Penetration Testing Report

Souvik Mondal

Lab Name

Password Reset Broken Logic

Objective

Exploit weaknesses in the password reset workflow to gain unauthorized access to a victim account by abusing broken validation logic.

Vulnerability Description

The application contains a broken password reset logic flaw within its authentication mechanism.

The password reset functionality fails to correctly validate and bind reset requests to the legitimate account owner, resulting in improper trust of user-controlled input.

Vulnerability Type

The application contains a broken password reset logic flaw within its authentication mechanism.

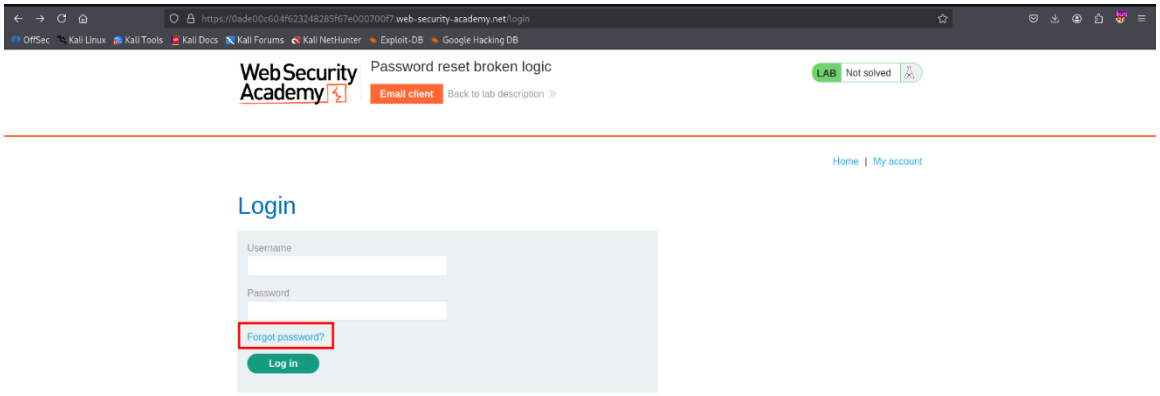
The password reset functionality fails to correctly validate and bind reset requests to the legitimate account owner, resulting in improper trust of user-controlled input.

Tools Used

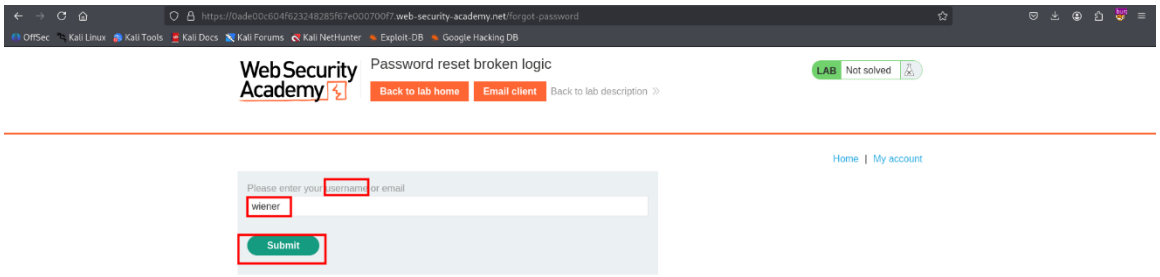
Burp Suite, Firefox Browser

Approach

1. Initiate the password reset process

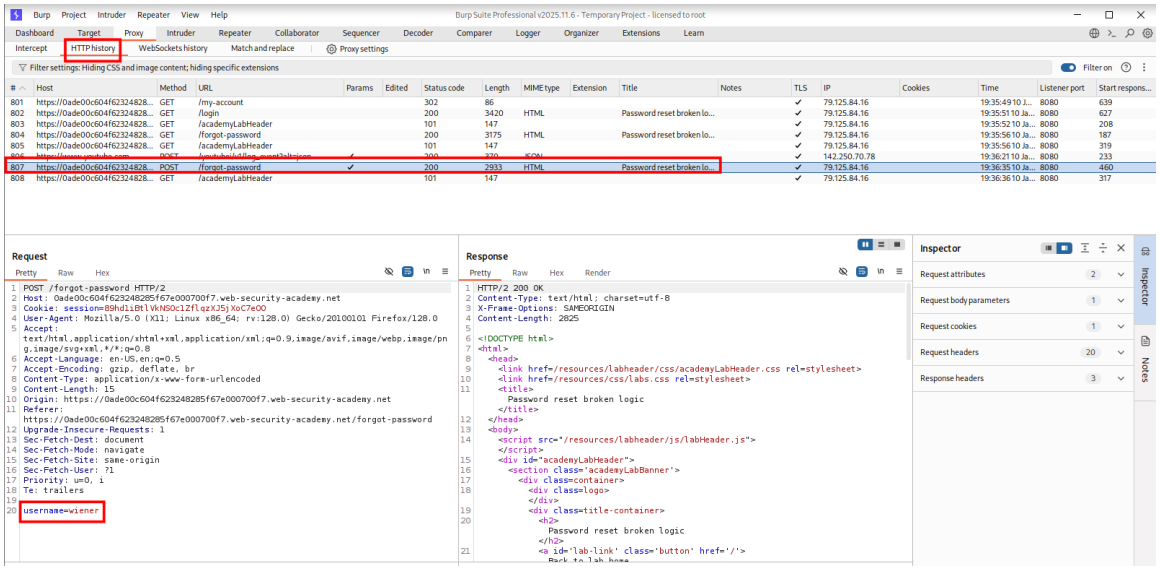


Img: SS 1.0



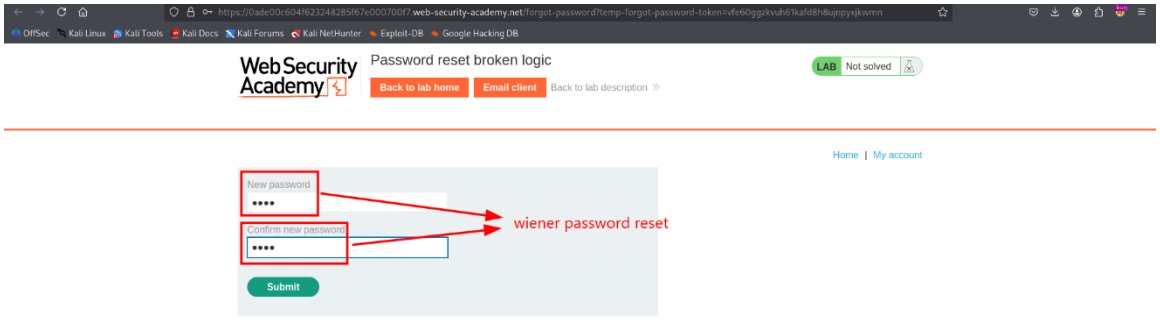
Img: SS 1.1

2. Intercept the reset request using Burp Suite

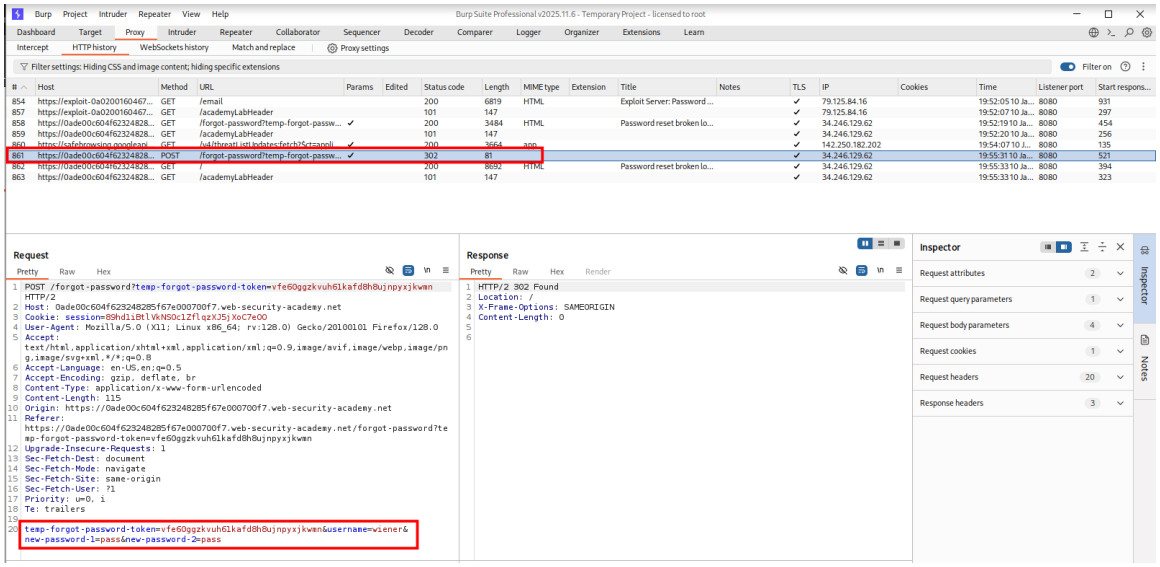


img: SS 1.2

3. Identify user-controllable parameters

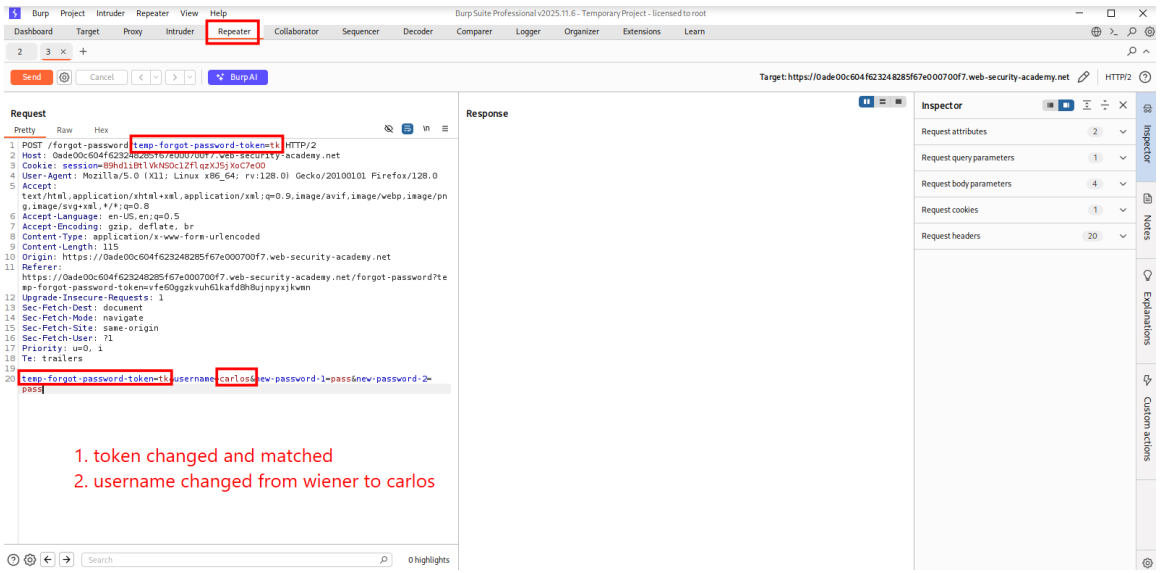


Img: SS 1.3



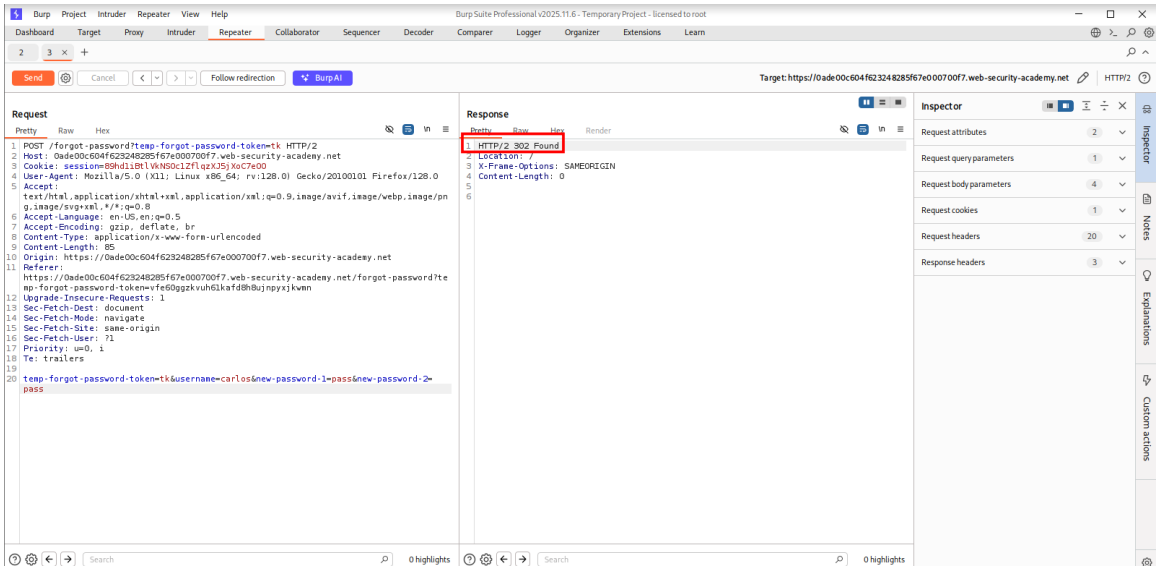
Img: SS 1.4

4. Modify logic-dependent values (token)



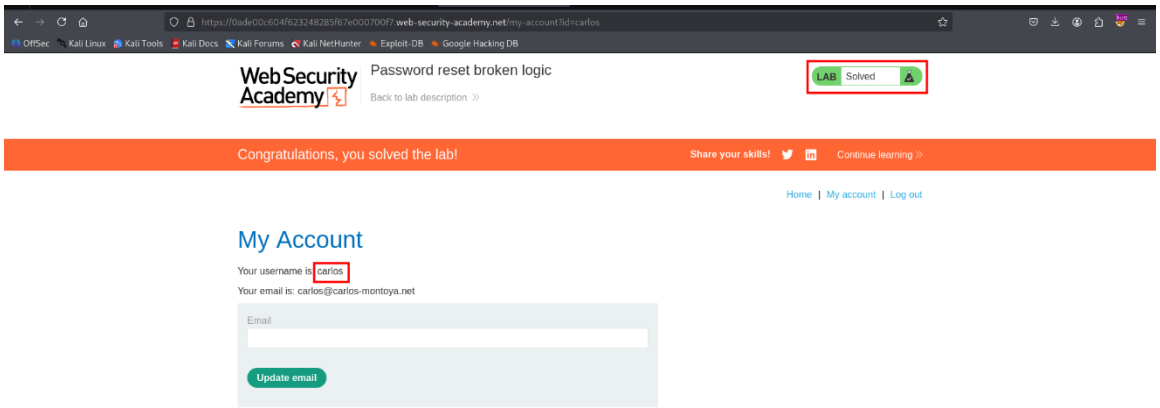
img: SS 1.5

5. Submit manipulated request



img : SS 1.6

6. Log in using the newly set password



img: SS 1.7

CVSS Vector

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

Severity

High

Impact

- Full account compromise

- Unauthorized access to sensitive data

- Potential lateral movement depending on privileges

- High business risk due to logic abuse

Key Findings

- The password reset mechanism failed to correctly associate reset actions with a specific user

- User-controlled parameters could be manipulated to target other accounts

- No effective server-side validation was enforced during the reset process

- This flaw allowed password reset for arbitrary users

Outcome

- Successfully reset the victim user’s password without authorization

- Gained full access to the target account

- Demonstrated a complete account takeover scenario due to logic abuse

Remediation

- Bind password reset tokens strictly to a specific user

- Enforce server-side validation of reset requests

- Use single-use, time-bound reset tokens

- Do not rely on client-controlled parameters for identity

- Implement robust logging and alerting for reset attempts