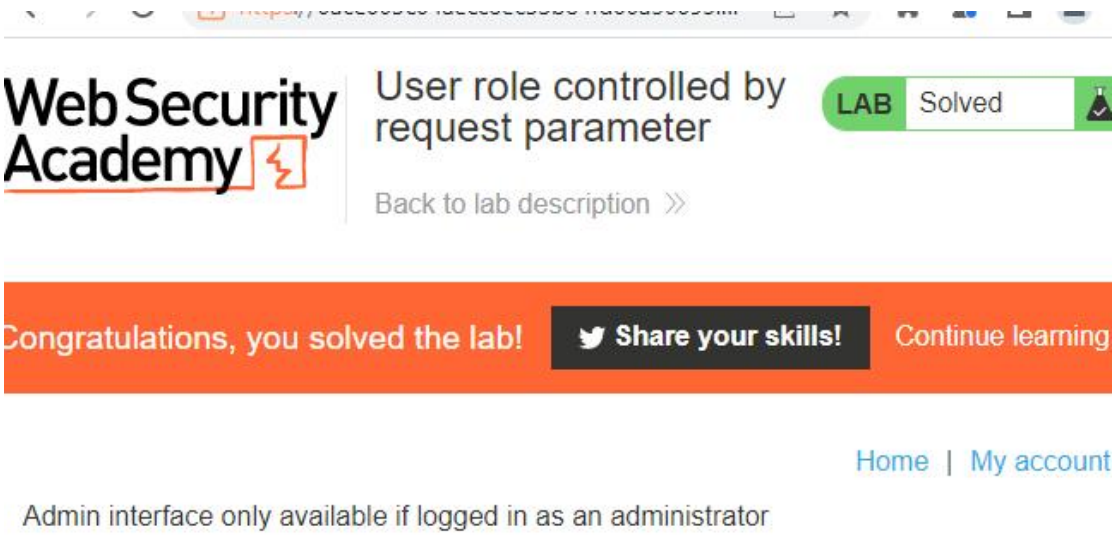
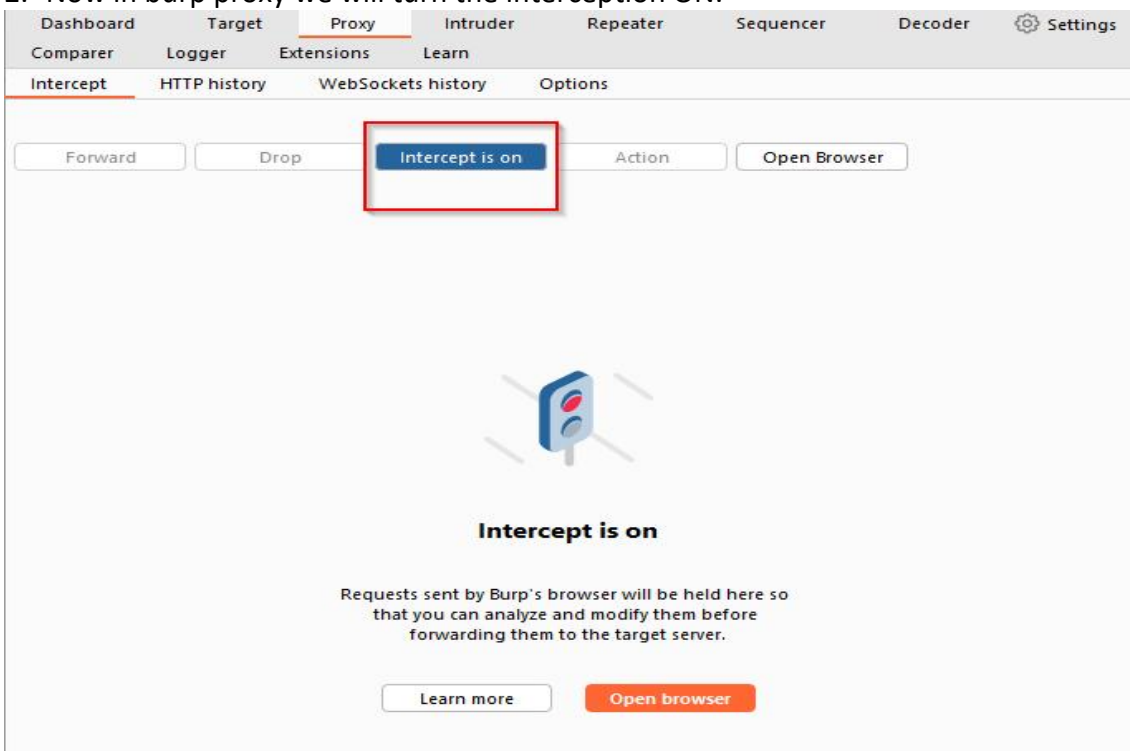
Lab: User role controlled by request parameter

1.First we need to go to the admin panel to see if we have access to the admin panel. In the url we will append /admin. And see the following message.

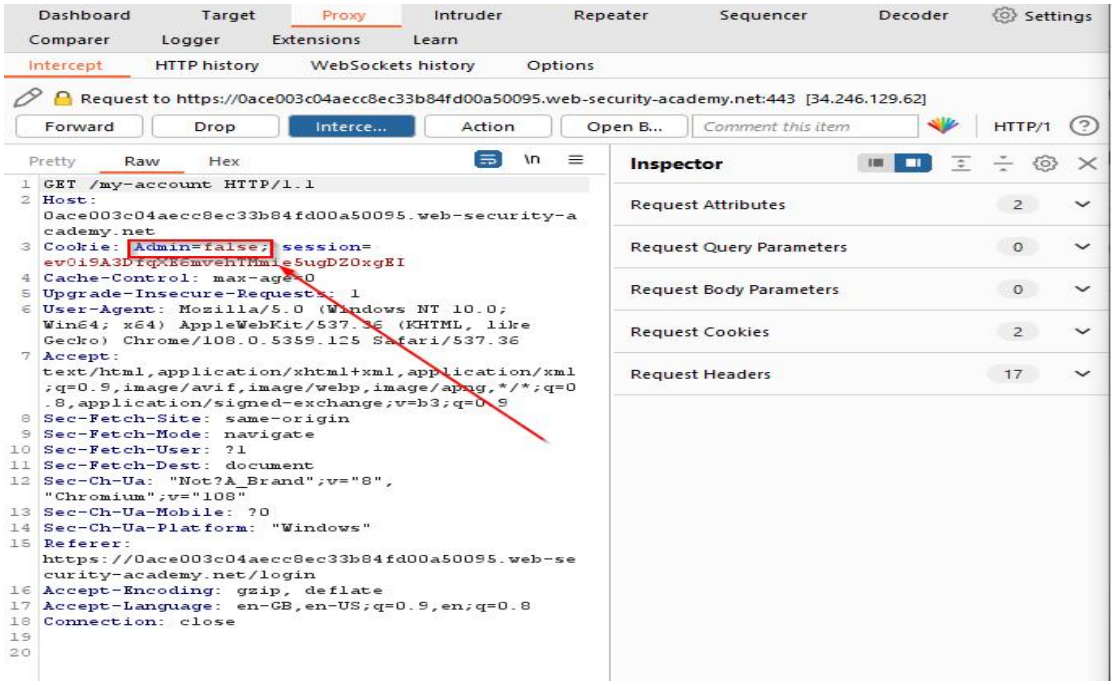


2. Now in burp proxy we will turn the interception ON.

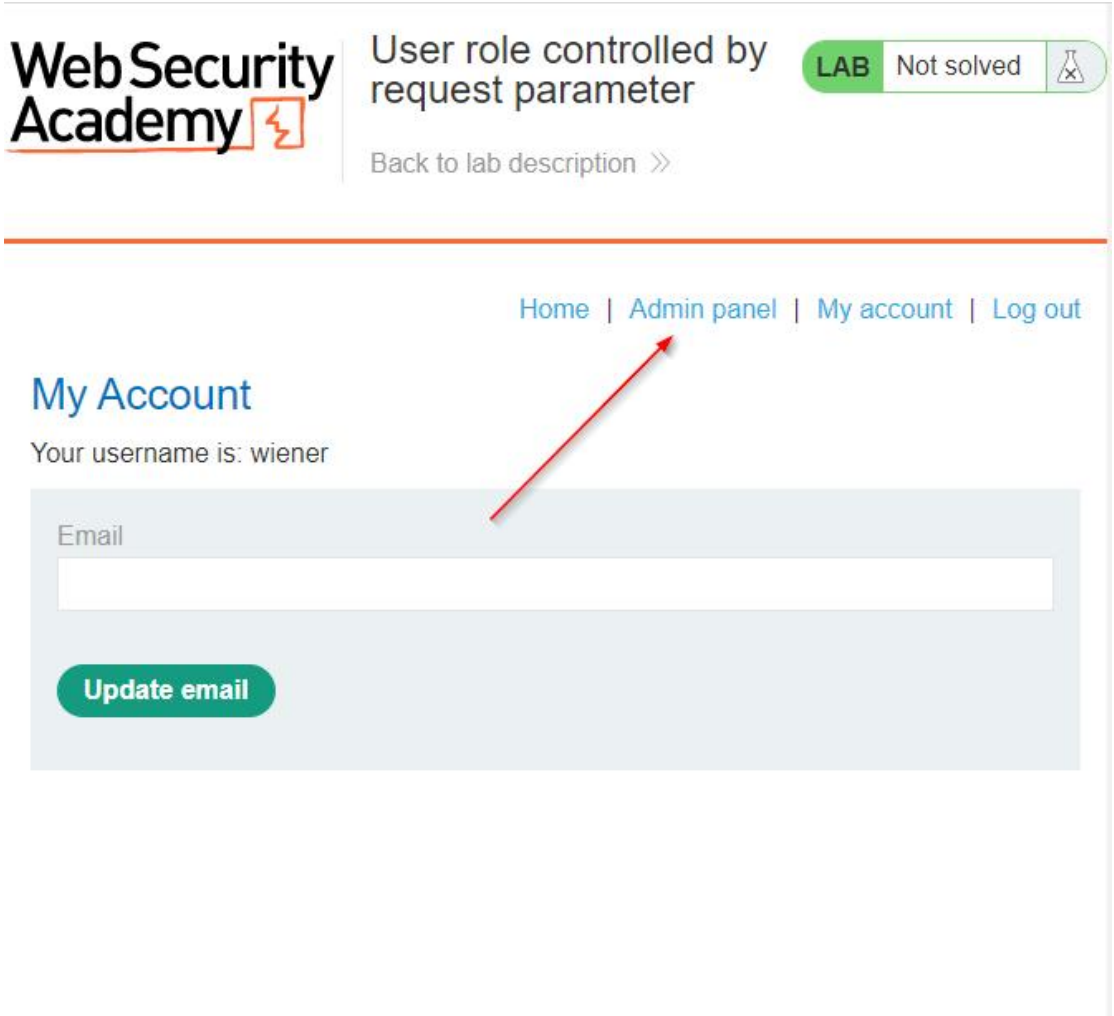


3. Now we will Complete and submit the login form

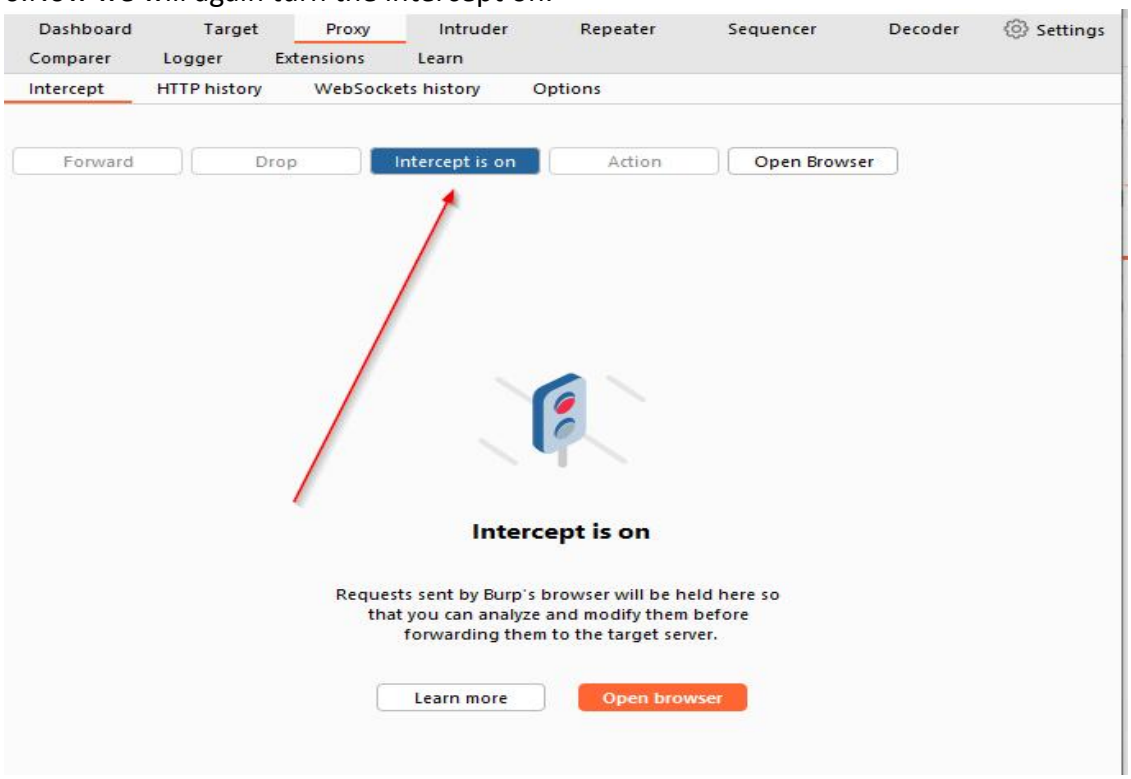
4. From the inercept we will change the Cookie Admin : False



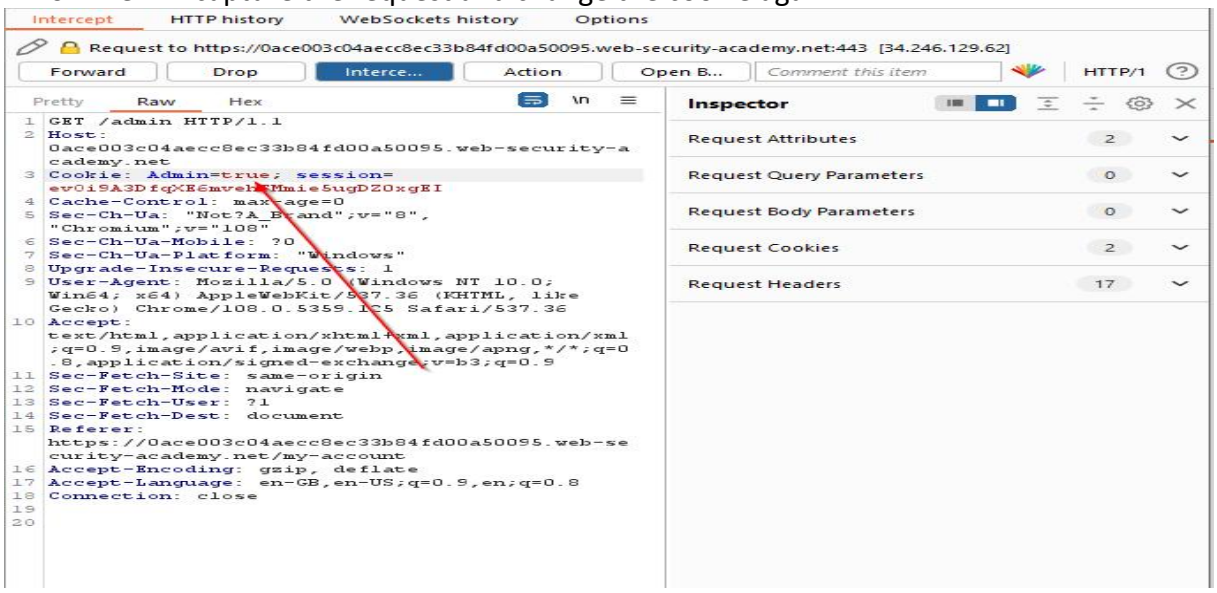
5.We will change it to “True” and forward to go to the Admin panel



6.Now we will again turn the intercept on.

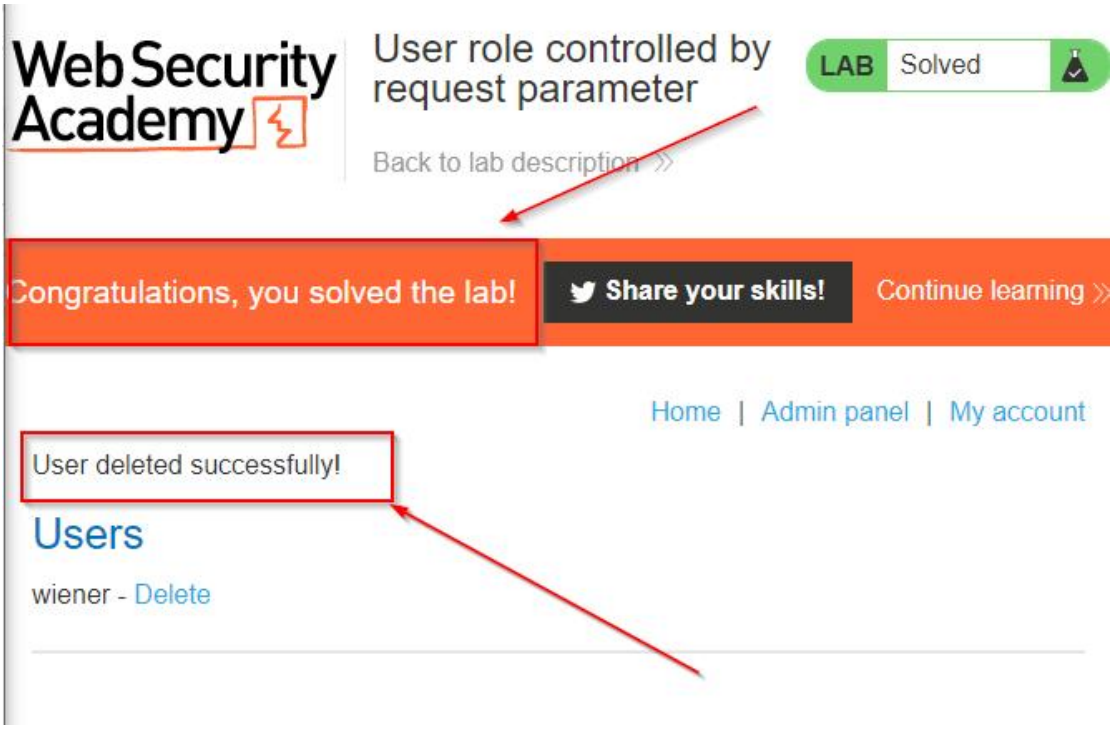


7.Now we will capture the request and change the cookie again.



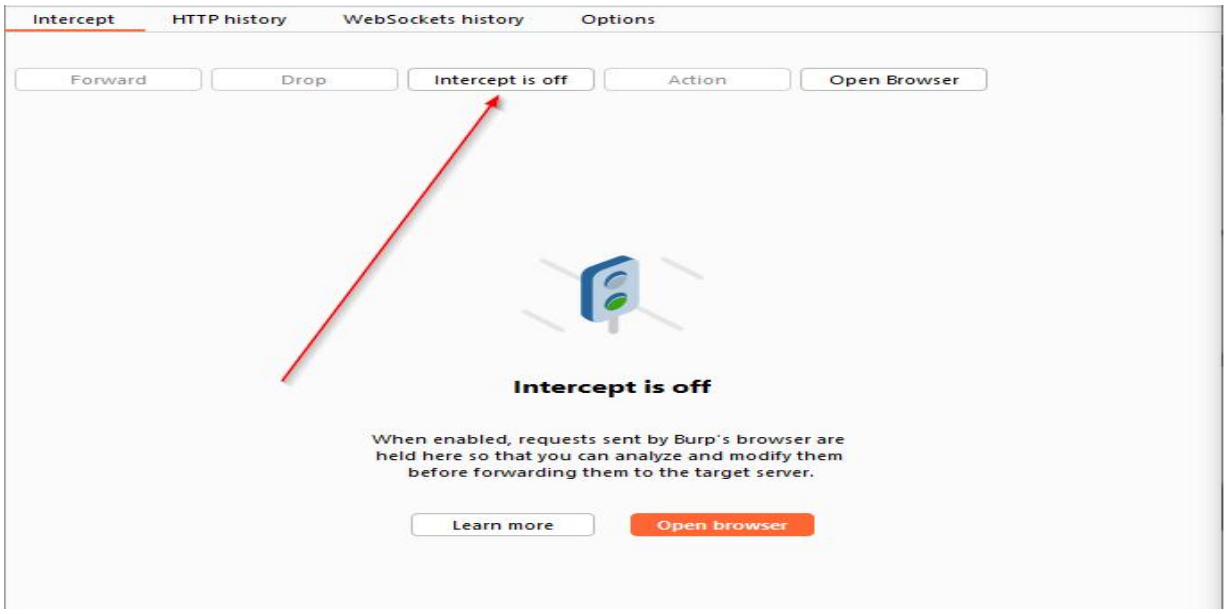
8. When forwarded we will be able to see the admin panel in the chromiam browser. And we will delete the carlos user and again click the forward button to solve the lab.

9. The lab is solved Now

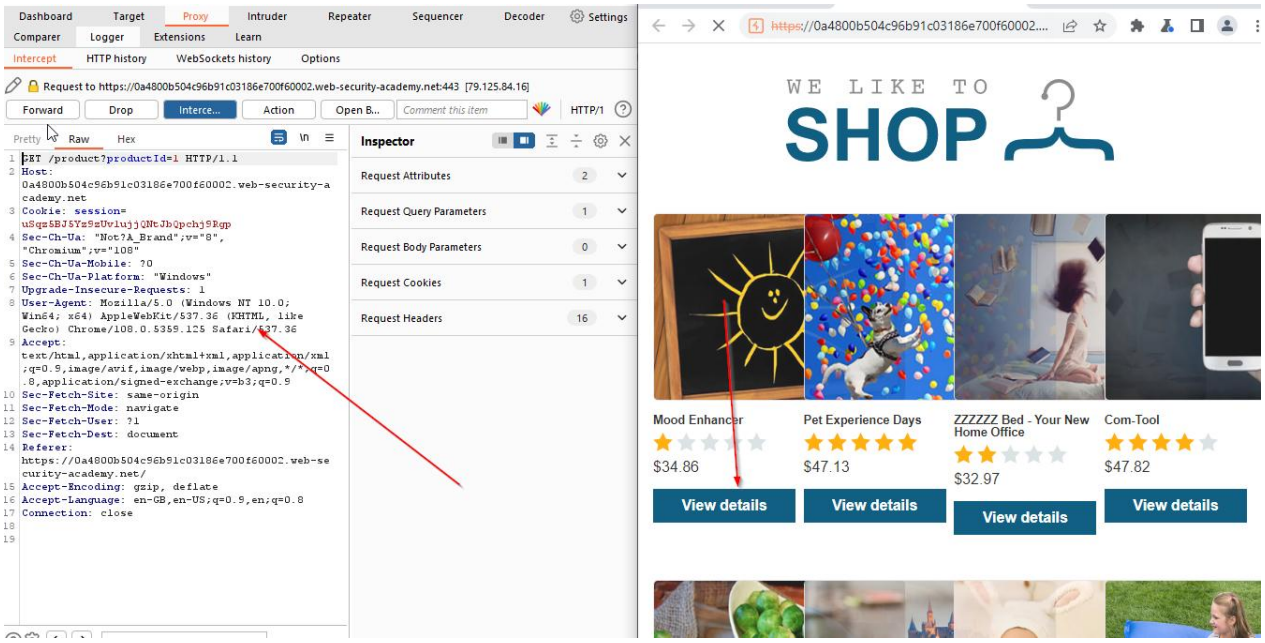


Lab 2: File path traversal, traversal sequences stripped non-recursively.

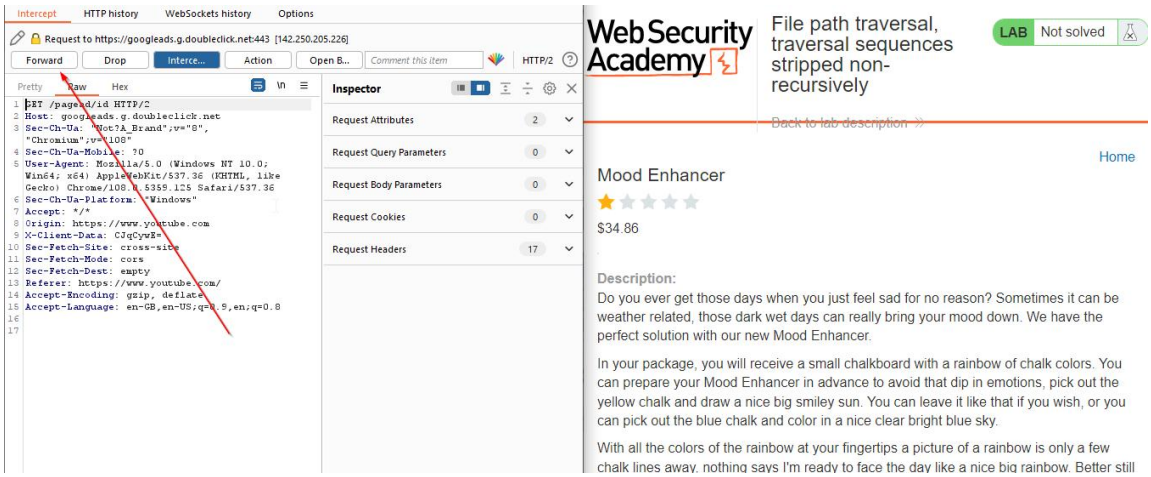
1. Go to the home page and from Burp suite turn the intercept on.



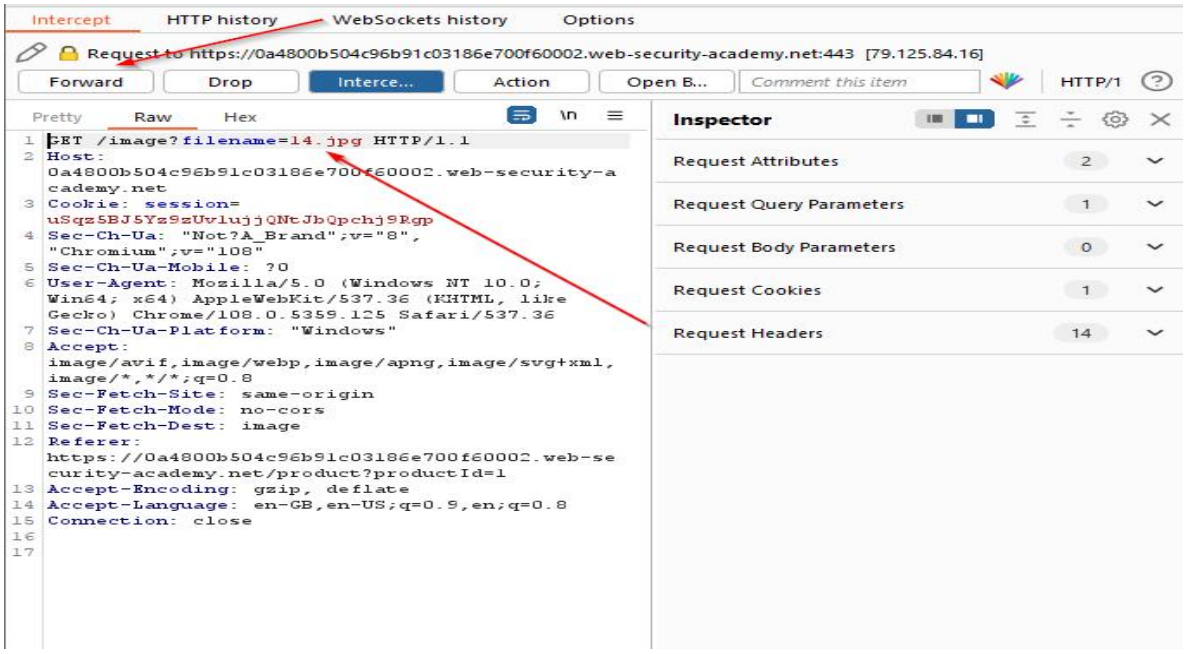
2. Click on the Veiw details of a product and capture the request.



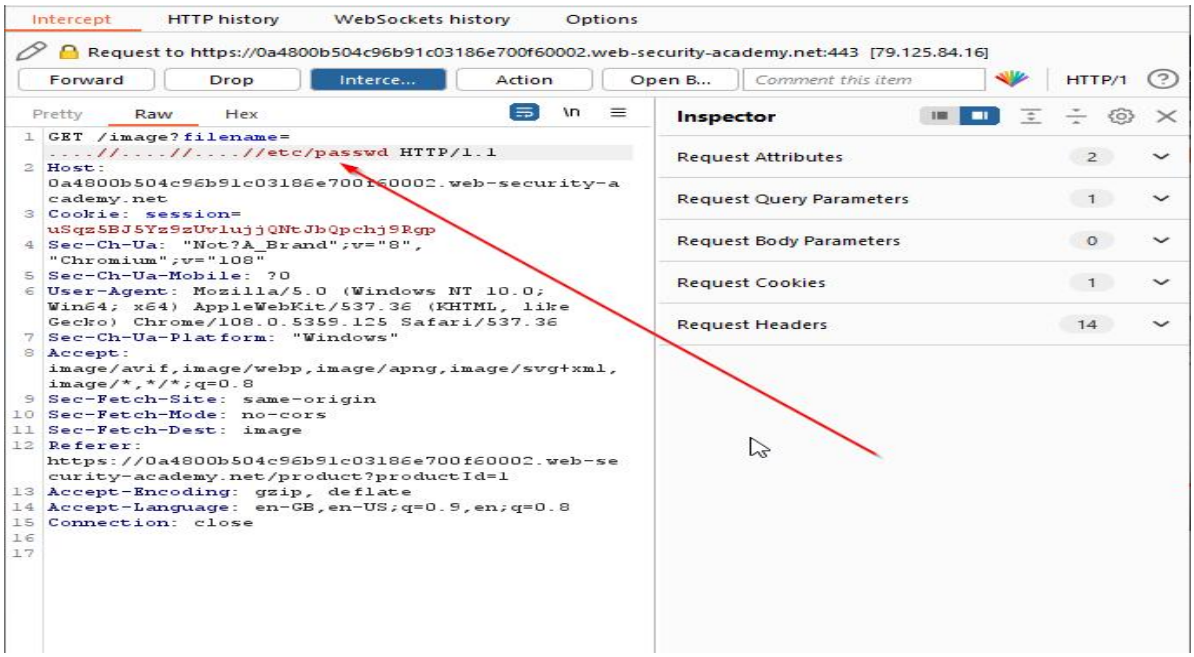
3. For ward the request.



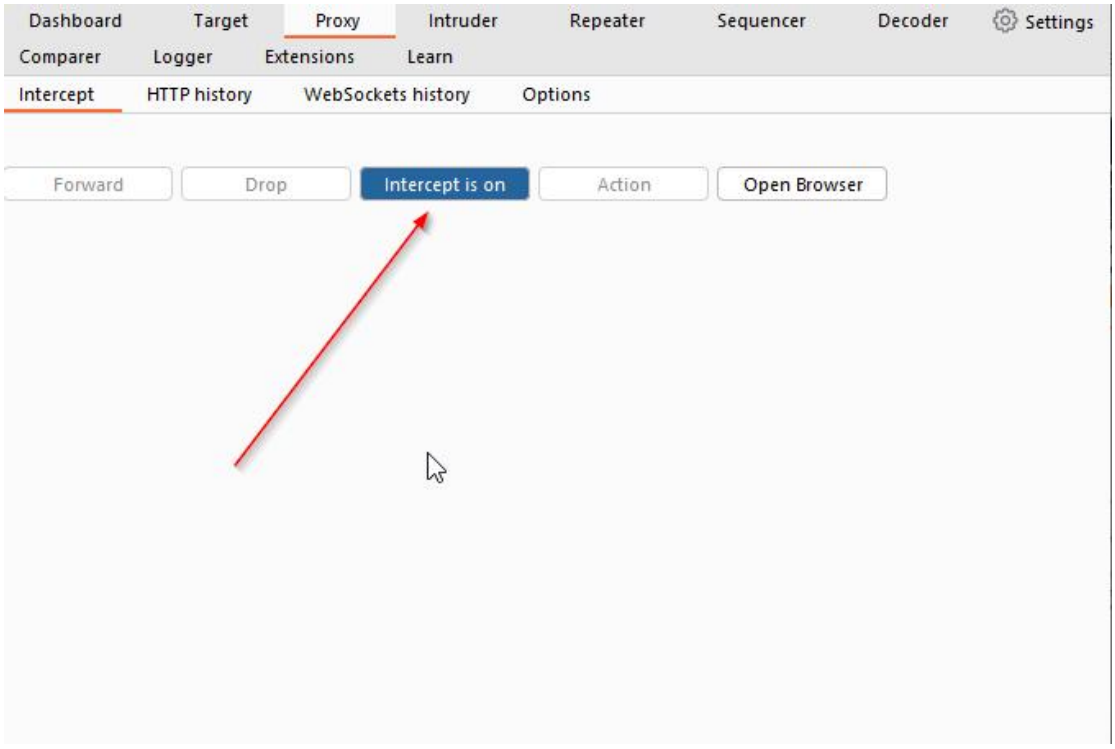
4. Now again click the forward button to forward the get request. We will get the file name



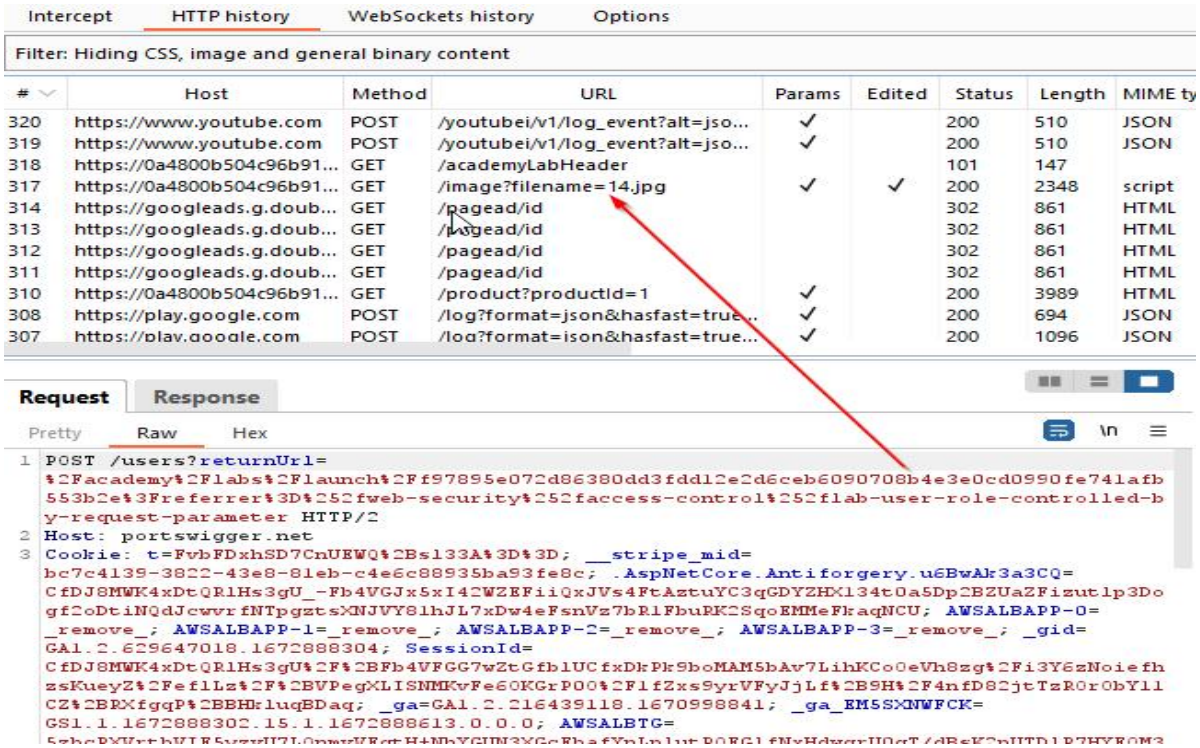
5. Now change the path like the following.



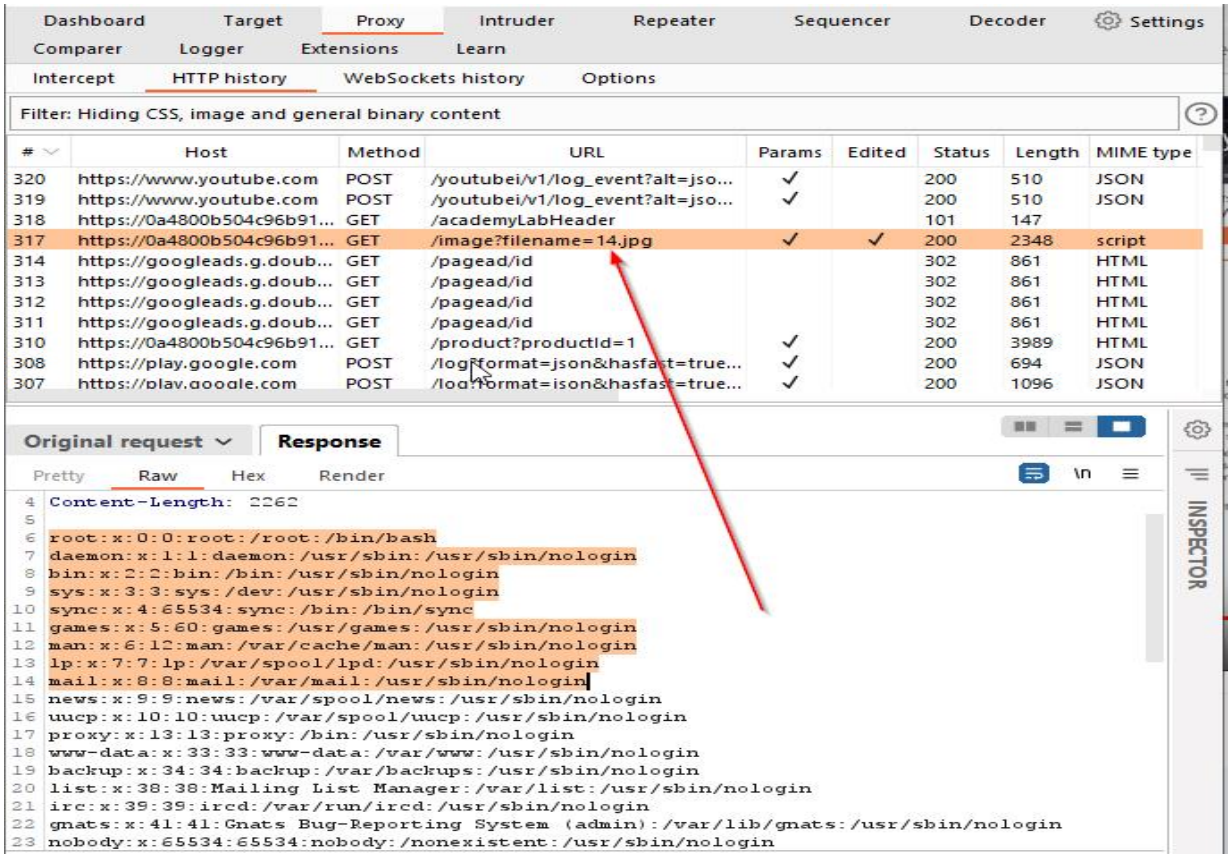
Now forward the request and finally turn the intercept off.



After turning of the intercept go to the http history and then find the get request with the file name .



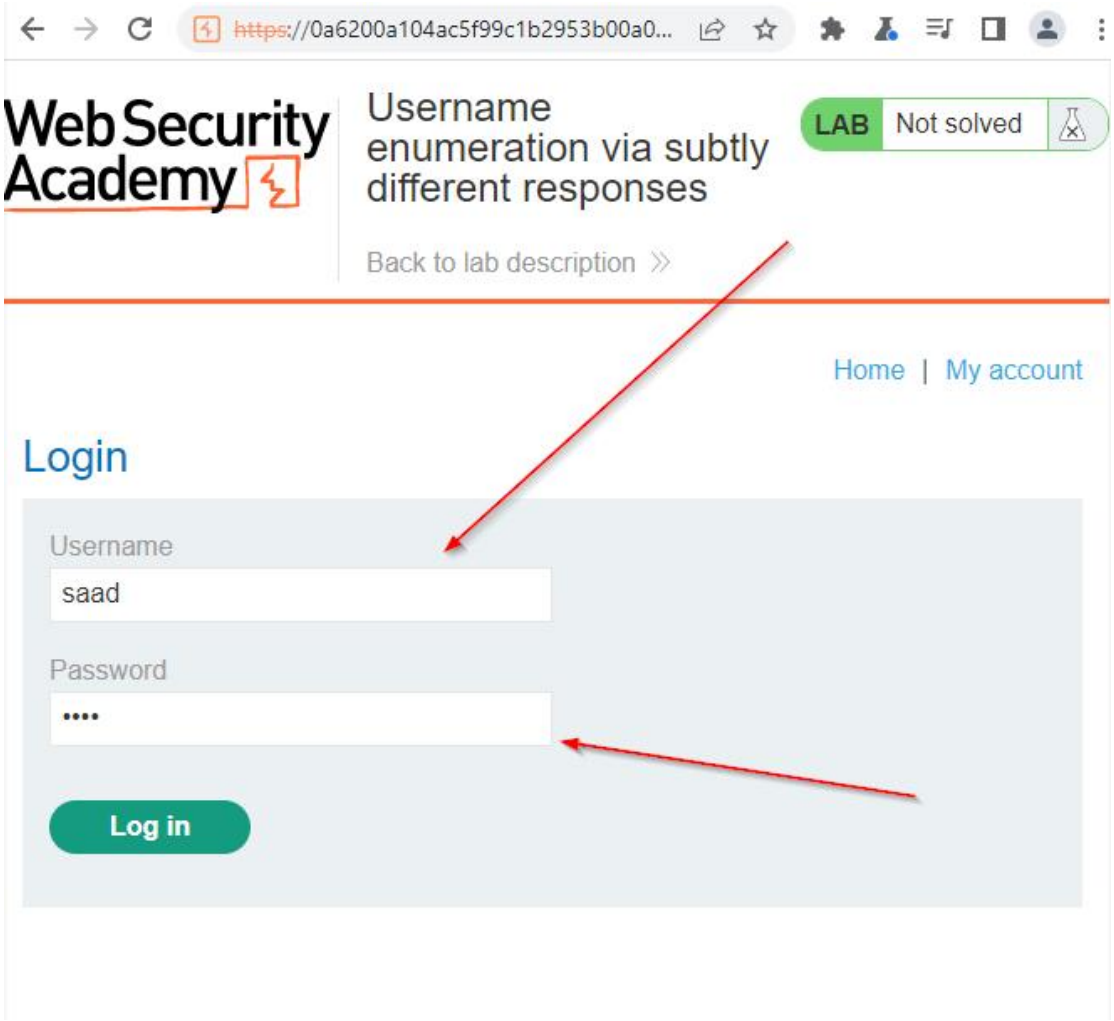
Open the file and see the response.



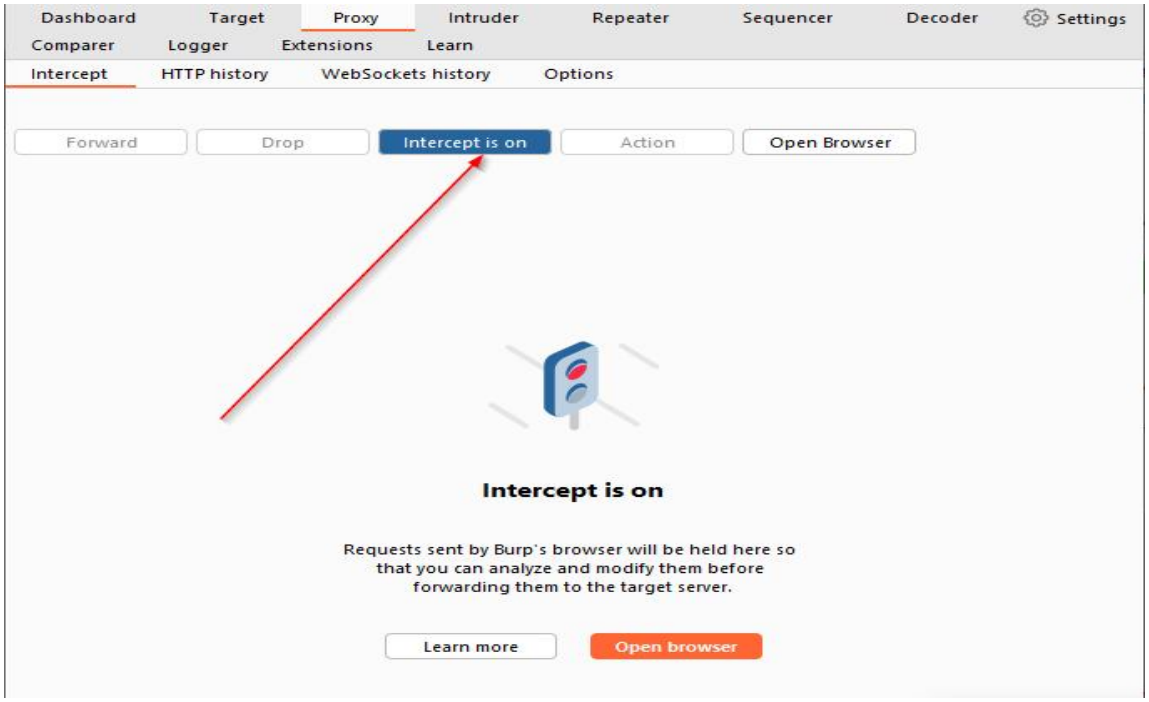
Now we will refresh the page from the browser. The lab will be solved.

Lab: Username enumeration via subtly different responses.

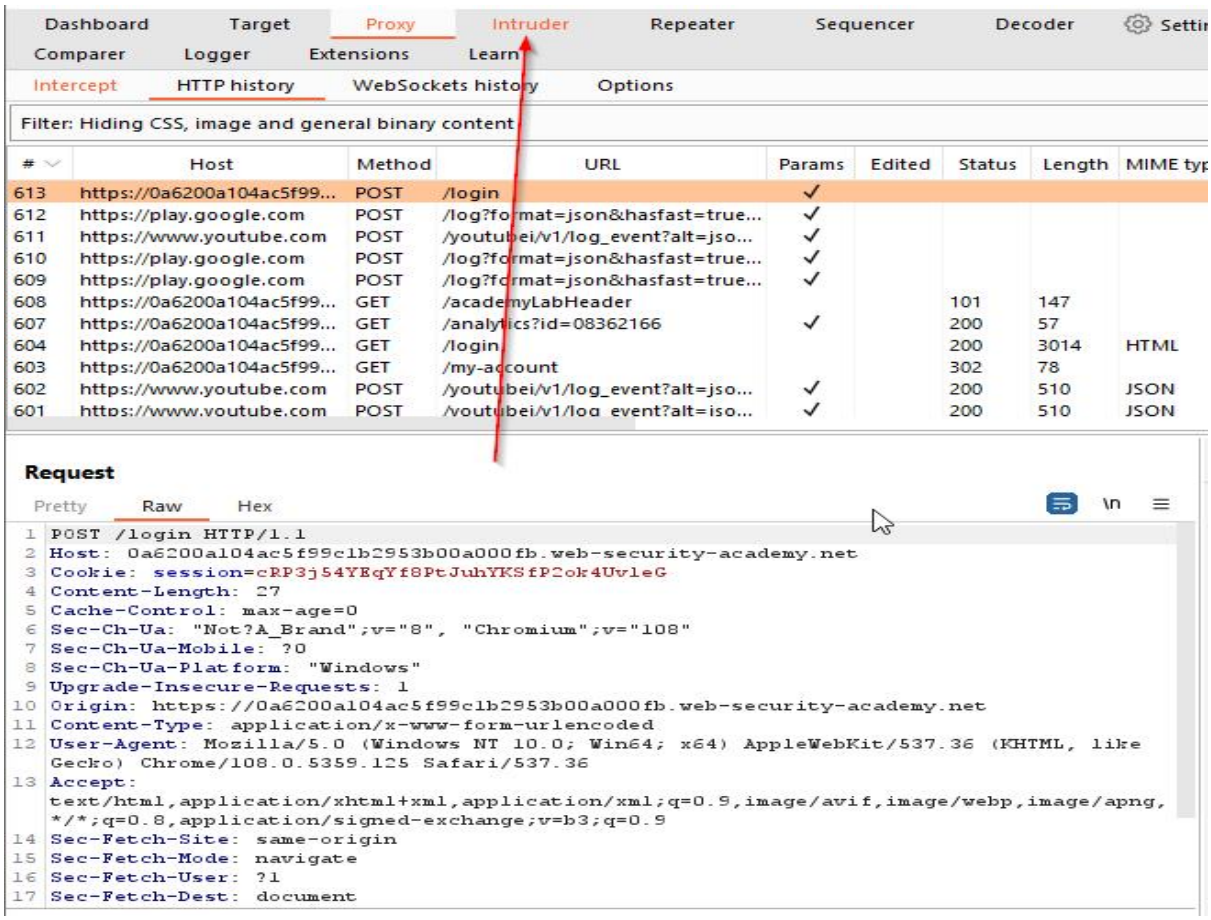
1. Go to the login page and pu the login credentials.



2.Then go to burp suite and turn the intercept on.



3.The click login from the browser and catch the request on the burp suite. Send the request to the intruder.



4.From the intruder make the password and email as variables.

Positions | Payloads | Resource Pool | Options

Choose an attack type

Start attack

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: 3b00a000fb.web-security-academy.net

Update Host header to match target

Add §
Clear §
Auto §
Refresh

```
 8 Sec-Ch-Ua-Platform: "Windows"
 9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a6200a104ac5f99c1b2953b00a000fb.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
13 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
   bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer:
   https://0a6200a104ac5f99c1b2953b00a000fb.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
21 Connection: close
22
23 username=§saad§&password=§1234§
```

Search... 0 matches Clear

3 payload positions Length: 1031

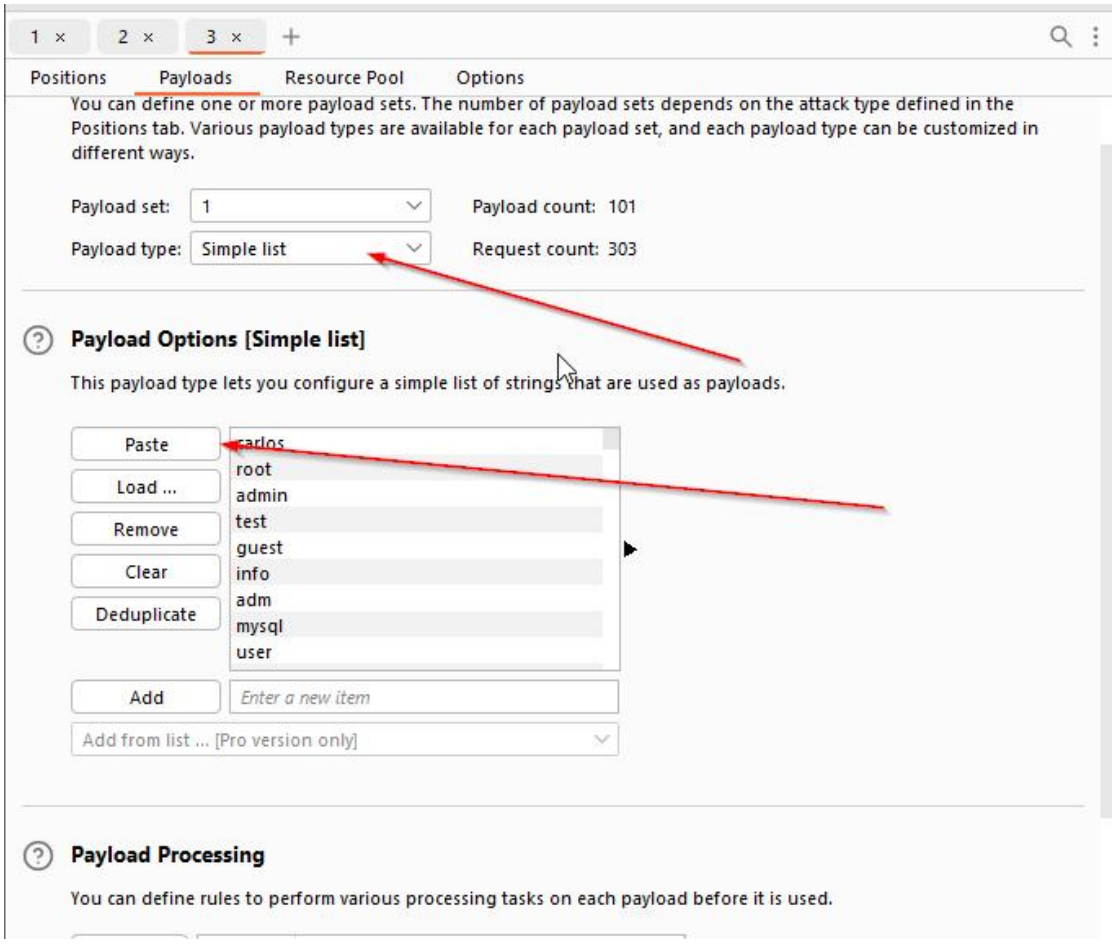
5.From the Authentication Lab user names copy the usernames.

Authentication lab usernames

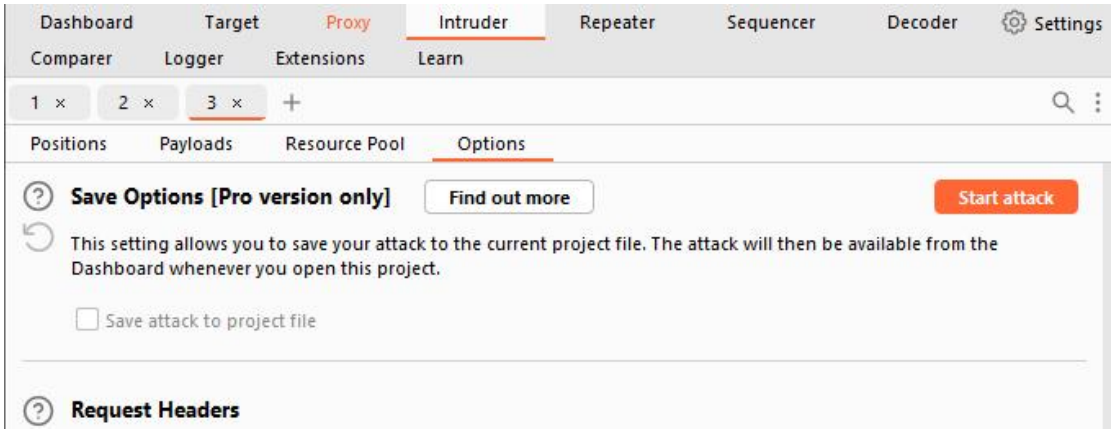
You can copy and paste the following list to Burp Intruder to help you solve the Authentication labs.

```
carlos
root
admin
test
guest
info
adm
mysql
user
administrator
oracle
ftp
pi
puppet
ansible
ec2-user
```

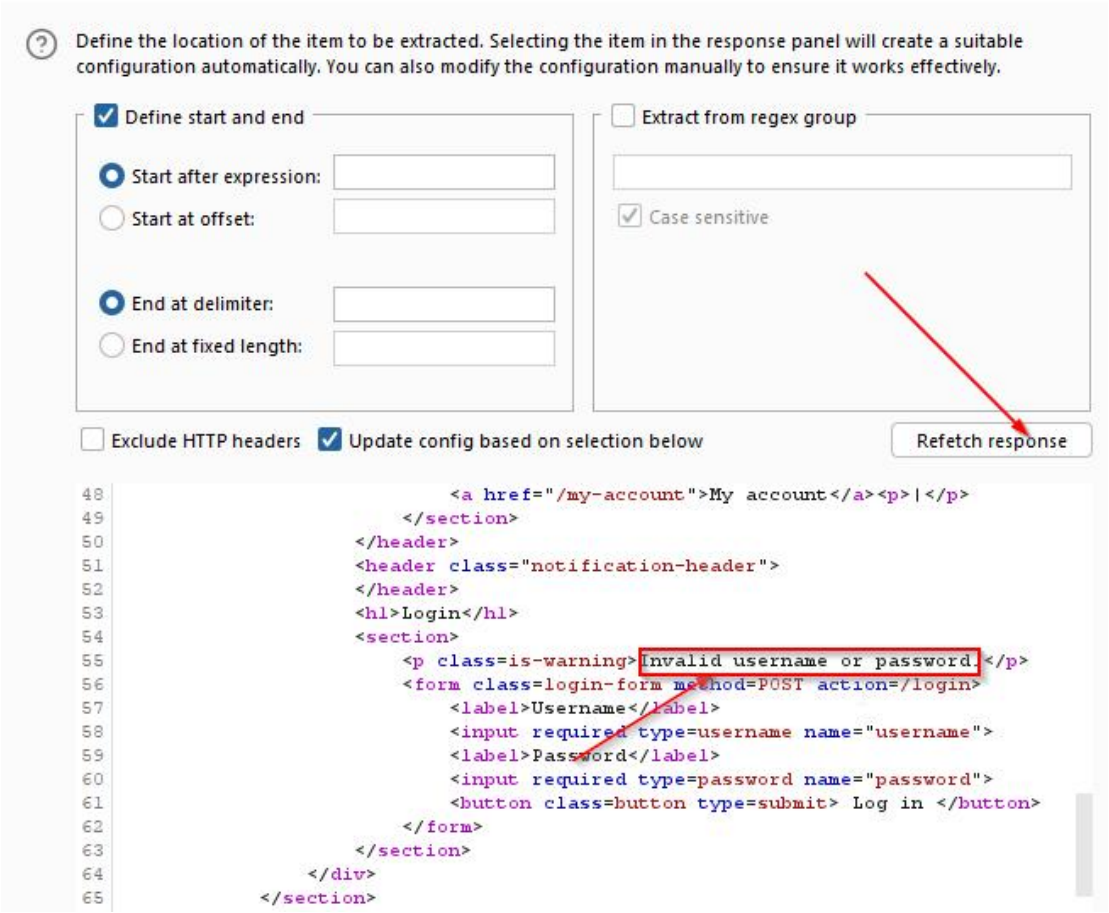
6.For the Payload 1 set the simple list and paste the usernames.



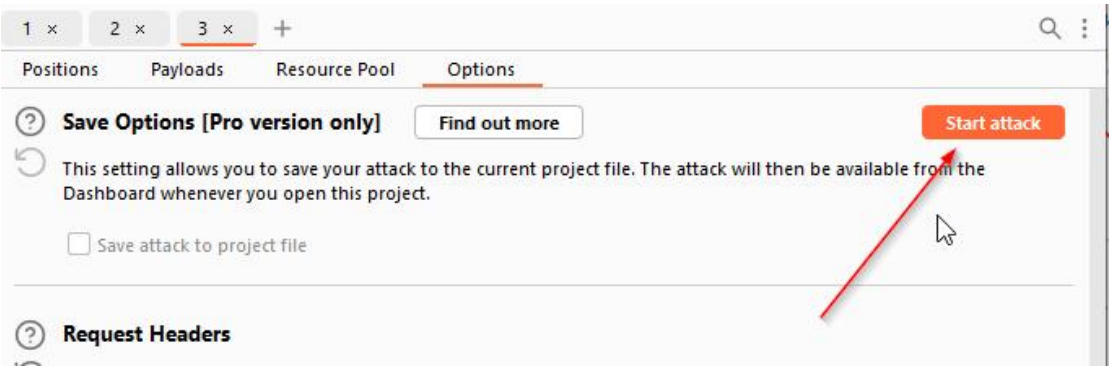
7.From the intruder click options



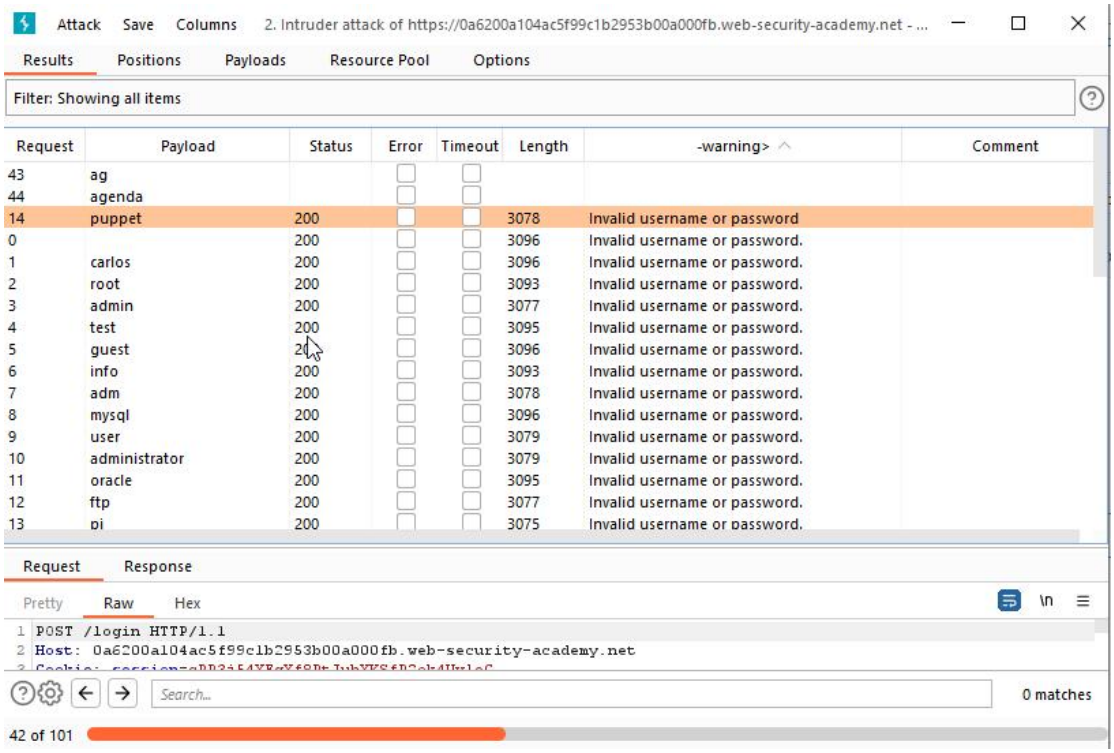
8.Add the Grep attack and click the fetch response and select the invalid username and password.



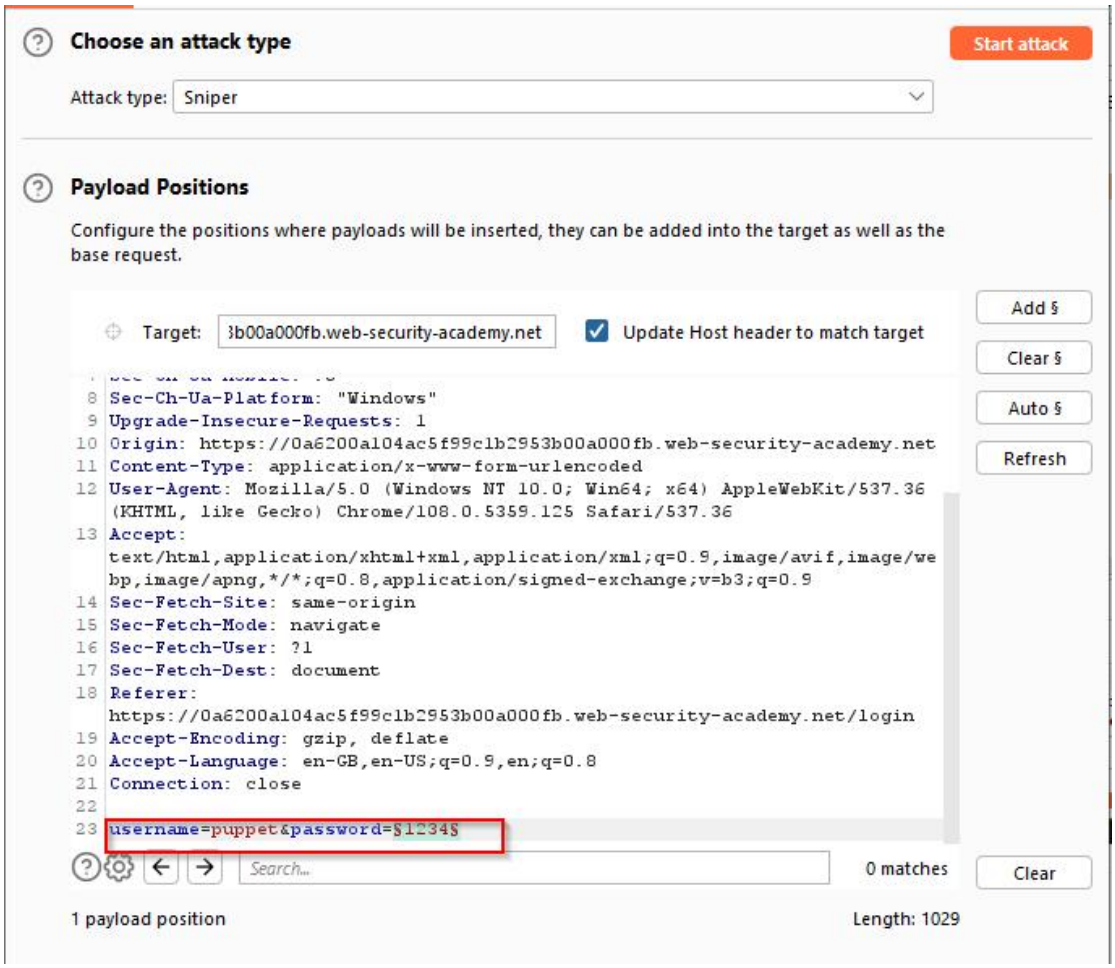
10. Now click the start attack.



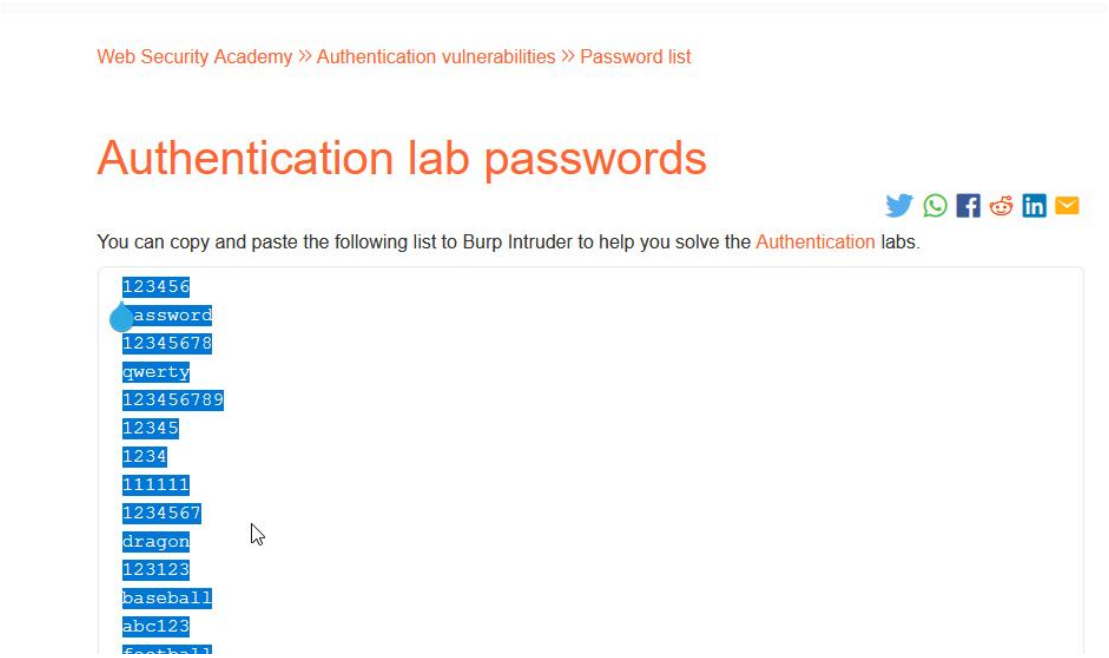
11.Now we have found out the username from the attack.



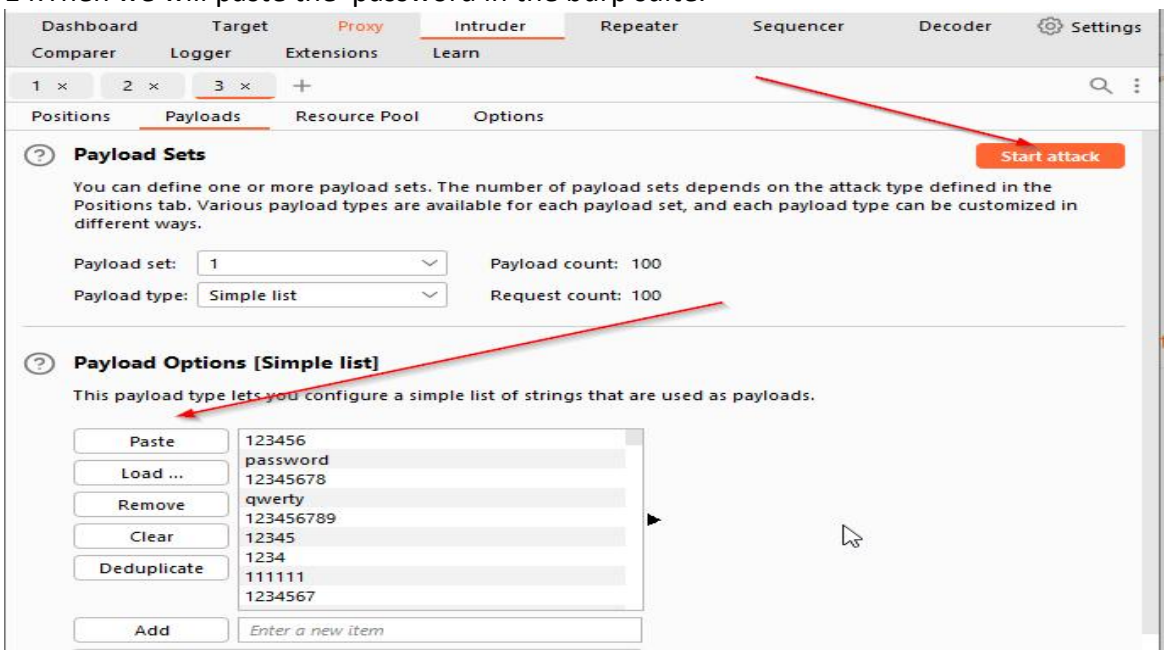
12.Now from the intruder we will change the username to the found username "puppet" and do a password attack.



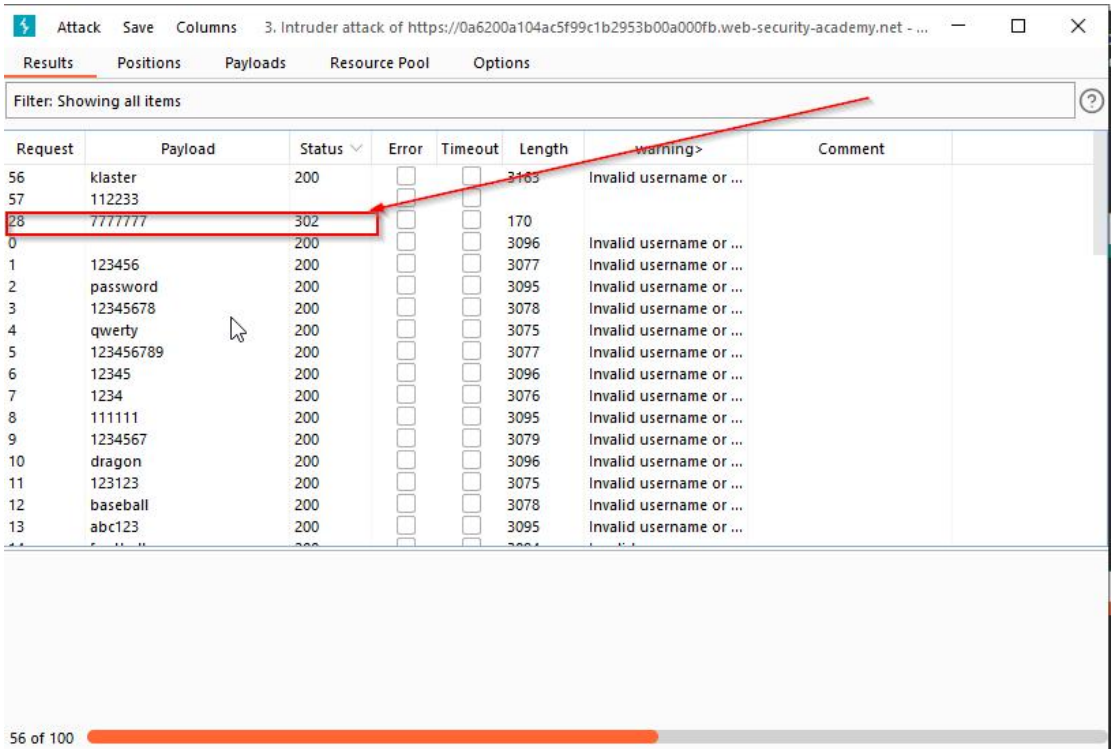
13.First we will copy the password from the passwords.



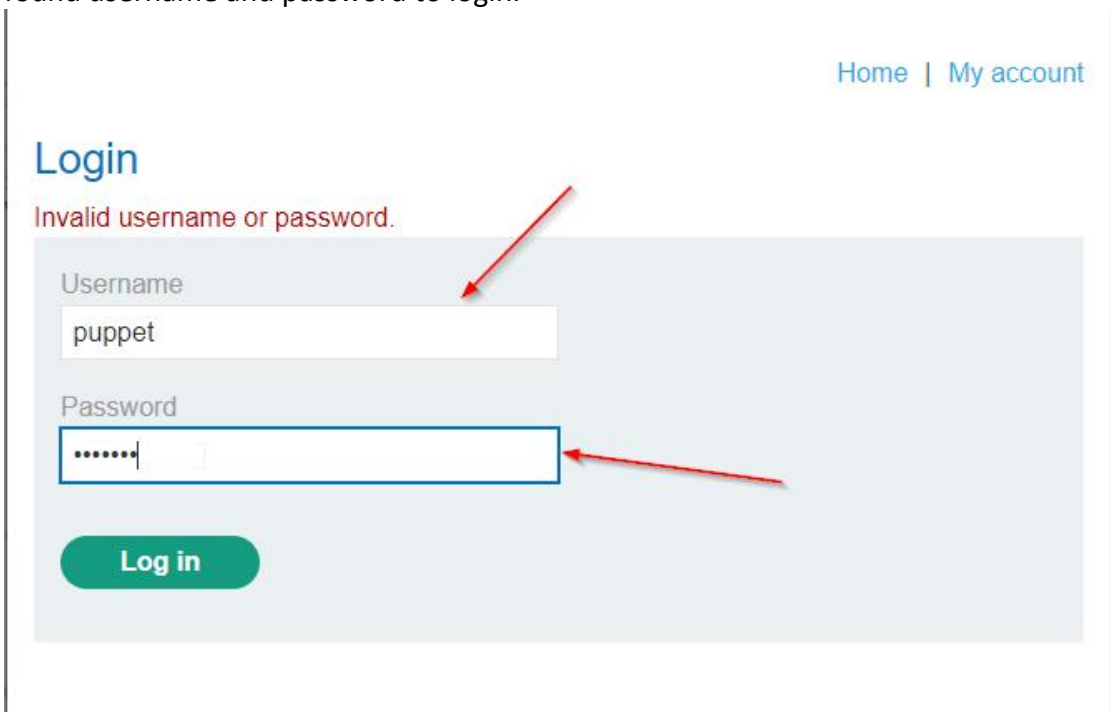
14.Then we will paste the password in the burp suite.



15.Then we will start the attack. And after the attack we will see that the request response for a password is 302 because a successful password will redirect to another page.



16.Now we have our username and password. We will go the login page and use the found username and password to login.



17.We will click login and the lab is solved.