

Authentication Vulnerability Report

Lab: Password Reset Broken
Logic

Platform: PortSwigger Web
Security Academy

Tester: Praisegod Aliyu

Date: 19 January 2026

Objective

The objective of this lab was to identify a logic flaw in the password reset functionality that allows unauthorized password reset without proper verification.

Vulnerability Type

Authentication Logic Flaw – Password Reset Broken Logic

OWASP Top 10 Category: A07 – Identification and Authentication Failures

Target Description

The target application implements a password reset feature that allows users to reset their passwords by submitting a reset request.

Vulnerability Discovery

Testing revealed that the password reset mechanism contained a logic flaw that allowed the password of a user account to be reset without correctly verifying the identity of the account owner.

Exploitation Steps

Initiated the password reset process for a user account.

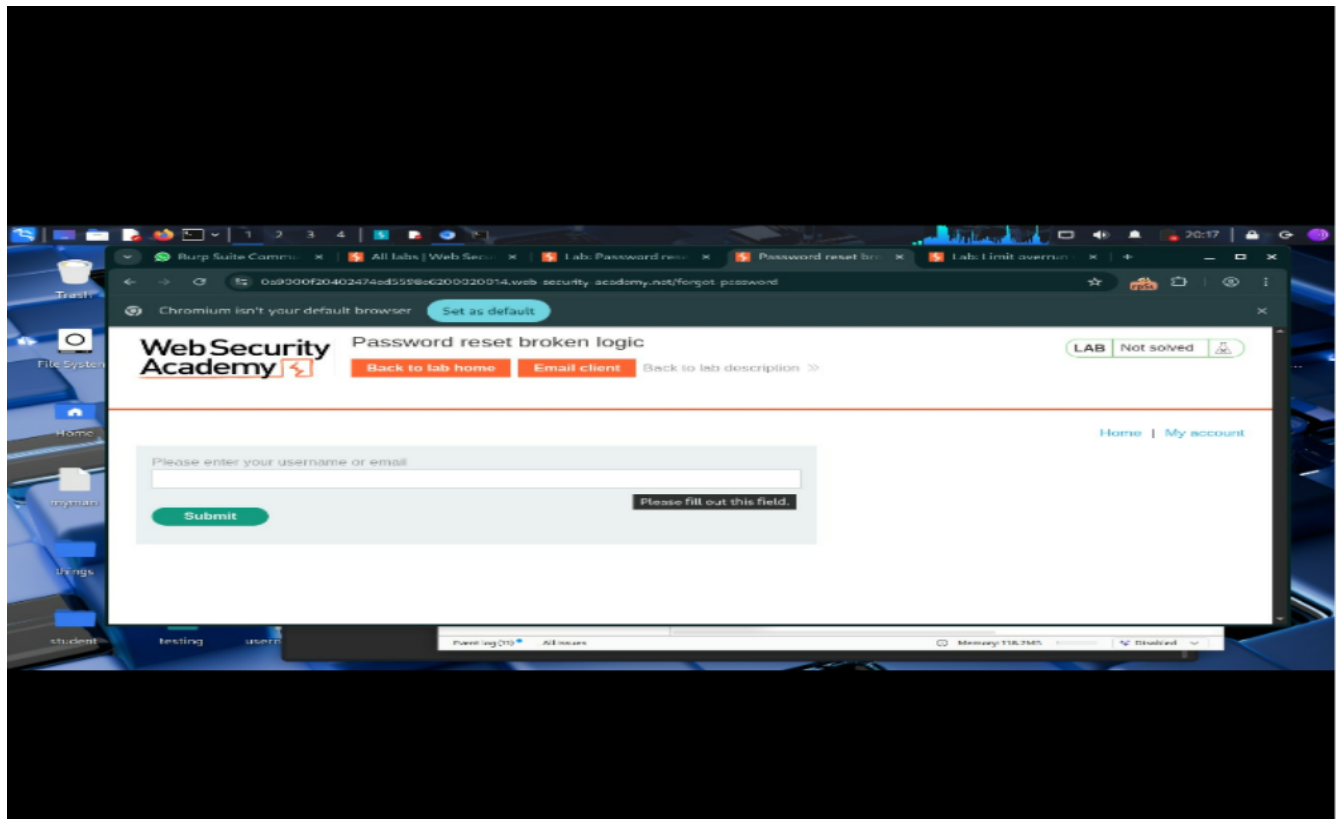
Intercepted the password reset request using Burp Suite.

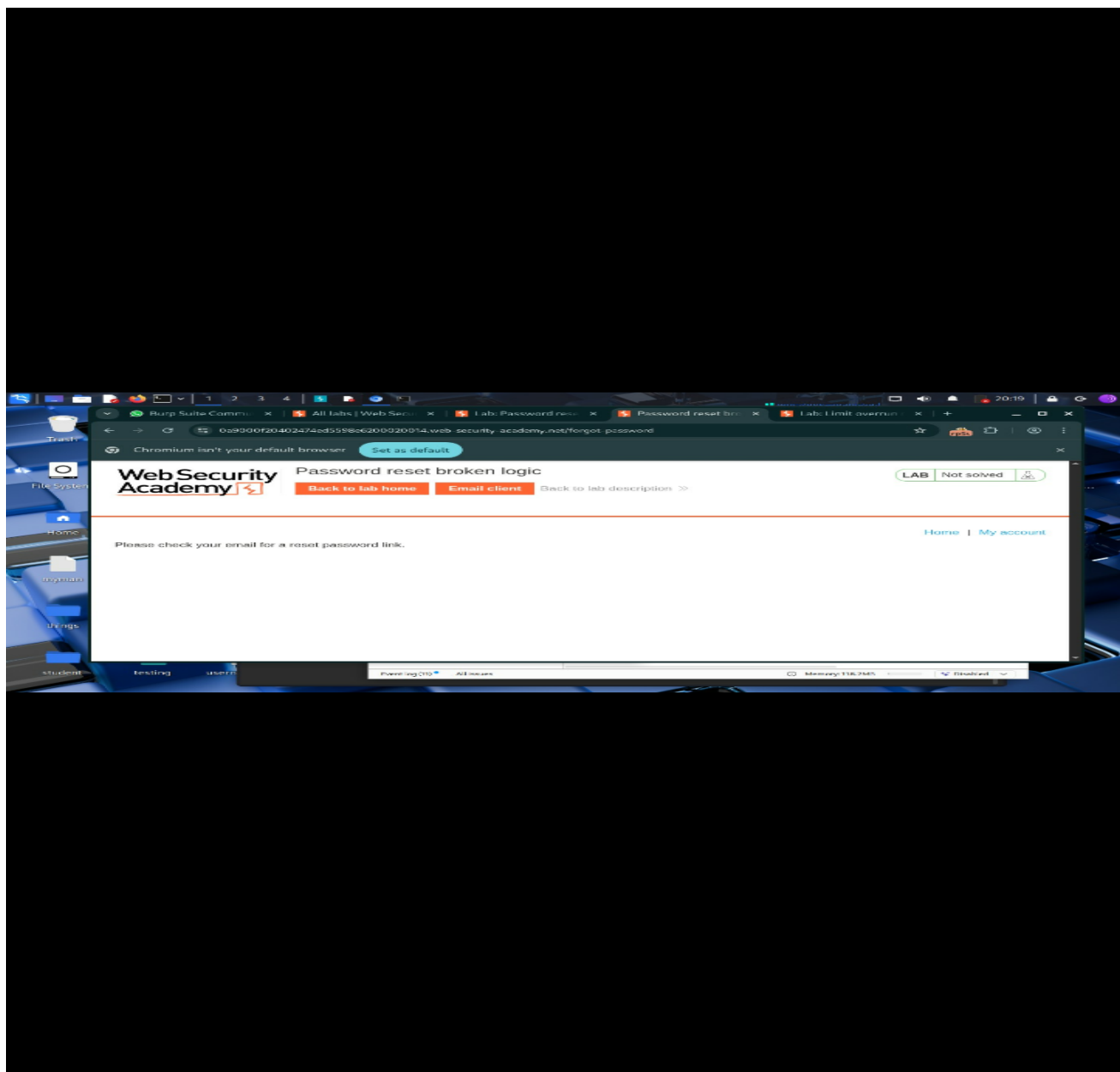
Modified the request parameters to bypass the intended verification logic.

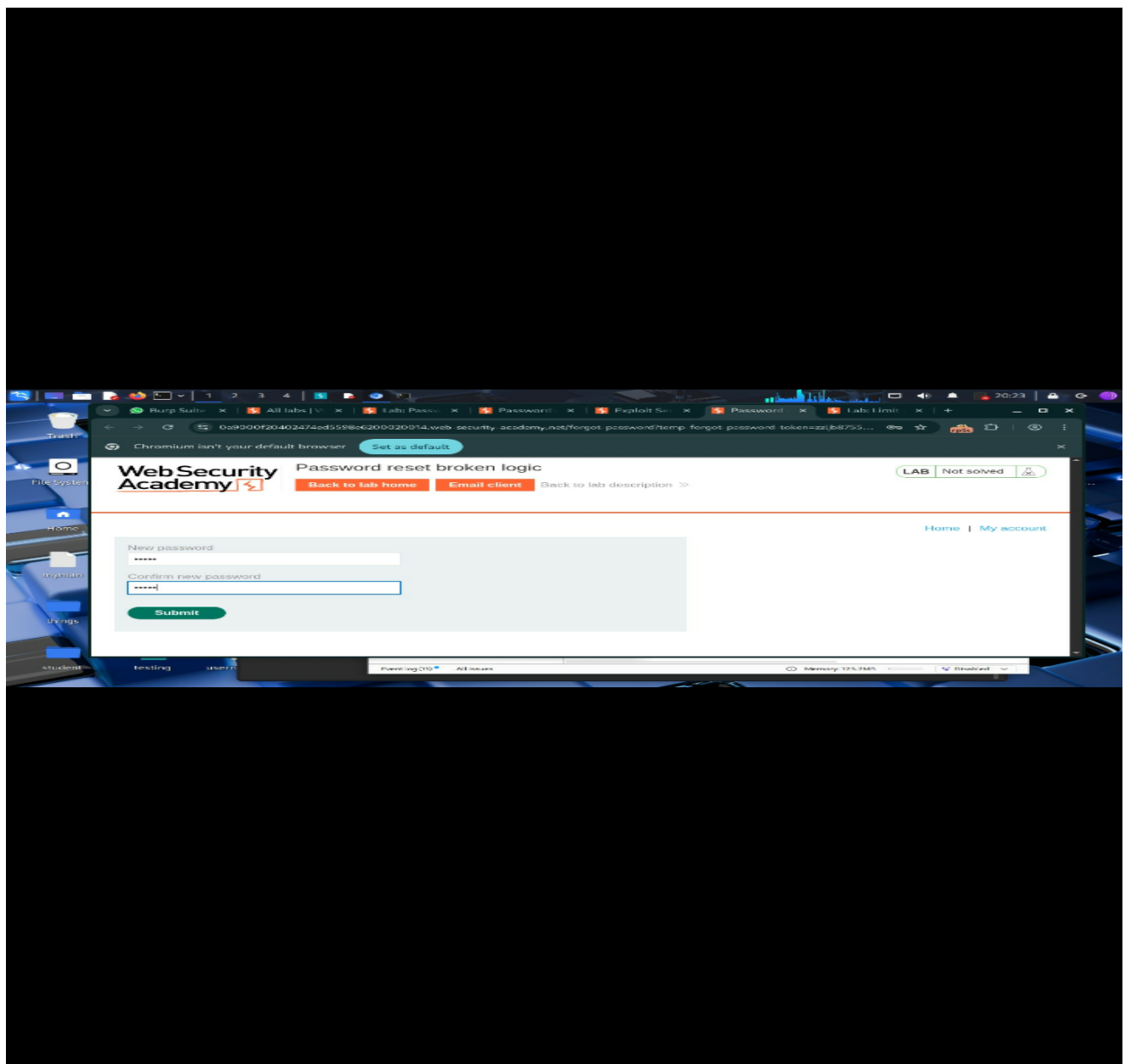
Successfully reset the password and gained access to the user account.

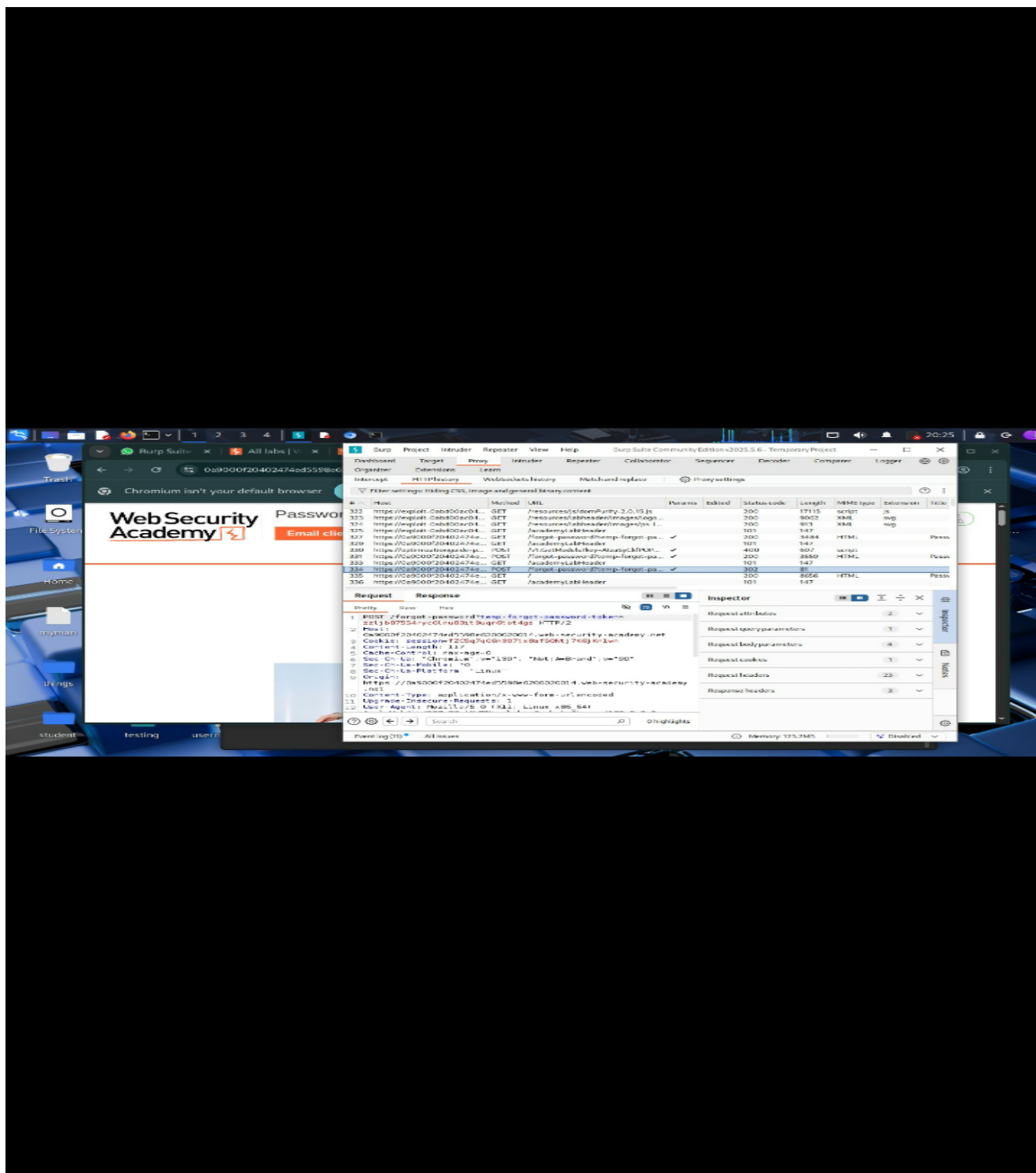
Proof of Exploitation

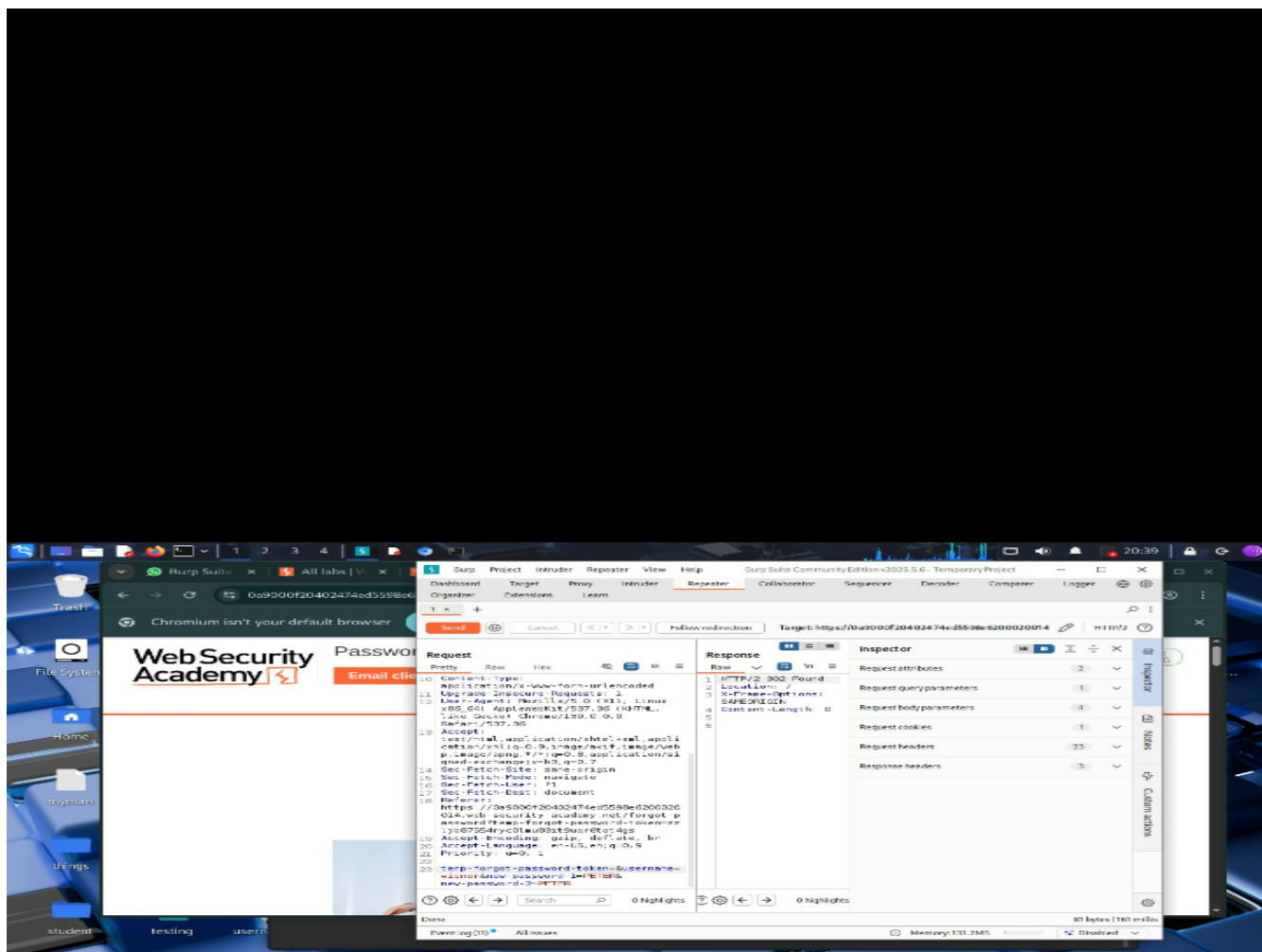
The screenshots below demonstrate successful password reset and account access without proper verification, confirming a broken password reset logic.

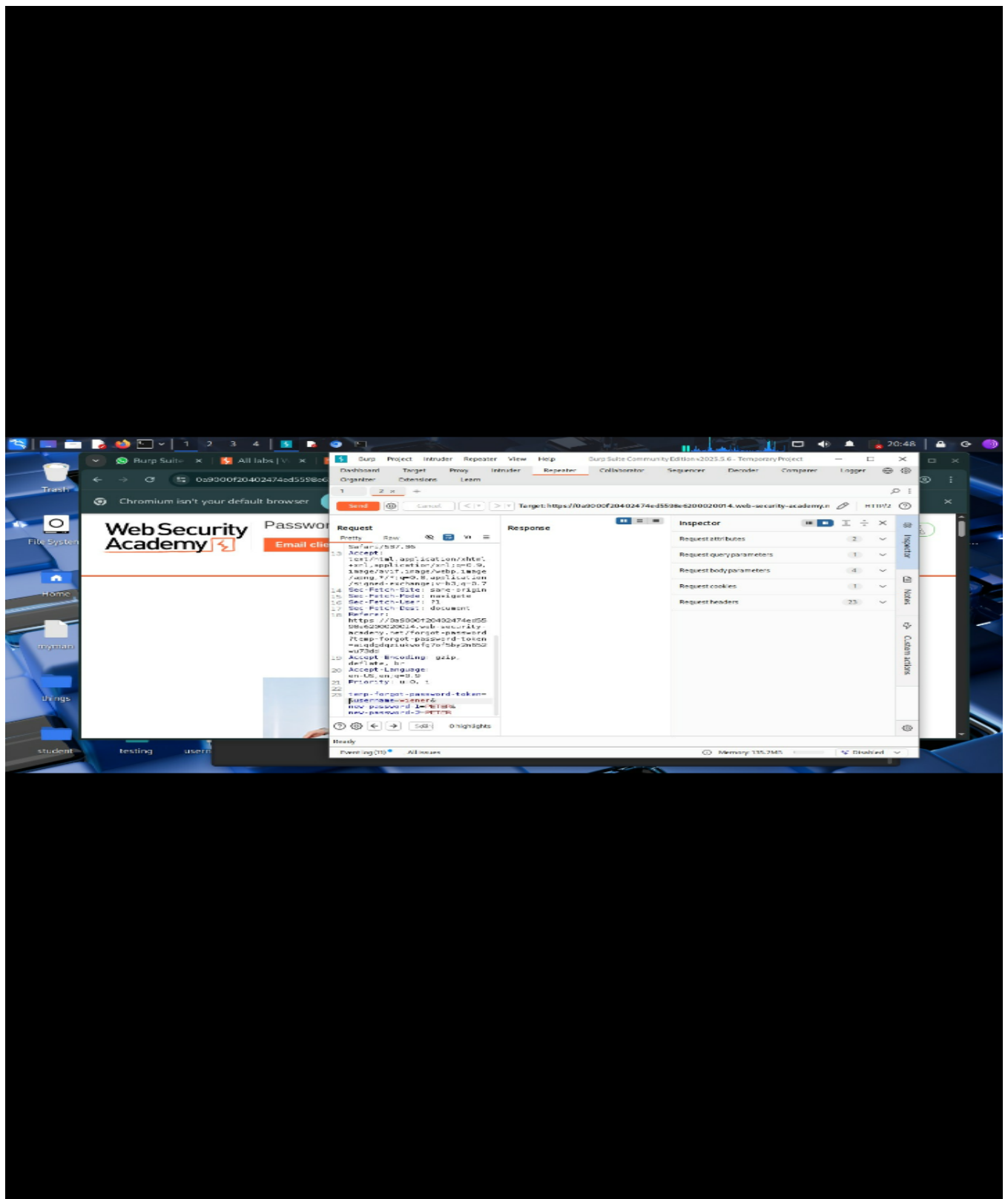


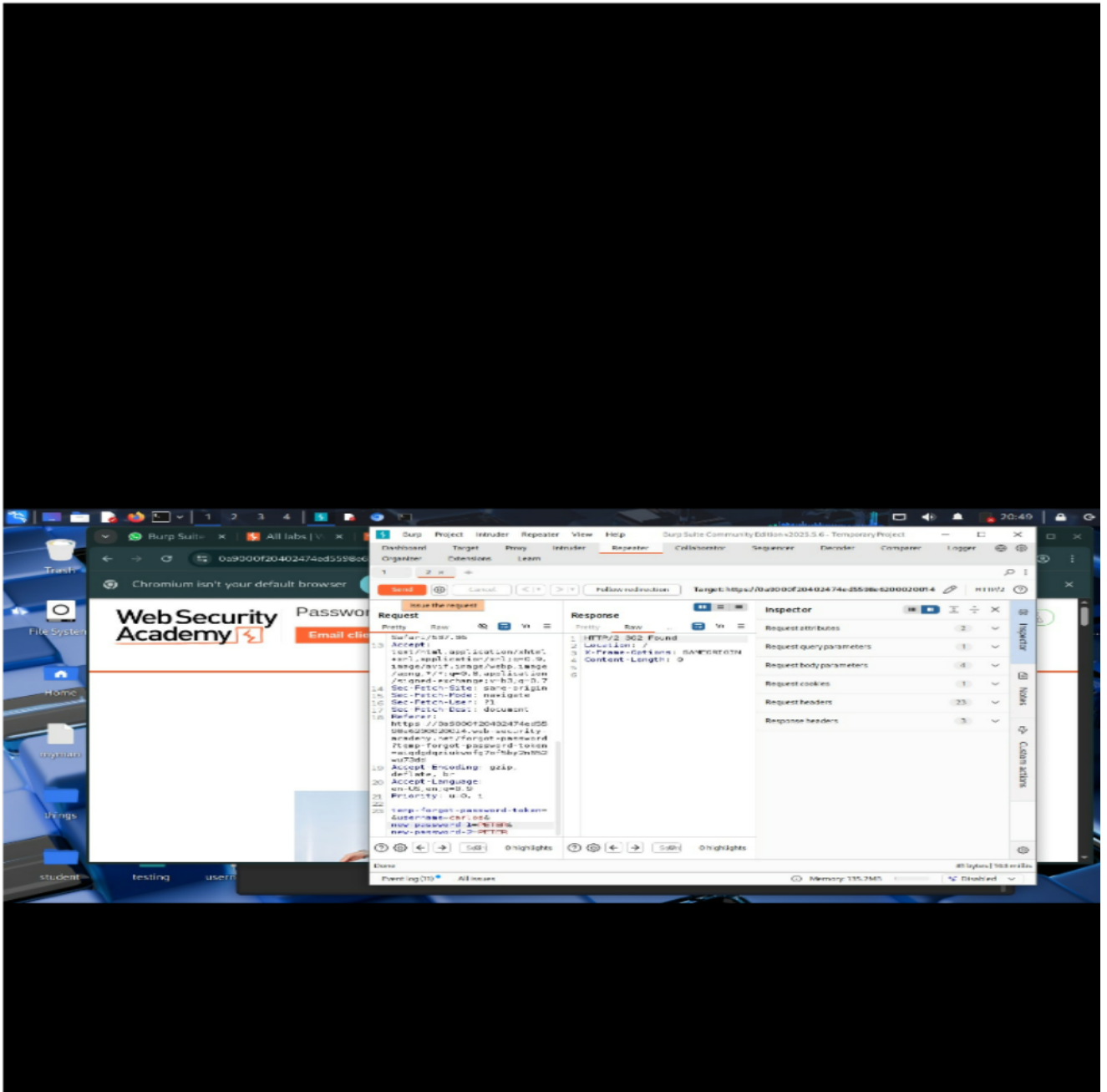


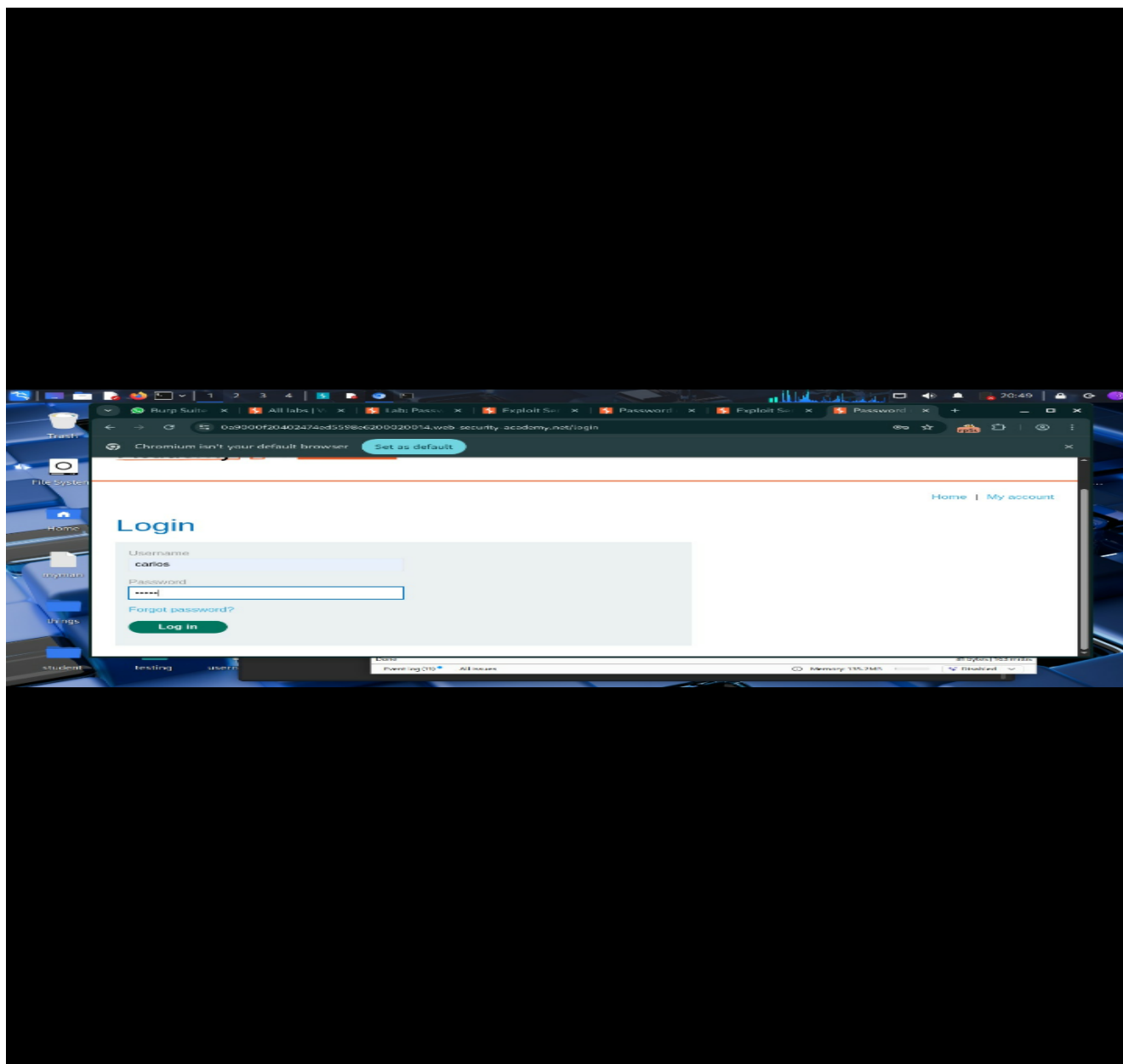


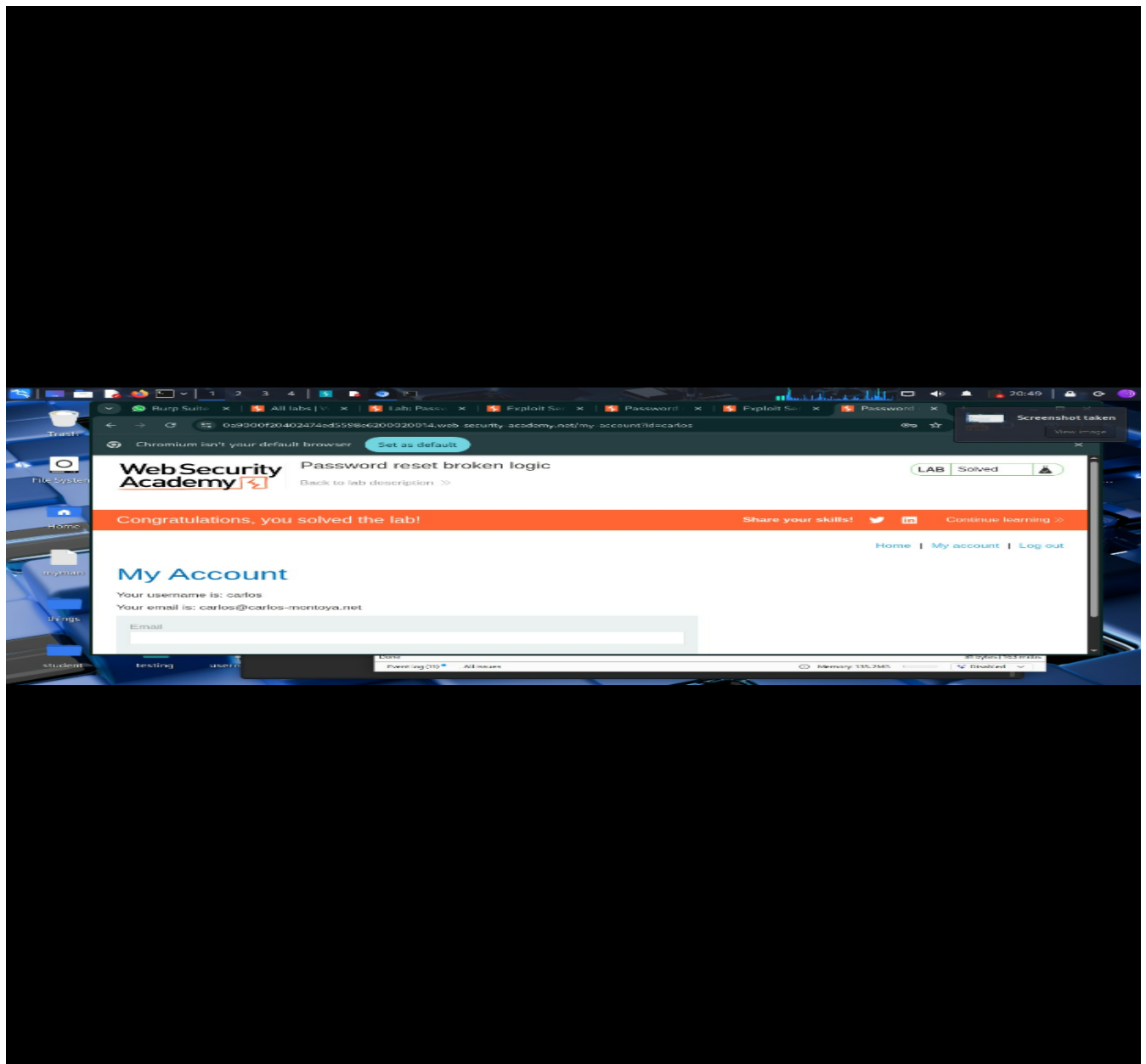












Impact

An attacker could exploit this vulnerability to reset passwords of other users, leading to unauthorized account access and possible account

takeover.

Remediation

Ensure password reset tokens are properly validated

Bind reset tokens to specific users and sessions

Implement strict server-side validation for reset requests

Disclaimer

This test was conducted in a controlled lab environment for educational and portfolio demonstration purposes only.