Insecure Direct Object Reference (IDOR) Vulnerability Report

Lab: Unauthorized API Object Access

Platform: PortSwigger Web Security Academy

Tester: Praisegod Aliyu

Date: [08 Jan, 2026]

Objective

The objective of this lab was to identify and exploit an Insecure Direct Object

Reference (IDOR) vulnerability in an API endpoint to retrieve another user's data

without proper authorization.

Vulnerability Type

Broken Access Control – IDOR (API-based)

OWASP Top 10 Category: A01 – Broken Access Control

Target Description

The target application exposes an API endpoint that retrieves user-specific data

based on a user-controlled object identifier included in the request.

Vulnerability Discovery

While analyzing API traffic using Burp Suite, it was observed that the API request

contained a user identifier parameter. Modifying this parameter did not trigger

any authorization checks, indicating a potential IDOR vulnerability.

Exploitation Steps

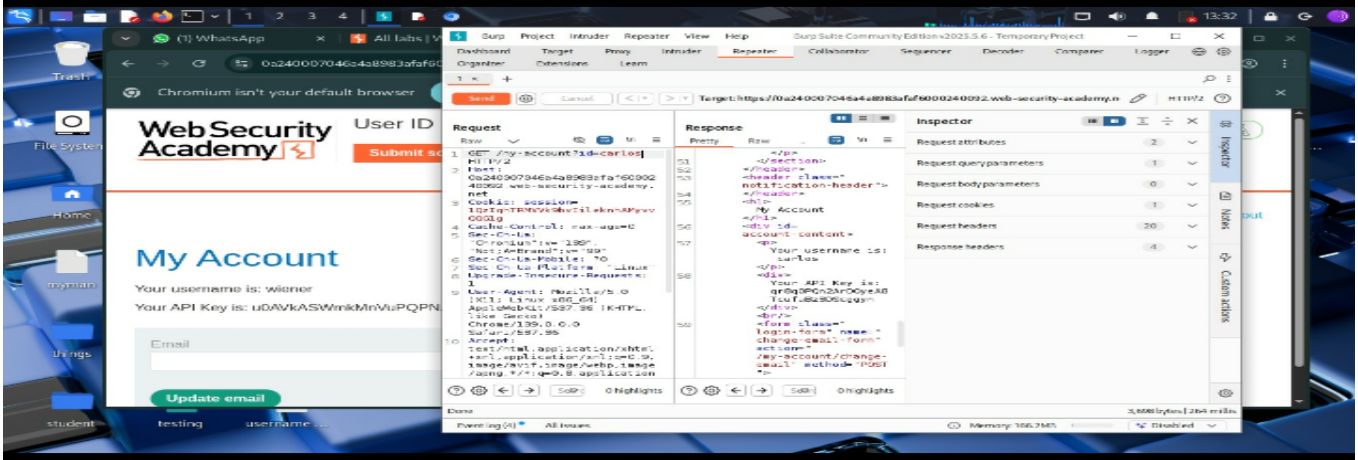
1. Logged into the application as a normal authenticated user.

2. Intercepted API requests using Burp Suite.

3. Identified the user identifier parameter within the API request.

4. Modified the user identifier to reference another user.

5. Sent the modified request and successfully retrieved another user's API data.


Web Security Academy
User ID
Submit solution
My Account
Your username is: wiener
Your API Key is: uDAVkASWmkMnVuPQPN
Email
Update email
Request
Response
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers

Impact

An attacker could exploit this vulnerability to access sensitive user information

through the API, potentially leading to privacy violations, data leakage,

and further account compromise.

Remediation

- Implement strict server-side authorization checks on all API endpoints

- Validate object ownership before returning data

- Use indirect object references where possible

- Apply role-based access control (RBAC)

Disclaimer

This vulnerability was exploited in a controlled lab environment

for educational and portfolio demonstration purposes only.