

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

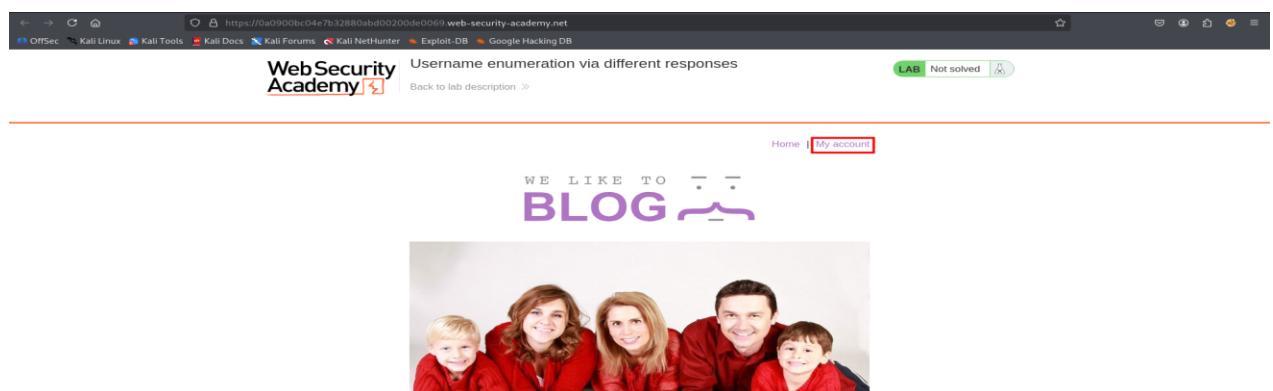
The objective of this assessment was to identify valid usernames by analyzing authentication response discrepancies and leverage the findings to gain unauthorized access.

Vulnerability Description

Authentication weakness

Approach

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



img: SS 1.0

- Intercepted authentication requests using Burp Suite.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A POST request is captured for the URL <https://0a0900bc04e7b32880abd00200de0069.web-security-academy.net/login>. The request body contains the payload: `username=kiddie&password=kiddie`. The 'Inspector' tab displays the request attributes, query parameters, body parameters, cookies, and headers.

Img: SS 1.1

- Conducted username enumeration using Burp Intruder (Sniper).

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Payloads' tab is open, showing a simple list of payloads: 'kiddie' and 'root'. The payload list also contains other users: 'carlos', 'root', 'admin', 'test', 'guest', 'info', 'adm', 'mysql', 'user', and 'administrator'. The 'Payload configuration' section allows for configuration of the payload list.

Img: SS 1.2

- Identified valid usernames through response length and behavior analysis.

The screenshot shows the OWASP ZAP Intruder tool interface. The title bar reads "9. Intruder attack of https://0a16008004b1a80d8201e3af00cc0086.web-security-academy.net". The main window displays a table of requests and their responses. A specific row is highlighted with a red box, showing a POST request to "/Login" with a status code of 200 and a response length of 3250. Below the table, the raw request and response are shown in a text editor. The raw request includes the URL and various headers. The raw response starts with "HTTP/1.1 200 OK". The bottom of the window shows a toolbar with icons for file operations and a status bar indicating "Finished".

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
95	att	200	331			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	avast	200	295			3248	
102	arcwright	200	291			3250	

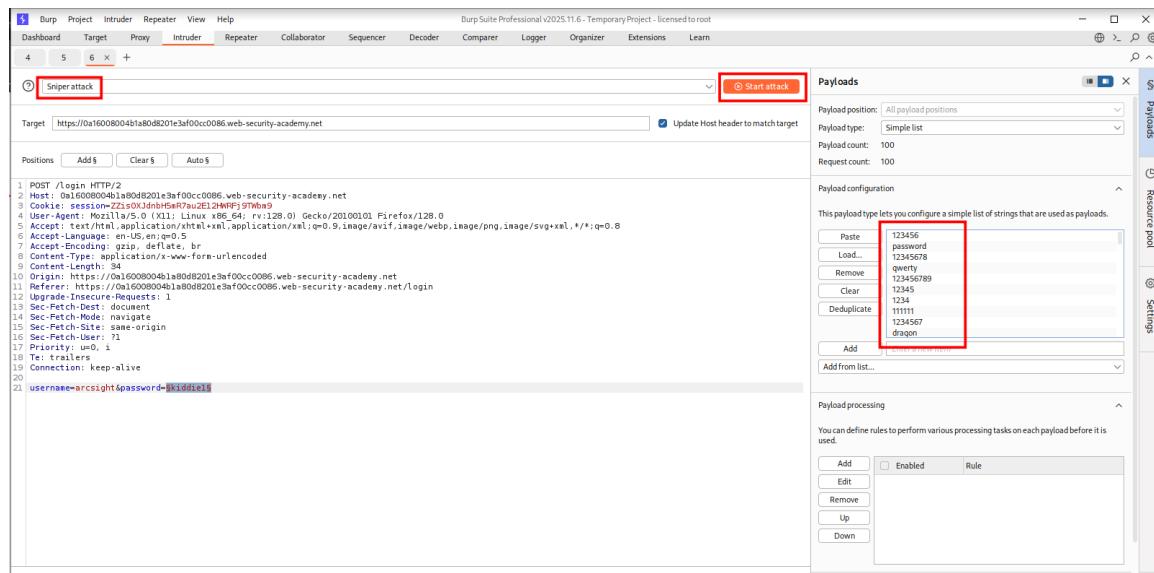
```

1 POST /Login HTTP/2
2 Host: 0a16008004b1a80d8201e3af00cc0086.web-security-academy.net
3 Cookie: session=Z2isOXJdnbb5wRau2E12WRFj9TWh9
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/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: 22
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=1
18 TEL: transfers
19 Connection: keep-alive
20
21 username=arcwright&password=kiddiel

```

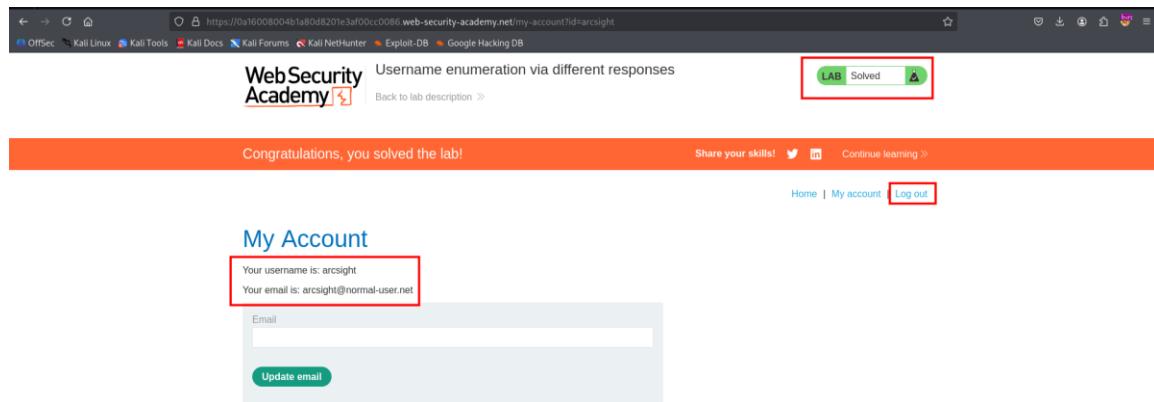
Img: SS 1.3

- 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)