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

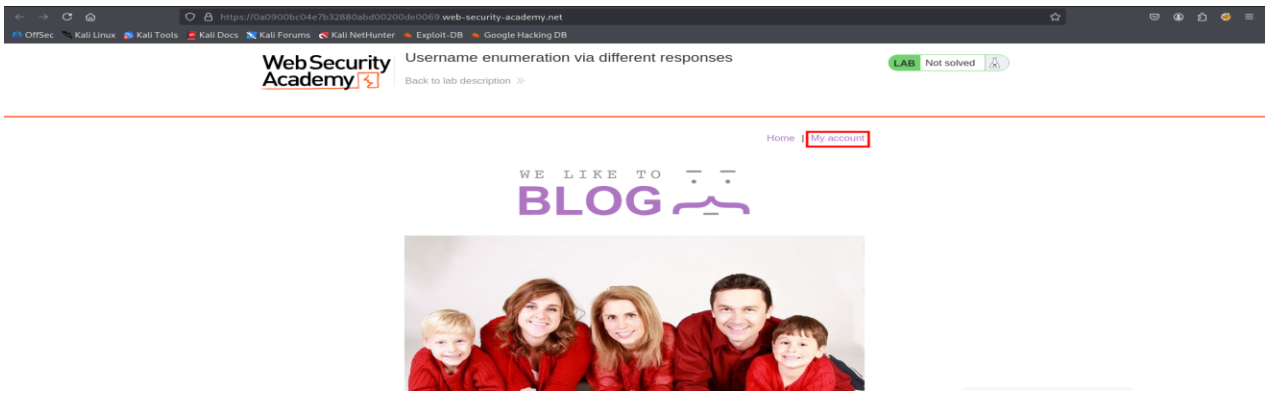
The objective of this assessment was to identify valid usernames by analyzing authentication response discrepancies and leverage the findings to gain unauthorized access.

Vulnerability Description

Authentication weakness

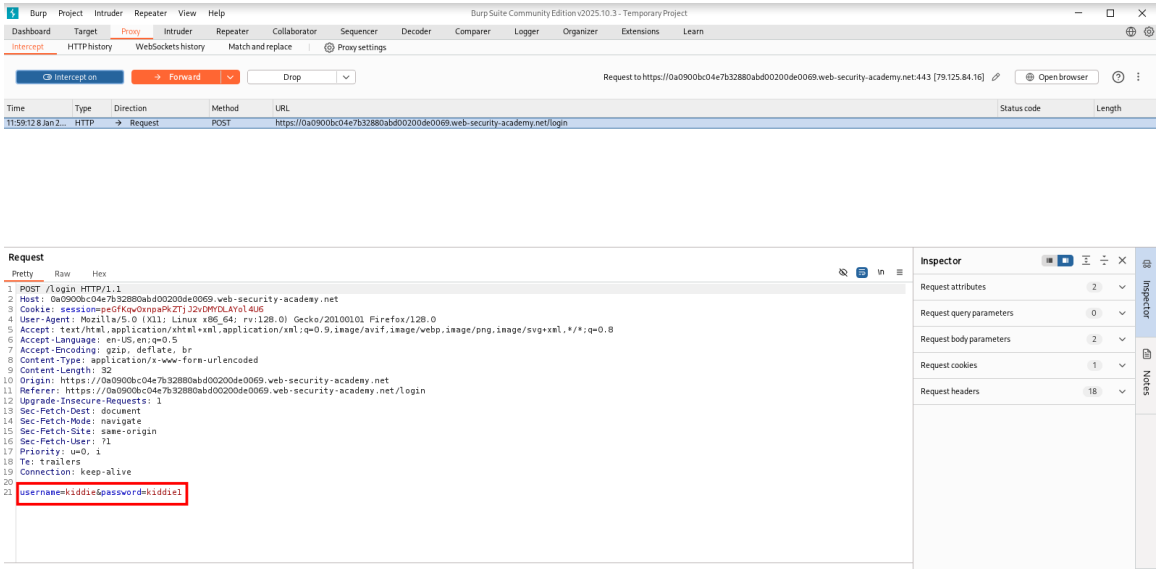
Approach

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



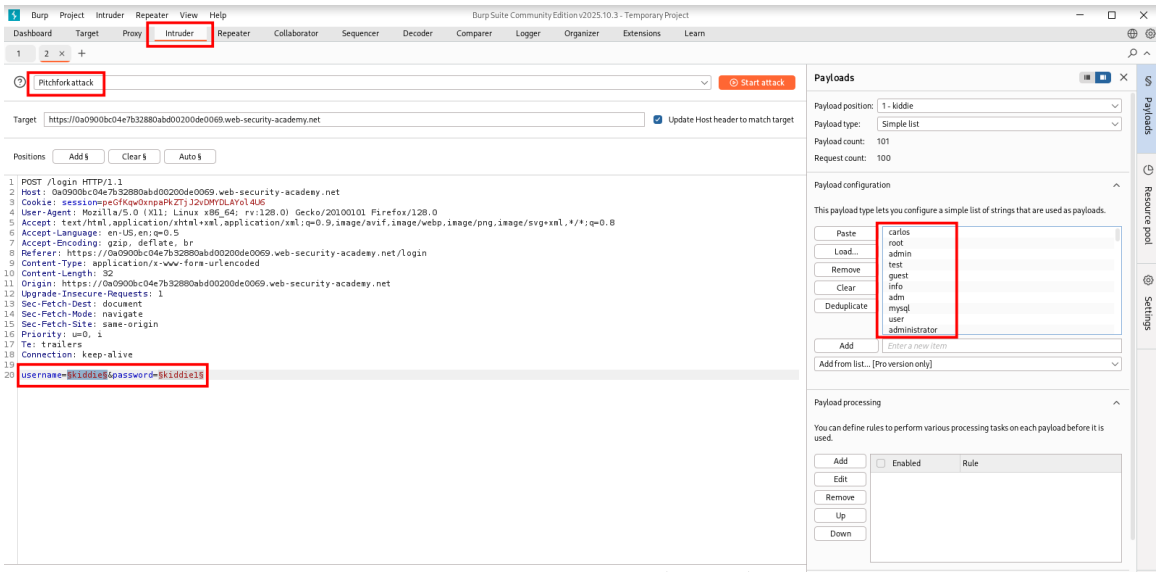
img: SS 1.0

- Intercepted authentication requests using Burp Suite.



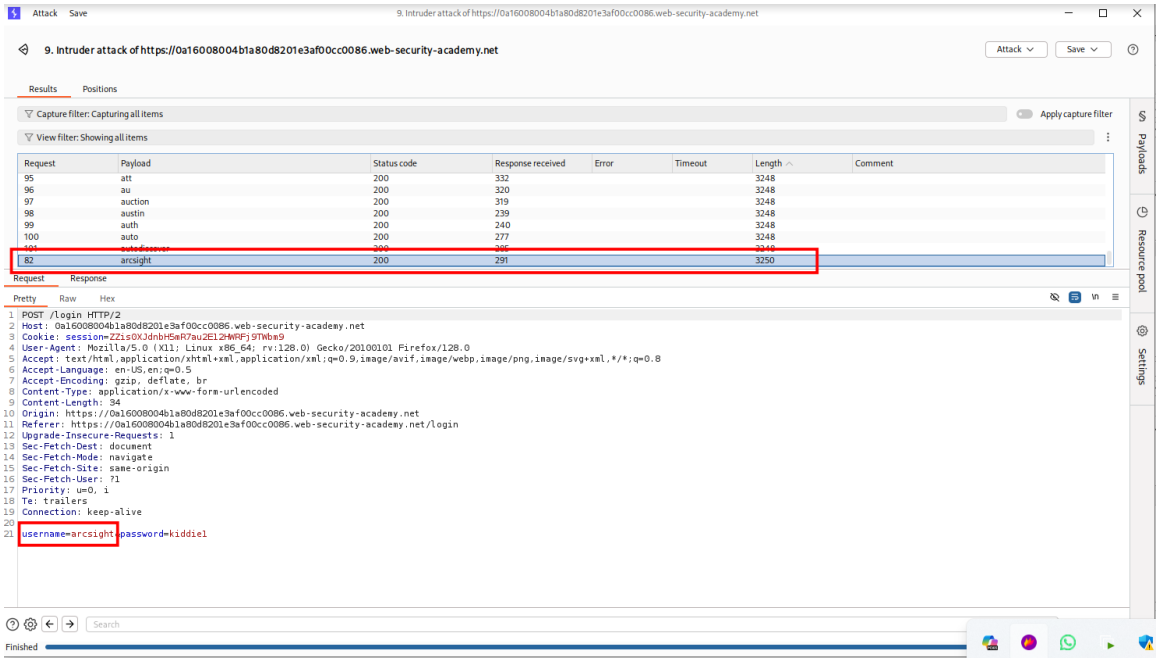
Img: SS 1.1

- Conducted username enumeration using Burp Intruder (Sniper).



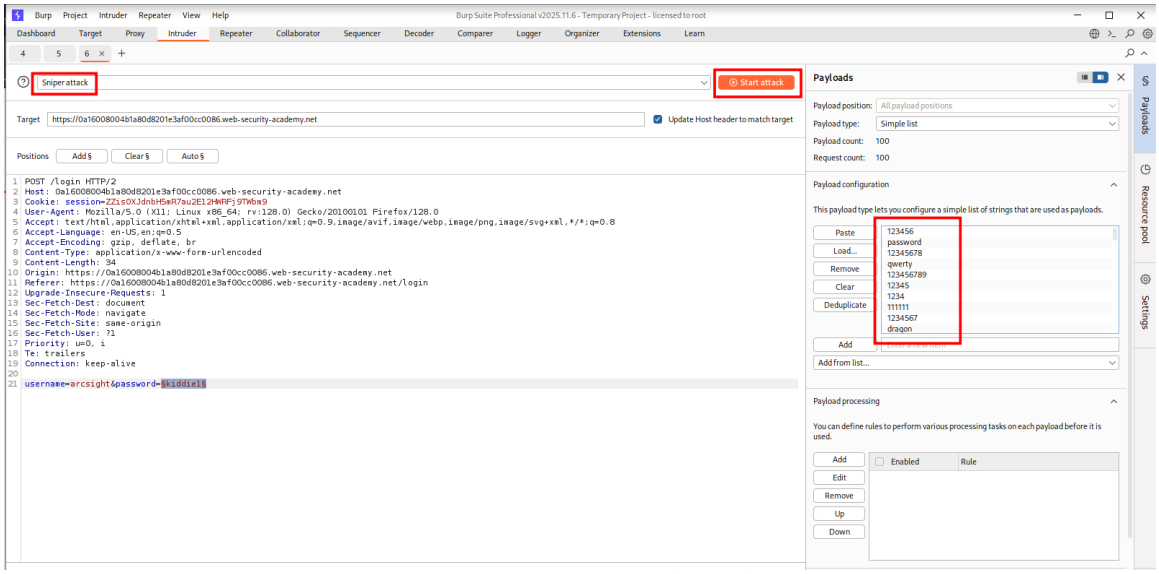
Img: SS 1.2

- Identified valid usernames through response length and behavior analysis.



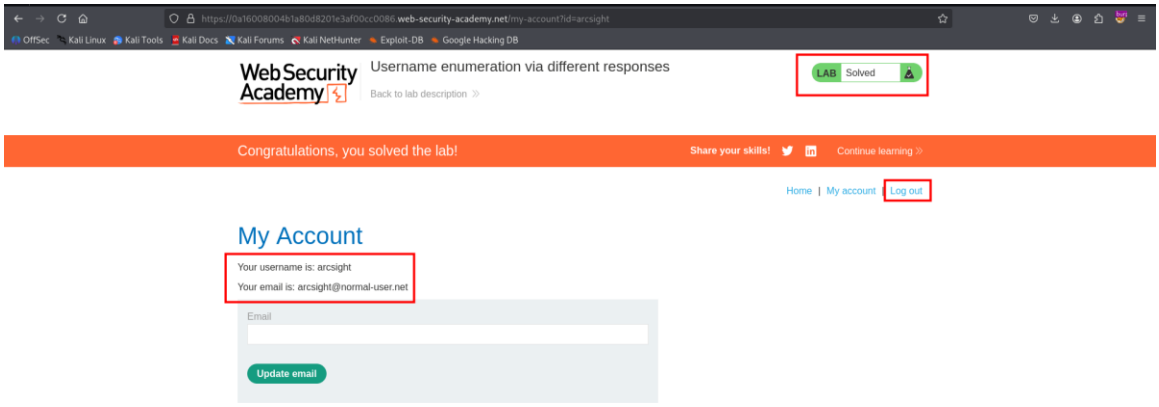
Img: SS 1.3

- 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)