical.html
 |
 | [!] Title: WordPress 2.8.6-4.9 - Authenticated JavaScript File Upload
 |     Fixed in: 4.8.4
 |     References:
 |      - https://wpscan.com/vulnerability/8966
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17092
 |      - https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/67d03a98c2cae5f41843c897f206adde299b0509
 |
 | [!] Title: WordPress 1.5.0-4.9 - RSS and Atom Feed Escaping
 |     Fixed in: 4.8.4
 |     References:
 |      - https://wpscan.com/vulnerability/8967
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17094
 |      - https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/f1de7e42df29395c3314bf85bff3d1f4f90541de
 |
 | [!] Title: WordPress 4.3.0-4.9 - HTML Language Attribute Escaping
 |     Fixed in: 4.8.4
 |     References:
 |      - https://wpscan.com/vulnerability/8968
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17093
 |      - https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/3713ac5ebc90fb2011e98dfd691420f43da6c09a
 |
 | [!] Title: WordPress 3.7-4.9 - 'newbloguser' Key Weak Hashing
 |     Fixed in: 4.8.4
 |     References:
 |      - https://wpscan.com/vulnerability/8969
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17091
 |      - https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/eaf1cfdc1fe0bdffabd8d879c591b864
```

```
d833326c
 |
 | [!] Title: WordPress 3.7-4.9.1 - MediaElement Cross-Site Scripting (XSS)
 |     Fixed in: 4.8.5
 |     References:
 |      - https://wpscan.com/vulnerability/9006
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5776
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9263
 |      - https://github.com/WordPress/WordPress/commit/3fe9cb61ee71fcfadb5e002399296fcc
1198d850
 |      - https://wordpress.org/news/2018/01/wordpress-4-9-2-security-and-maintenance-re
lease/
 |      - https://core.trac.wordpress.org/ticket/42720
 |
 | [!] Title: WordPress <= 4.9.4 - Application Denial of Service (DoS) (unpatched)
 |     References:
 |      - https://wpscan.com/vulnerability/9021
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6389
 |      - https://baraktawily.blogspot.fr/2018/02/how-to-dos-29-of-world-wide-websites.h
tml
 |      - https://github.com/quitten/doser.py
 |      - https://thehackernews.com/2018/02/wordpress-dos-exploit.html
 |
 | [!] Title: WordPress 3.7-4.9.4 - Remove localhost Default
 |     Fixed in: 4.8.6
 |     References:
 |      - https://wpscan.com/vulnerability/9053
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10101
 |      - https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-re
lease/
 |      - https://github.com/WordPress/WordPress/commit/804363859602d4050d9a38a21f5a65d9
aec18216
 |
 | [!] Title: WordPress 3.7-4.9.4 - Use Safe Redirect for Login
 |     Fixed in: 4.8.6
 |     References:
 |      - https://wpscan.com/vulnerability/9054
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10100
 |      - https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-re
lease/
 |      - https://github.com/WordPress/WordPress/commit/14bc2c0a6fde0da04b47130707e01df8
50eedc7e
 |
 | [!] Title: WordPress 3.7-4.9.4 - Escape Version in Generator Tag
 |     Fixed in: 4.8.6
 |     References:
 |      - https://wpscan.com/vulnerability/9055
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10102
 |      - https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-re
lease/
 |      - https://github.com/WordPress/WordPress/commit/31a4369366d6b8ce30045d4c838de241
2c77850d
 |
 | [!] Title: WordPress <= 4.9.6 - Authenticated Arbitrary File Deletion
 |     Fixed in: 4.8.7
 |     References:
 |      - https://wpscan.com/vulnerability/9100
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12895
 |      - https://blog.ripstech.com/2018/wordpress-file-delete-to-code-execution/
 |      - http://blog.vulnspy.com/2018/06/27/Wordpress-4-9-6-Arbitrary-File-Delection-Vu
```

```
lnerbility-Exploit/
 |      - https://github.com/WordPress/WordPress/commit/c9dce0606b0d7e6f494d4abe7b193ac0
46a322cd
 |      - https://wordpress.org/news/2018/07/wordpress-4-9-7-security-and-maintenance-re
lease/
 |      - https://www.wordfence.com/blog/2018/07/details-of-an-additional-file-deletion-
vulnerability-patched-in-wordpress-4-9-7/
 |
 | [!] Title: WordPress <= 5.0 - Authenticated File Delete
 |     Fixed in: 4.8.8
 |     References:
 |      - https://wpscan.com/vulnerability/9169
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20147
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |
 | [!] Title: WordPress <= 5.0 - Authenticated Post Type Bypass
 |     Fixed in: 4.8.8
 |     References:
 |      - https://wpscan.com/vulnerability/9170
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20152
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |      - https://blog.ripstech.com/2018/wordpress-post-type-privilege-escalation/
 |
 | [!] Title: WordPress <= 5.0 - PHP Object Injection via Meta Data
 |     Fixed in: 4.8.8
 |     References:
 |      - https://wpscan.com/vulnerability/9171
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20148
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |
 | [!] Title: WordPress <= 5.0 - Authenticated Cross-Site Scripting (XSS)
 |     Fixed in: 4.8.8
 |     References:
 |      - https://wpscan.com/vulnerability/9172
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20153
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |
 | [!] Title: WordPress <= 5.0 - Cross-Site Scripting (XSS) that could affect plugins
 |     Fixed in: 4.8.8
 |     References:
 |      - https://wpscan.com/vulnerability/9173
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20150
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |      - https://github.com/WordPress/WordPress/commit/fb3c6ea0618fcb9a51d4f2c1940e9efc
d4a2d460
 |
 | [!] Title: WordPress <= 5.0 - User Activation Screen Search Engine Indexing
 |     Fixed in: 4.8.8
 |     References:
 |      - https://wpscan.com/vulnerability/9174
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20151
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |
 | [!] Title: WordPress <= 5.0 - File Upload to XSS on Apache Web Servers
 |     Fixed in: 4.8.8
 |     References:
 |      - https://wpscan.com/vulnerability/9175
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20149
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |      - https://github.com/WordPress/WordPress/commit/246a70bdbfac3bd45ff71c7941deef1b
```

```
b206b19a
 |
 | [!] Title: WordPress 3.7-5.0 (except 4.9.9) - Authenticated Code Execution
 |     Fixed in: 5.0.1
 |     References:
 |      - https://wpscan.com/vulnerability/9222
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8942
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8943
 |      - https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/
 |      - https://www.rapid7.com/db/modules/exploit/multi/http/wp_crop_rce
 |
 | [!] Title: WordPress 3.9-5.1 - Comment Cross-Site Scripting (XSS)
 |     Fixed in: 4.8.9
 |     References:
 |      - https://wpscan.com/vulnerability/9230
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9787
 |      - https://github.com/WordPress/WordPress/commit/0292de60ec78c5a44956765189403654
fe4d080b
 |      - https://wordpress.org/news/2019/03/wordpress-5-1-1-security-and-maintenance-re
lease/
 |      - https://blog.ripstech.com/2019/wordpress-csrf-to-rce/
 |
 | [!] Title: WordPress <= 5.2.2 - Cross-Site Scripting (XSS) in URL Sanitisation
 |     Fixed in: 4.8.10
 |     References:
 |      - https://wpscan.com/vulnerability/9867
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16222
 |      - https://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-re
lease/
 |      - https://github.com/WordPress/WordPress/commit/30ac67579559fe42251b5a9f887211bf
61a8ed68
 |      - https://hackerone.com/reports/339483
 |
 | [!] Title: WordPress <= 5.2.3 - Stored XSS in Customizer
 |     Fixed in: 4.8.11
 |     References:
 |      - https://wpscan.com/vulnerability/9908
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17674
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-se
curity-release-breakdown.html
 |
 | [!] Title: WordPress <= 5.2.3 - Unauthenticated View Private/Draft Posts
 |     Fixed in: 4.8.11
 |     References:
 |      - https://wpscan.com/vulnerability/9909
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17671
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-se
curity-release-breakdown.html
 |      - https://github.com/WordPress/WordPress/commit/f82ed753cf00329a5e41f2cb6dc52108
5136f308
 |      - https://0day.work/proof-of-concept-for-wordpress-5-2-3-viewing-unauthenticated
-posts/
 |
 | [!] Title: WordPress <= 5.2.3 - Stored XSS in Style Tags
 |     Fixed in: 4.8.11
 |     References:
 |      - https://wpscan.com/vulnerability/9910
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17672
```

```
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-se
curity-release-breakdown.html
 |
 | [!] Title: WordPress <= 5.2.3 - JSON Request Cache Poisoning
 |     Fixed in: 4.8.11
 |     References:
 |      - https://wpscan.com/vulnerability/9911
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17673
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://github.com/WordPress/WordPress/commit/b224c251adfa16a5f84074a3c0886270
c9df38de
 |      - https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-se
curity-release-breakdown.html
 |
 | [!] Title: WordPress <= 5.2.3 - Server-Side Request Forgery (SSRF) in URL Validation
 |     Fixed in: 4.8.11
 |     References:
 |      - https://wpscan.com/vulnerability/9912
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17669
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17670
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://github.com/WordPress/WordPress/commit/9db44754b9e4044690a6c32fd74b9d5f
e26b07b2
 |      - https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-se
curity-release-breakdown.html
 |
 | [!] Title: WordPress <= 5.2.3 - Admin Referrer Validation
 |     Fixed in: 4.8.11
 |     References:
 |      - https://wpscan.com/vulnerability/9913
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17675
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://github.com/WordPress/WordPress/commit/b183fd1cca0b44a92f0264823dd9f22d
2fd8b8d0
 |      - https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-se
curity-release-breakdown.html
 |
 | [!] Title: WordPress <= 5.3 - Authenticated Improper Access Controls in REST API
 |     Fixed in: 4.8.12
 |     References:
 |      - https://wpscan.com/vulnerability/9973
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20043
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16788
 |      - https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-re
lease/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-g7rg-h
chx-c2gw
 |
 | [!] Title: WordPress <= 5.3 - Authenticated Stored XSS via Crafted Links
 |     Fixed in: 4.8.12
 |     References:
 |      - https://wpscan.com/vulnerability/9975
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16773
 |      - https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-re
lease/
 |      - https://hackerone.com/reports/509930
 |      - https://github.com/WordPress/wordpress-develop/commit/1f7f3f1f59567e2504f0fbeb
d51ccf004b3ccb1d
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-xvg2-m
```

```
2f4-83m7
 |
 | [!] Title: WordPress <= 5.3 - Authenticated Stored XSS via Block Editor Content
 |     Fixed in: 4.8.12
 |     References:
 |      - https://wpscan.com/vulnerability/9976
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16781
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16780
 |      - https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-re
lease/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-pg4x-6
4rh-3c9v
 |
 | [!] Title: WordPress <= 5.3 - wp_kses_bad_protocol() Colon Bypass
 |     Fixed in: 4.8.12
 |     References:
 |      - https://wpscan.com/vulnerability/10004
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20041
 |      - https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-re
lease/
 |      - https://github.com/WordPress/wordpress-develop/commit/b1975463dd995da19bb40d3f
a0786498717e3c53
 |
 | [!] Title: WordPress < 5.4.1 - Password Reset Tokens Failed to Be Properly Invalidate
d
 |     Fixed in: 4.8.13
 |     References:
 |      - https://wpscan.com/vulnerability/10201
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11027
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47634/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-i
n-todays-wordpress-5-4-1-security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-ww7v-j
g8c-q6jw
 |
 | [!] Title: WordPress < 5.4.1 - Unauthenticated Users View Private Posts
 |     Fixed in: 4.8.13
 |     References:
 |      - https://wpscan.com/vulnerability/10202
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11028
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47635/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-i
n-todays-wordpress-5-4-1-security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-xhx9-7
59f-6p2w
 |
 | [!] Title: WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in Customizer
 |     Fixed in: 4.8.13
 |     References:
 |      - https://wpscan.com/vulnerability/10203
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11025
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47633/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-i
n-todays-wordpress-5-4-1-security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4mhg-j
6fx-5g3c
 |
```

```
 | [!] Title: WordPress < 5.4.1 - Cross-Site Scripting (XSS) in wp-object-cache
 |     Fixed in: 4.8.13
 |     References:
 |      - https://wpscan.com/vulnerability/10205
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11029
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47637/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-568w-8m88-8g2c
 |
 | [!] Title: WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in File Uploads
 |     Fixed in: 4.8.13
 |     References:
 |      - https://wpscan.com/vulnerability/10206
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11026
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47638/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-3gw2-4656-pfr2
 |      - https://hackerone.com/reports/179695
 |
 | [!] Title: WordPress <= 5.2.3 - Hardening Bypass
 |     Fixed in: 4.8.11
 |     References:
 |      - https://wpscan.com/vulnerability/10259
 |      - https://blog.ripstech.com/2020/wordpress-hardening-bypass/
 |      - https://hackerone.com/reports/436928
 |      - https://wordpress.org/news/2019/11/wordpress-5-2-4-update/
 |
 | [!] Title: WordPress < 5.4.2 - Authenticated XSS via Media Files
 |     Fixed in: 4.8.14
 |     References:
 |      - https://wpscan.com/vulnerability/10264
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4047
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-8q2w-5m27-wm27
 |
 | [!] Title: WordPress < 5.4.2 - Open Redirection
 |     Fixed in: 4.8.14
 |     References:
 |      - https://wpscan.com/vulnerability/10265
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4048
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/10e2a50c523cf0b9785555a688d7d36a40fbeccf
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-q6pw-gvf4-5fj5
 |
 | [!] Title: WordPress < 5.4.2 - Authenticated Stored XSS via Theme Upload
 |     Fixed in: 4.8.14
 |     References:
 |      - https://wpscan.com/vulnerability/10266
```

```
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4049
 |      - https://www.exploit-db.com/exploits/48770/
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-87h4-phjv-rm6p
 |      - https://hackerone.com/reports/406289
 |
 | [!] Title: WordPress < 5.4.2 - Misuse of set-screen-option Leading to Privilege Escalation
 |     Fixed in: 4.8.14
 |     References:
 |      - https://wpscan.com/vulnerability/10267
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4050
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/dda0ccdd18f6532481406cabede19ae2ed1f575d
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4vpv-fgg2-gcqc
 |
 | [!] Title: WordPress < 5.4.2 - Disclosure of Password-Protected Page/Post Comments
 |     Fixed in: 4.8.14
 |     References:
 |      - https://wpscan.com/vulnerability/10268
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25286
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/c075eec24f2f3214ab0d0fb0120a23082e6b1122

[+] WordPress theme in use: twentyseventeen
 | Location: http://10.129.64.192/wp-content/themes/twentyseventeen/
 | Last Updated: 2020-12-09T00:00:00.000Z
 | Readme: http://10.129.64.192/wp-content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 2.5
 | Style URL: http://10.129.64.192/wp-content/themes/twentyseventeen/style.css?ver=4.8
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.129.64.192/wp-content/themes/twentyseventeen/style.css?ver=4.8, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01 <=========> (22 / 22) 100.00% Time: 00:00:01

[i] No Config Backups Found.
```

```
[+] WPVulnDB API OK
 | Plan: free
 | Requests Done (during the scan): 2
 | Requests Remaining: 46

[+] Finished: Sat Dec 19 21:41:43 2020
[+] Requests Done: 56
[+] Cached Requests: 5
[+] Data Sent: 12.172 KB
[+] Data Received: 318.125 KB
[+] Memory used: 184.555 MB
[+] Elapsed time: 00:00:15
```