

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.

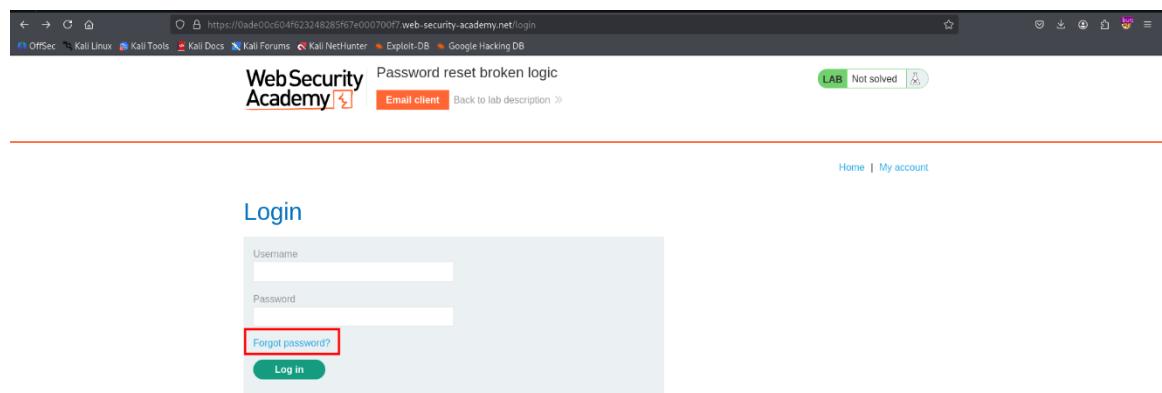
The password reset functionality fails to correctly validate and bind reset requests to the legitimate account owner, resulting in improper trust of user-controlled input.

Tools Used

Burp Suite, Firefox Browser

Approach

1. Initiate the password reset process



The screenshot shows a web browser window with the URL <https://ade00c604f623248285f67e000700f7.web-security-academy.net/login>. The page title is "Password reset broken logic". At the top right, there is a green button labeled "LAB" and a status message "Not solved". Below the title, there are two input fields for "Username" and "Password", and a red-bordered "Forgot password?" link. A green "Log in" button is at the bottom. The browser's address bar shows the full URL, and the top navigation bar includes links for OffSec, Kali Linux, Kali Tools, Kali Deco, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB.

Img: SS 1.0

WebSecurity Academy

Password reset broken logic

LAB Not solved

Back to lab home Email client Back to lab description >

Please enter your or email
wiener

Submit

Img: SS 1.1

2. Intercept the reset request using Burp Suite

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response...
801	https://0xde0c04f623248285f67e000700f7...	GET	/my-account			302	86			Password reset broken lo...	✓	79.125.84.16			19:35:49 10.J...	8080	639
802	https://0xde0c04f623248285f67e000700f7...	POST	/forgot-password	username=wiener		200	3420	HTML			✓	79.125.84.16			19:35:51 10.J...	8080	627
803	https://0xde0c04f623248285f67e000700f7...	GET	/academyLabHeader			101	147				✓	79.125.84.16			19:35:52 10.J...	8080	208
804	https://0xde0c04f623248285f67e000700f7...	GET	/forgot-password			200	3175	HTML		Password reset broken lo...	✓	79.125.84.16			19:35:56 10.J...	8080	187
805	https://0xde0c04f623248285f67e000700f7...	GET	/academyLabHeader			101	147				✓	79.125.84.16			19:35:56 10.J...	8080	319
806	https://0xde0c04f623248285f67e000700f7...	POST	/forgot-password	username=wiener		200	230	JSON			✓	142.250.70.78			19:36:21 10.J...	8080	233
807	https://0xde0c04f623248285f67e000700f7...	POST	/forgot-password	username=wiener		200	2933	HTML		Password reset broken lo...	✓	79.125.84.16			19:36:35 10.J...	8080	460
808	https://0xde0c04f623248285f67e000700f7...	GET	/academyLabHeader			101	147				✓	79.125.84.16			19:36:36 10.J...	8080	317

img: SS 1.2

3. Identify user-controllable parameters



Img: SS 1.3

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start respond...
854	https://exploit-0x0200f6467...	GET	/email			200	6819	HTML		Exploit Server: Password ...		✓	79.125.84.16		19:52:49 10.Ju...	8080	931
857	https://exploit-0x0200f6467...	GET	/academyLabHeader			101	147					✓	79.125.84.16		19:52:07 10.Ju...	8080	297
858	https://0ade00c604f6232482...	GET	/forgot-password?temp-forgot-passw...			200	3484	HTML		Password reset broken lo...		✓	34.246.129.62		19:52:19 10.Ju...	8080	454
859	https://0ade00c604f6232482...	GET	/academyLabHeader			101	147					✓	34.246.129.62		19:52:20 10.Ju...	8080	256
860	https://0ade00c604f6232482...	GET	/academyLabHeader			101	147					✓	142.250.182.202		19:54:07 10.Ju...	8080	135
861	https://0ade00c604f6232482...	GET	/forgot-password?temp-forgot-passw...			200	35	HTML				✓	34.246.129.62		19:53:59 10.Ju...	8080	521
862	https://0ade00c604f6232482...	GET	/forgot-password?temp-forgot-passw...			200	8692	HTML		Password reset broken lo...		✓	34.246.129.62		19:53:33 10.Ju...	8080	394
863	https://0ade00c604f6232482...	GET	/academyLabHeader			101	147					✓	34.246.129.62		19:53:33 10.Ju...	8080	323

Img: SS 1.4

4. Modify logic-dependent values (token)

The screenshot shows the Burp Suite Professional interface. The 'Repeater' tab is selected. In the 'Request' pane, a POST request is displayed with several parameters highlighted in red:

- temp-forgot-password-token=tk
- username=carlos
- new-password-l=pass&new-password-2=pass

The 'Response' pane shows the server's response:

```
HTTP/2.0 302 Found
Location: /
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

The 'Inspector' pane on the right lists the request attributes, query parameters, body parameters, cookies, and headers.

Notes:

1. token changed and matched
2. username changed from wiener to carlos

img: SS 1.5

5. Submit manipulated request

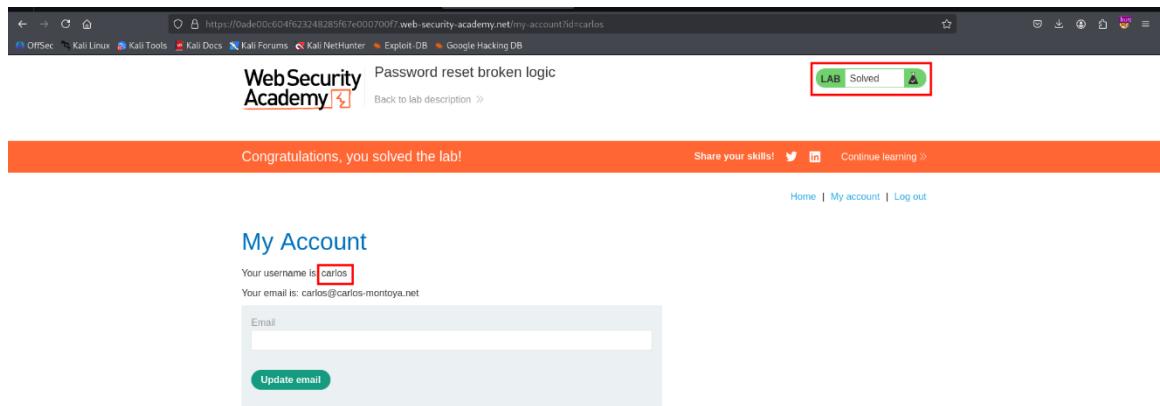
The screenshot shows the Burp Suite Professional interface. The 'Repeater' tab is selected. The 'Request' pane contains the same manipulated POST request as in the previous screenshot. The 'Response' pane now displays the successful response:

```
HTTP/2.0 302 Found
Location: /
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

The 'Inspector' pane on the right lists the response headers.

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