Authentication Bypass – Lab Report

Submitted By:
Name: Arsalan Khan
Position/Role: Internee
Date: August 10, 2025

Platform:
PortSwigger Labs

Objective:
To understand and exploit authentication bypass vulnerabilities in web applications, learning various techniques attackers use to circumvent login mechanisms and gain unauthorized access.

Tools Used:

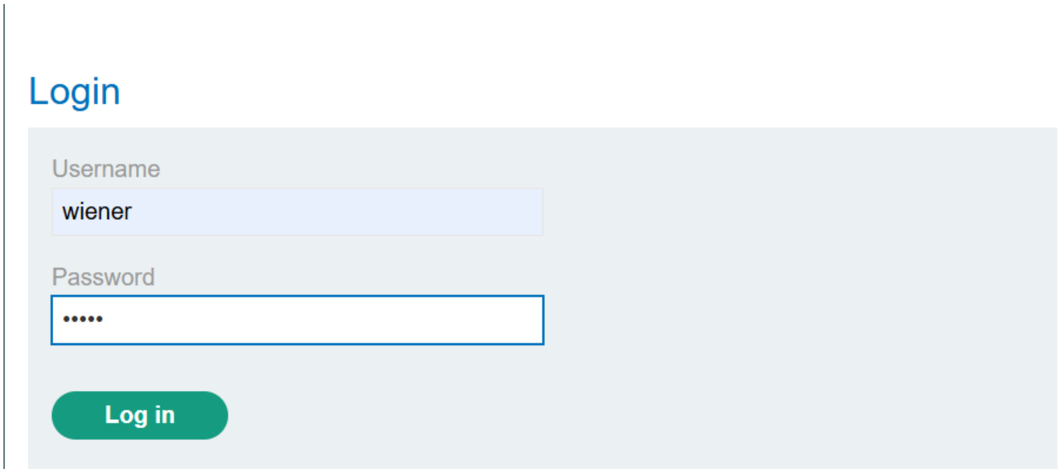
- Burp Suite
- Web Browser Developer Tools

Lab: 2FA Simple Bypass

Description:
This lab demonstrates a two-factor authentication (2FA) bypass vulnerability. Although 2FA is implemented, the application fails to properly enforce the second factor. By manipulating the URL, an attacker who has valid login credentials can bypass the 2FA verification step and access a victim's account.

Steps Performed:

1. Accessed the lab and logged in using the provided credentials for user `wiener:peter`.

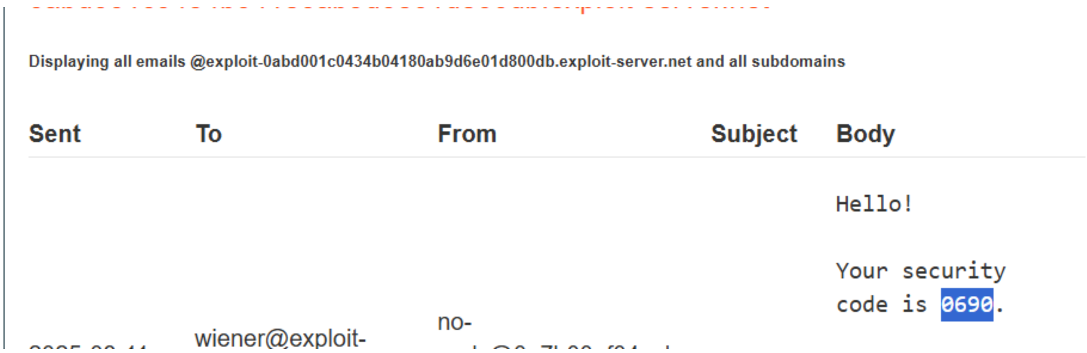


Login

Username: wiener

Password: •••••

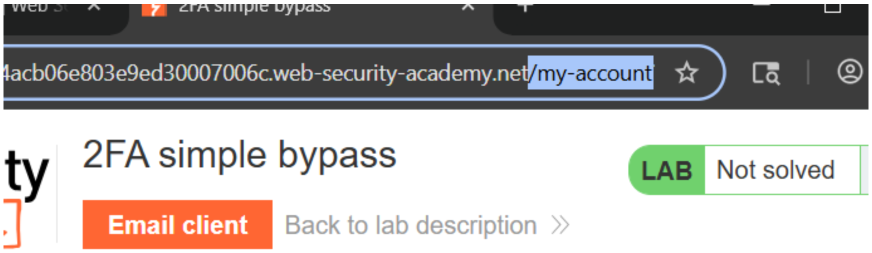
2. Upon successful login, received the 2FA verification code via the in-lab email client and completed the 2FA process.



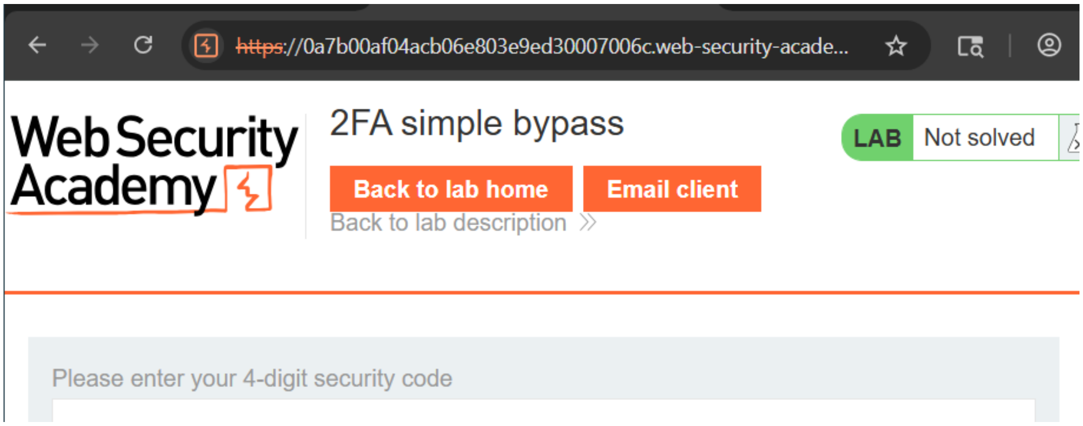
Displaying all emails @exploit-0abd001c0434b04180ab9d6e01d800db.exploit-server.net and all subdomains

Sent	To	From	Subject	Body
	wiener@exploit-	no-		Hello! Your security code is 0690.

3. Navigated to the account page and noted the URL (`/my-account`).

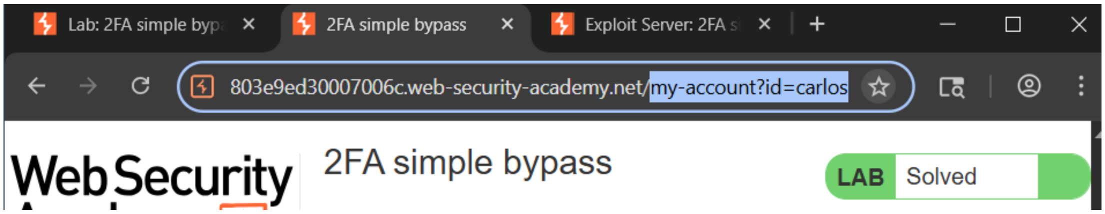


4. Logged out from the current session.
5. Logged in again, this time using the victim's credentials (`carlos:montoya`).

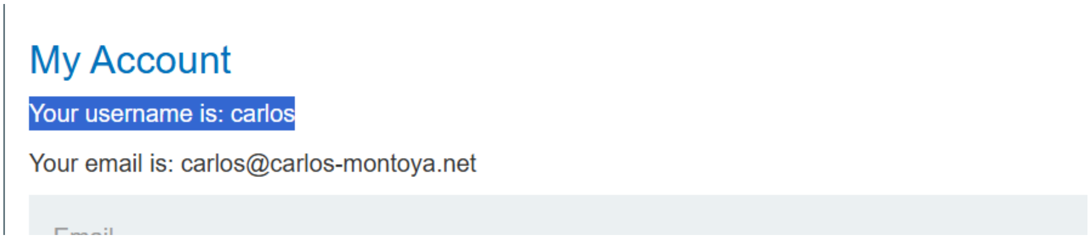


Please enter your 4-digit security code

6. When prompted for the 2FA code, instead of submitting a code, manually changed the URL in the browser to `/my-account`.



7. The victim’s account page loaded without requiring the 2FA verification, confirming the bypass.
8. Lab solved.


My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Vulnerability:

Two-Factor Authentication Bypass via Insecure URL Access
The application does not enforce 2FA properly and allows direct URL access to authenticated pages without verifying the second factor, letting attackers bypass 2FA after submitting valid credentials.

Mitigation:

- Enforce 2FA verification before granting access to any authenticated resources.
- Implement server-side checks to ensure 2FA has been successfully completed before allowing access to sensitive pages.
- Use secure session management that flags whether 2FA is verified for each session.
- Conduct regular security testing on authentication flows.