Authentication Vulnerability Report

Lab: Username Enumeration via Different Responses

Platform: PortSwigger Web Security Academy

Tester: Praisegod Aliyu

Date: 8 January 2026

Objective

The objective of this lab was to identify a username enumeration vulnerability by analyzing different authentication error responses returned by the application.

Vulnerability Type

Authentication Logic Flaw – Username Enumeration

OWASP Top 10 Category: A07 – Identification and Authentication Failures

Target Description

The target application contains a login functionality that validates user credentials and returns error messages based on the authentication result.

Vulnerability Discovery

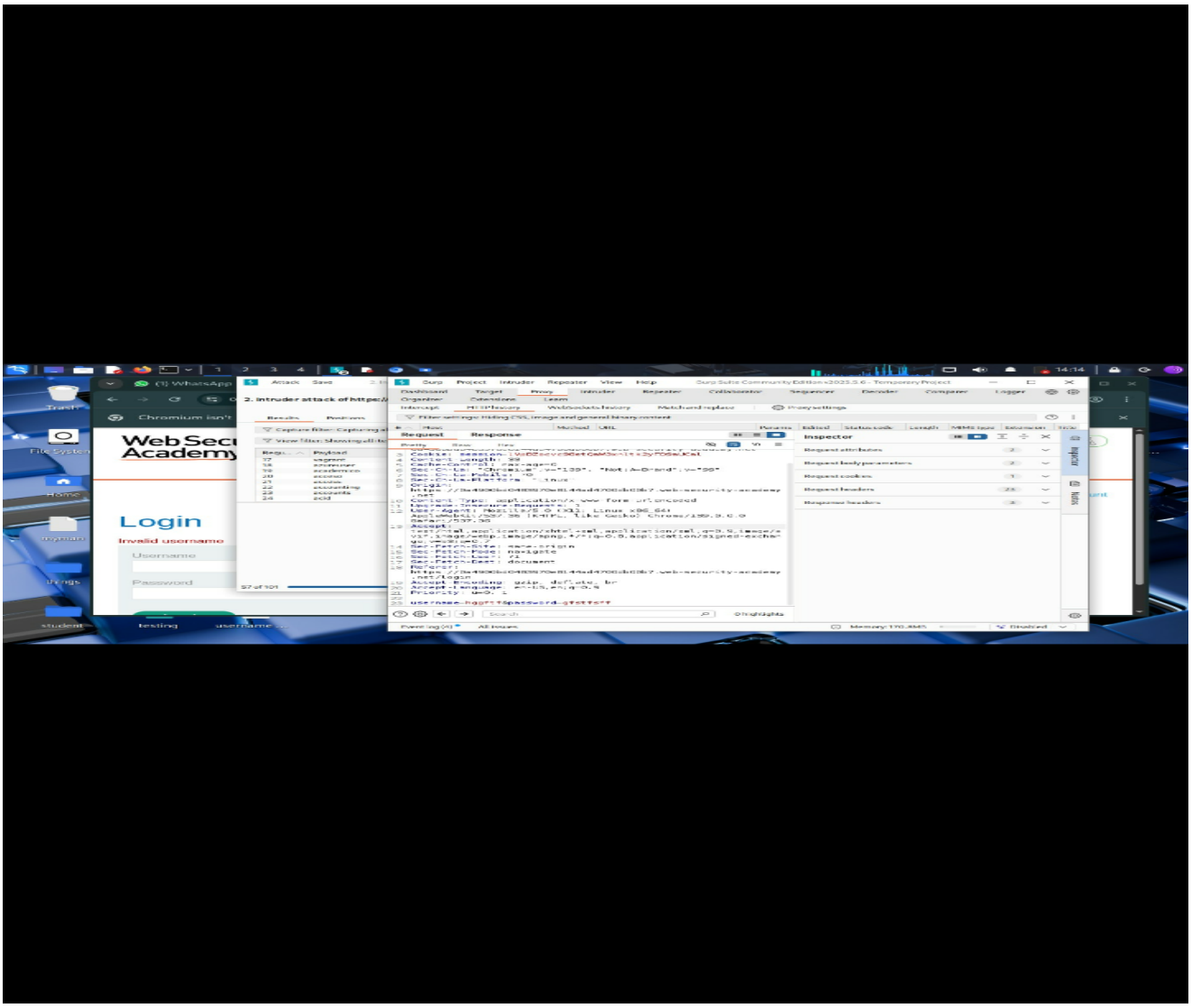
Submitted login requests with invalid usernames and observed the error message.

Submitted login requests using a valid username with an incorrect password.

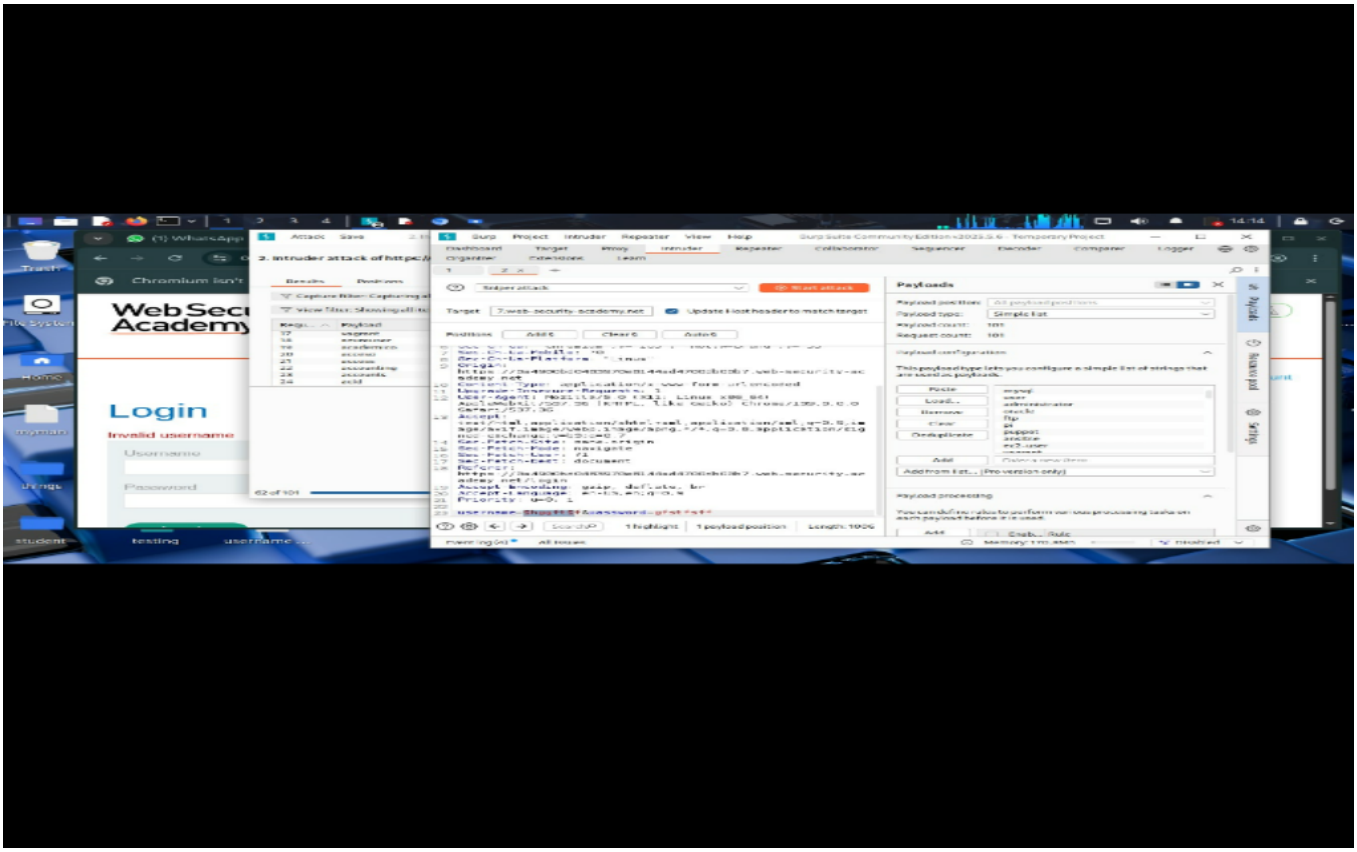
Compared the server responses and identified distinct messages for valid and invalid usernames.

Proof of Exploitation

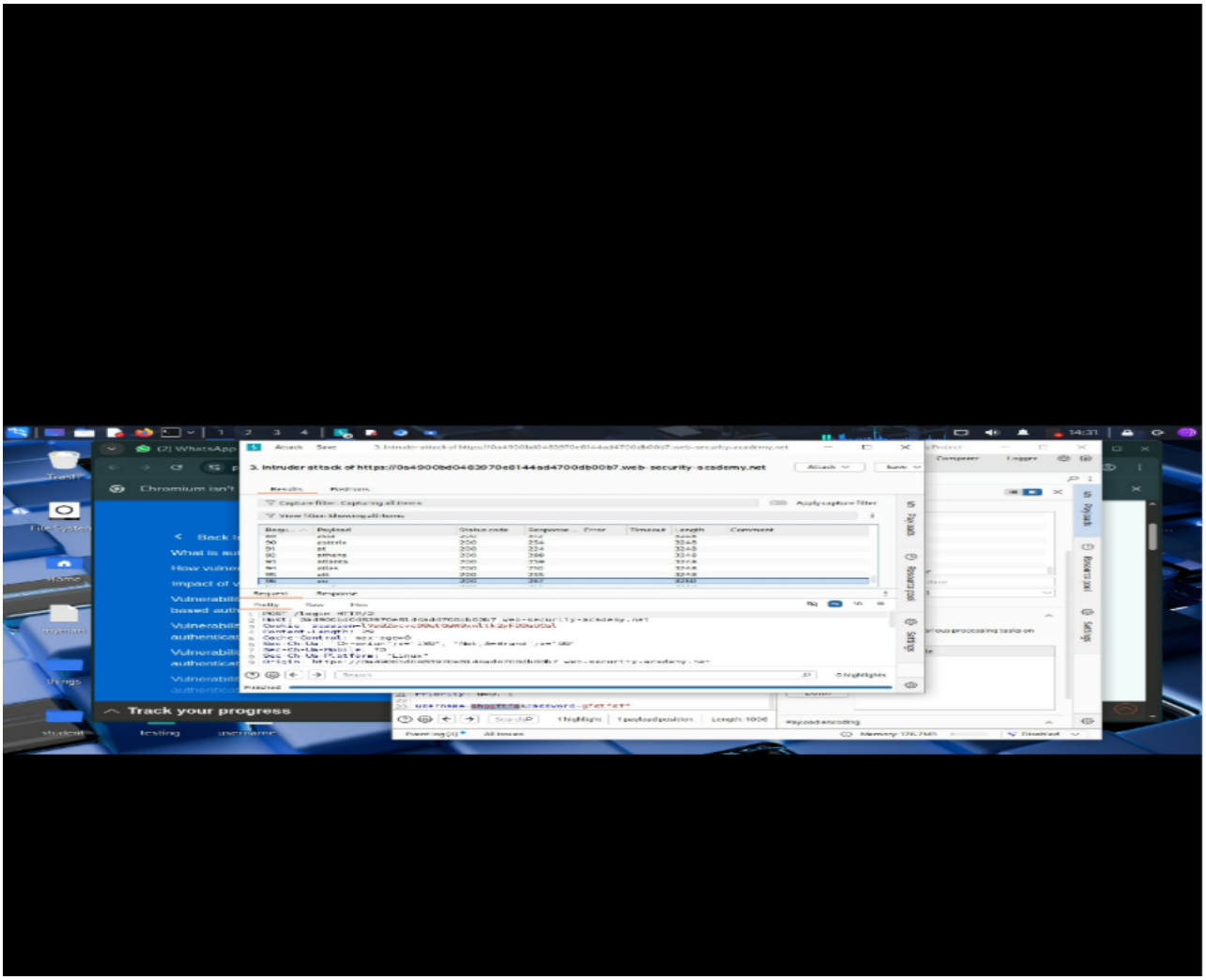
The screenshots below demonstrate different server responses when using valid and invalid usernames, confirming a username enumeration vulnerability.

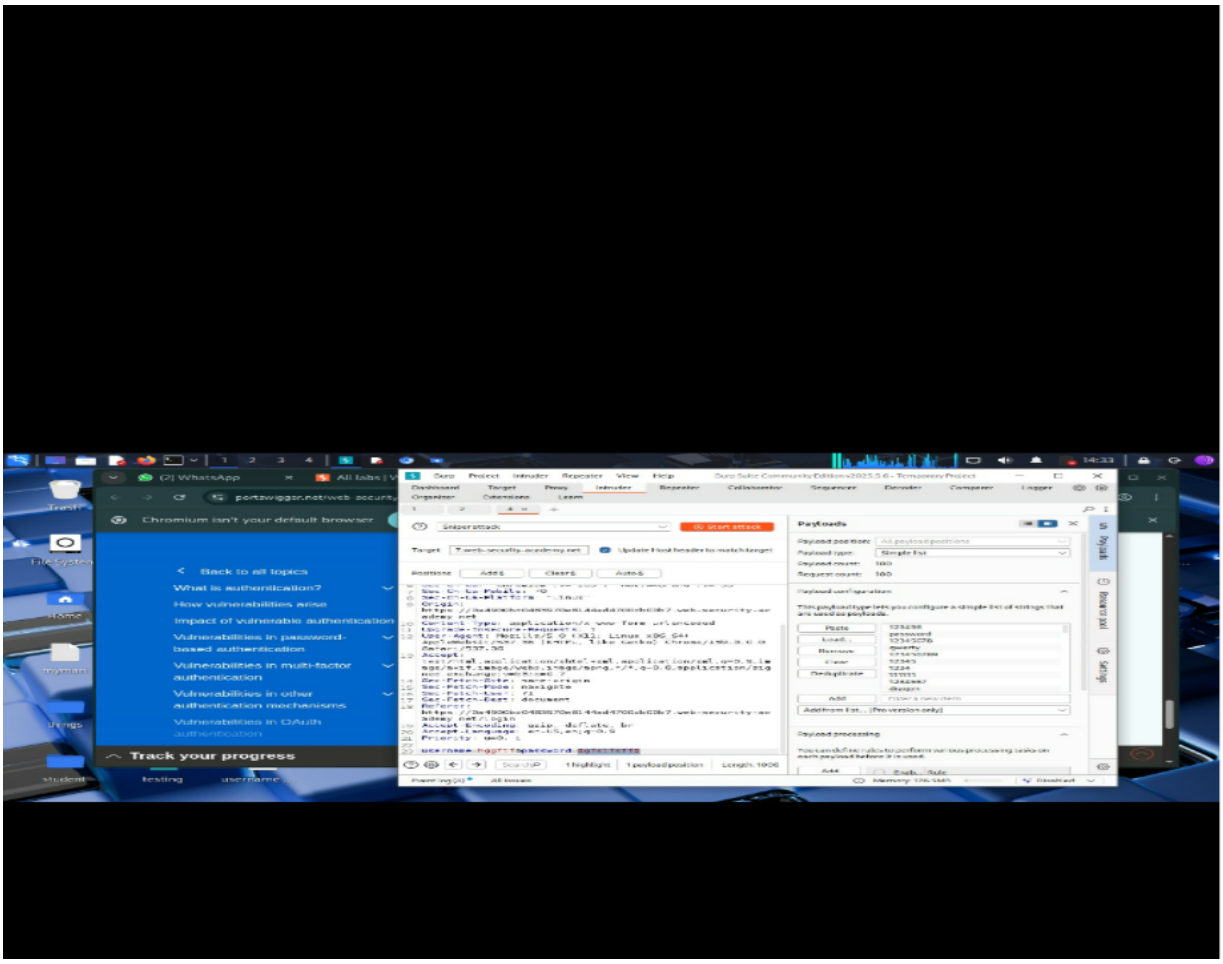


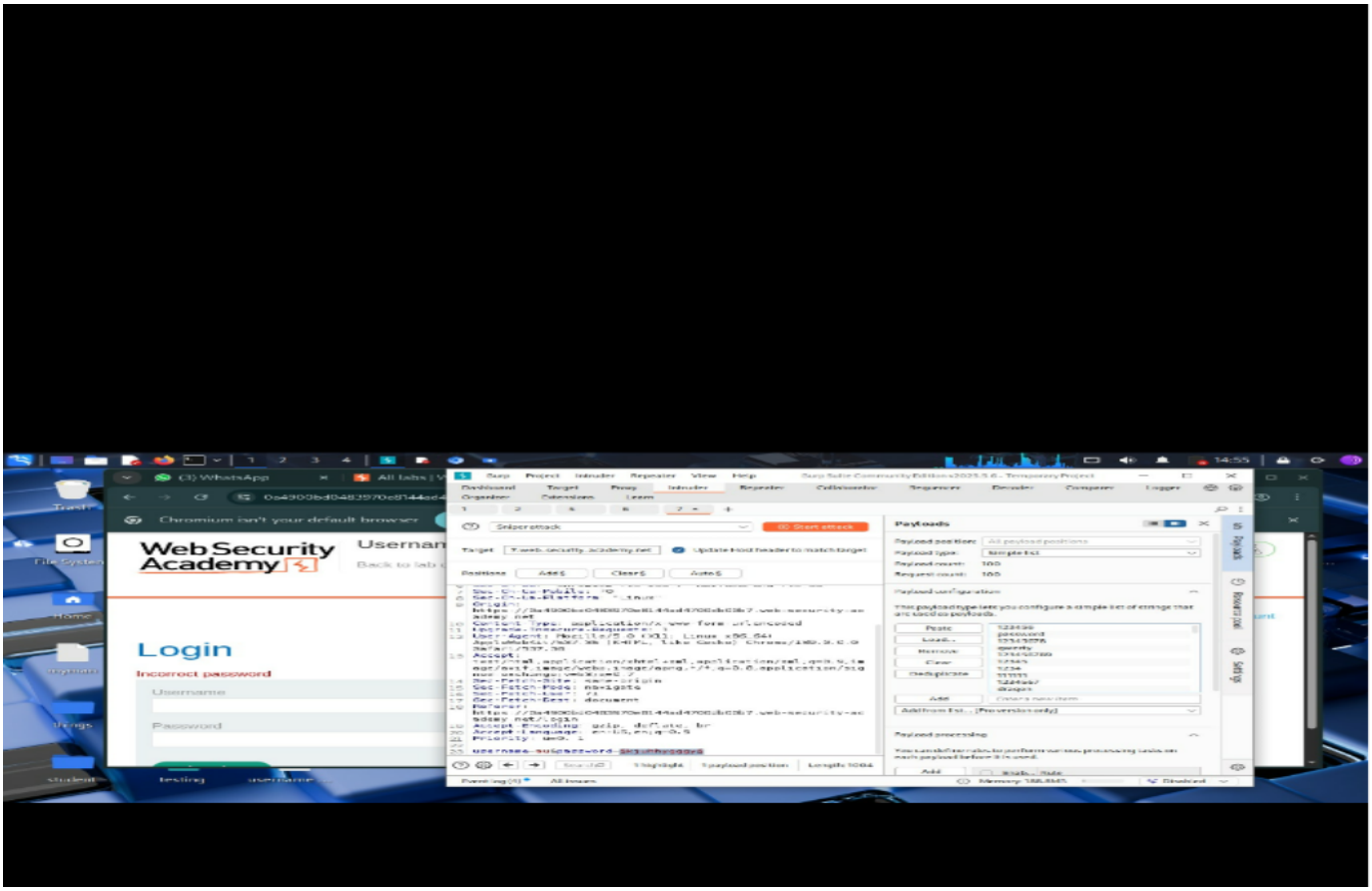
Intercept the request (with the wrong username and password)

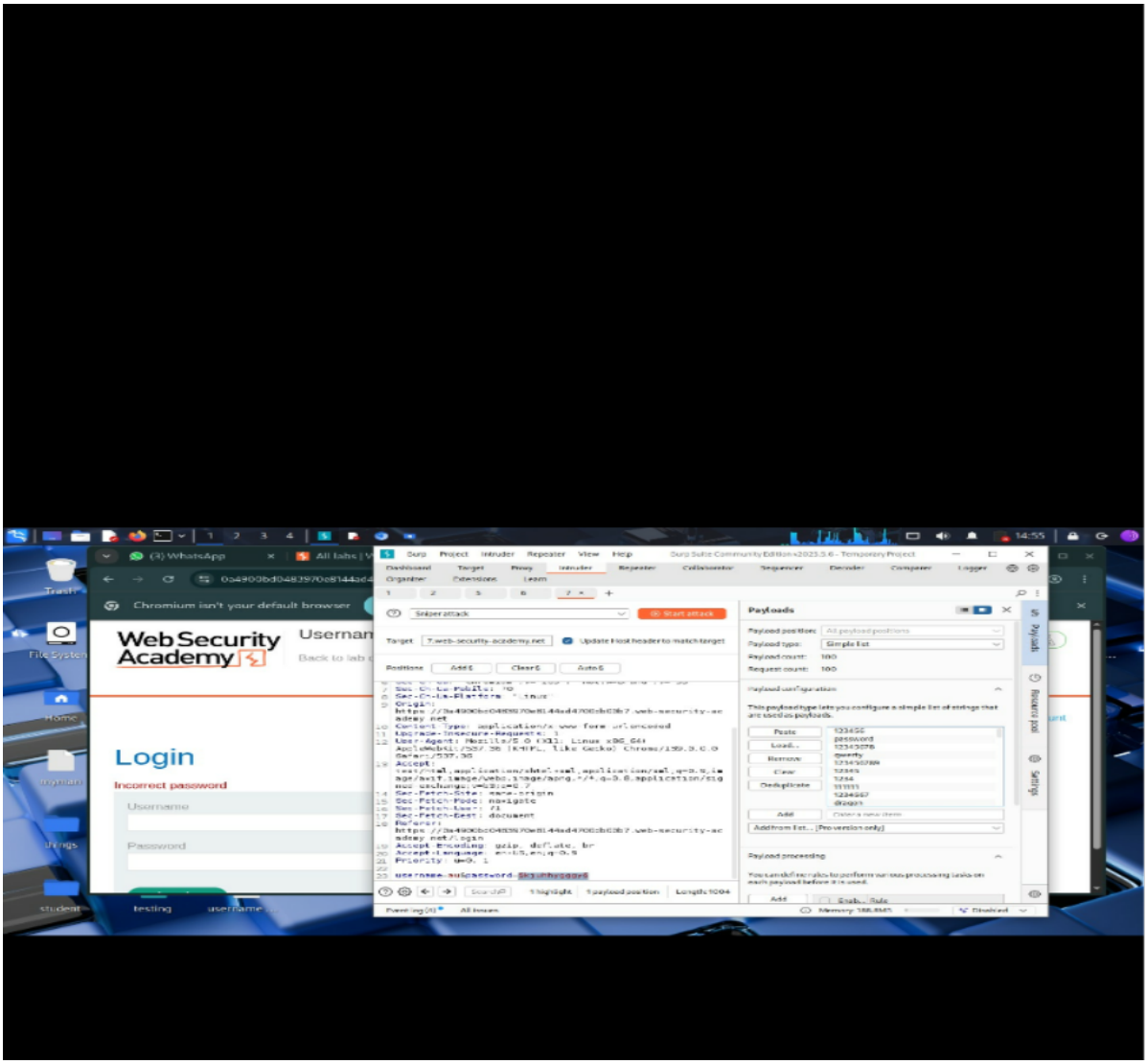


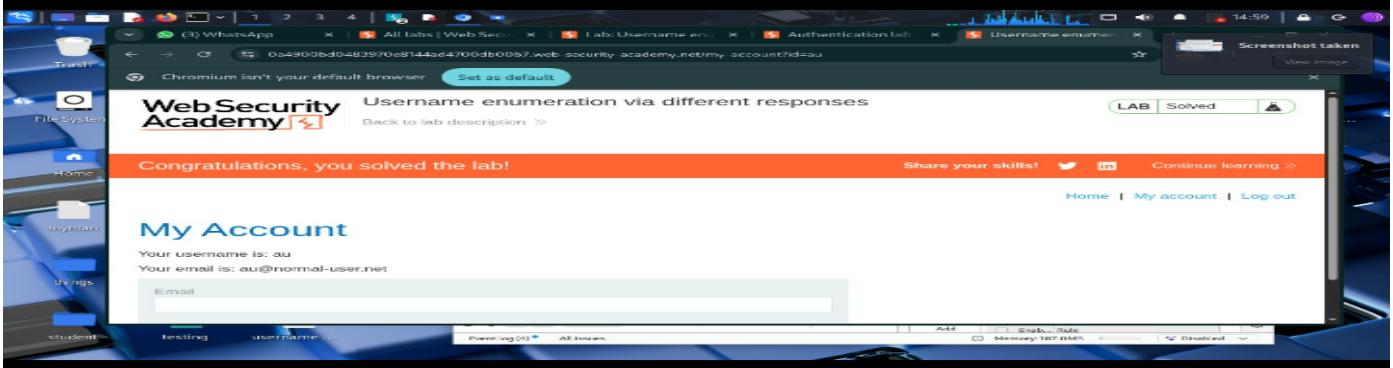
Adding payload to the username in intruder

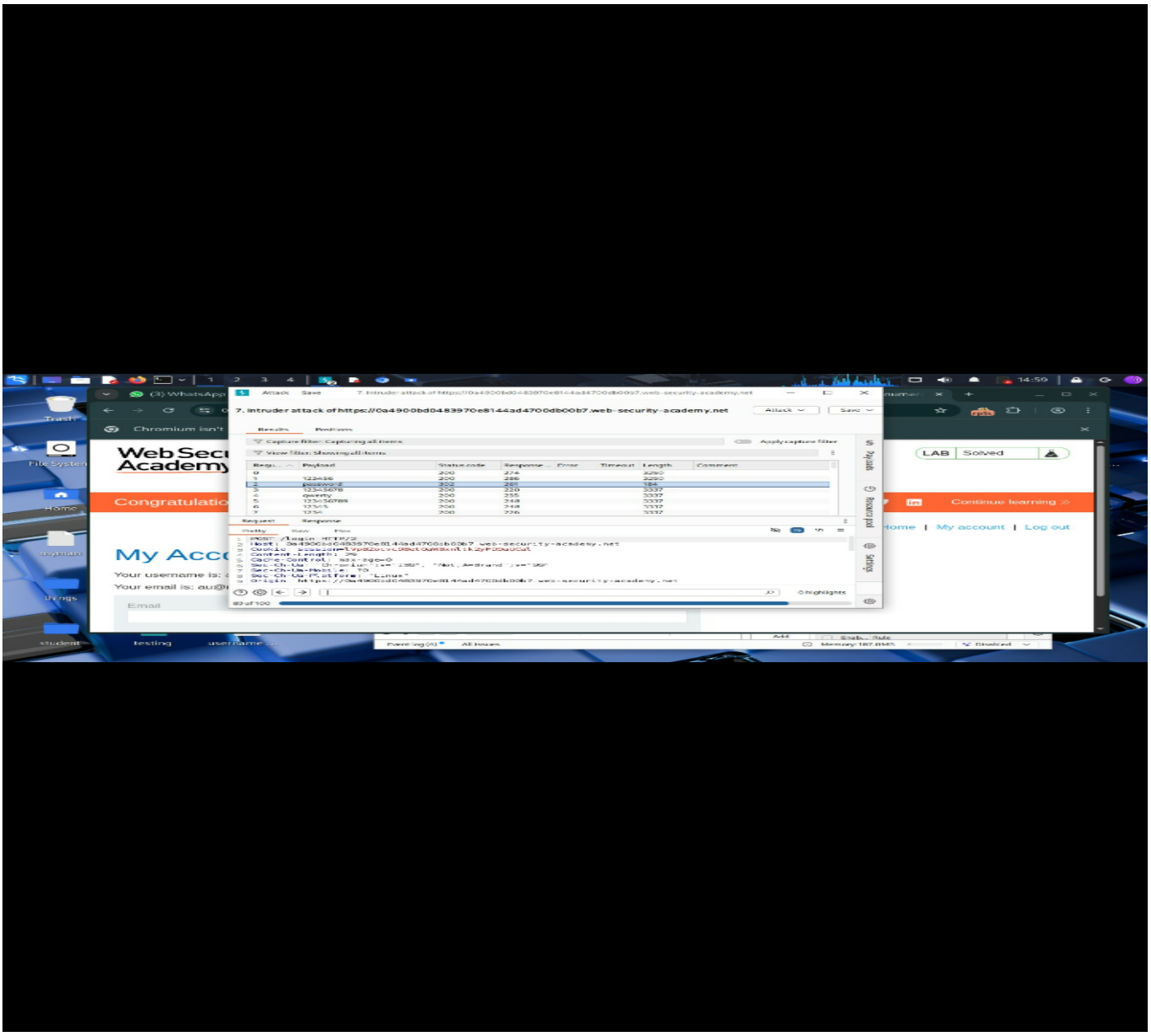

3. Intruder attack of https://0a4900bd0463970c8144ad4700db00b7.web-security-academy.net
Track your progress


Chromium isn't your default browser
Back to all topics
What is authentication?
How vulnerabilities arise
Impact of vulnerable authentication
Vulnerabilities in password-based authentication
Vulnerabilities in multi-factor authentication
Vulnerabilities in other authentication mechanisms
Vulnerabilities in OAuth authentication
Track your progress
Payloads


Web Security Academy
Login
Incorrect password
Username
Password
Chromium isn't your default browser
Sniper attack
Payloads


Web Security Academy
Login
Incorrect password
Username
Password
Payloads
Payload position:
Payload type:
Simple list
Payload count:
Request count:
Paste
Load...
Remove
Clear
Deduplicate
Add
Add from list... [Pro version only]
Payload processing
Payload encoding
Sniper attack
Start attack
Target:
Update Host header to match target
Positions
Add §
Clear §
Auto §
1 highlight
1 payload position
Length: 1094


Chromium isn't your default browser
Set as default
Web Security Academy
Username enumeration via different responses
Back to lab description
LAB
Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Log out
My Account
Your username is: au
Your email is: au@normal-user.net
Email



Impact

An attacker could exploit this vulnerability to enumerate valid usernames, which could later be used to facilitate brute-force attacks or account

compromise

Remediation

Use generic authentication error messages

Avoid revealing whether a username exists

Implement rate limiting on login attempts

Disclaimer

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