Task 2 Report: API Security Testing Lab

Target: Damn Vulnerable Web App (DVWA) - Authorisation Bypass Module

1. Findings Log

Test ID	Vulnerability	Severity	Target Endpoint
008	Broken Object Level Authorization (BOLA) - Write	Critical	`/vulnerabilities/authbypass/change_user_details.php`

2. Testing Checklist

- Enumerate API endpoints: Completed. Discovered the `change_user_details.php` endpoint via proxy history.
- Test for BOLA (Burp Suite): Completed. Successfully modified another user's details by changing the `id` parameter in a JSON payload.
- Fuzz GraphQL queries (Postman): Not applicable for this target.

3. API Test Summary

Testing of the `change_user_details.php` API endpoint revealed a Critical BOLA vulnerability. By modifying the `id` value in the JSON payload from 2 to 1, the server successfully processed an unauthorized request to change another user's data. This demonstrates a complete lack of server-side authorization checks on API calls, allowing for unauthorized data modification.

4. Evidence

4.1. API Endpoint Discovery

The vulnerable POST endpoint was discovered through manual traffic analysis in Burp Suite.
Evidence: `04_API_Endpoint_Discovery.png`

4.2. Successful BOLA Exploitation

The server responded with a `200 OK` status and a confirmation message, proving the unauthorized write operation was successful.
Evidence: `05_BOLA_Exploit_Success.png`