Cyber Security Test Reports

Insecure Direct Object References (IDOR)

CWE: CWE-639
OWASP Category: A01:2021 - Broken Access Control

Description:
Attackers can access restricted data by modifying URL parameters.

Business Impact:
- Exposure of sensitive user data
- Unauthorized modifications of records
- Privacy violations

Detection Method:
- Intercepted HTTP requests using Burp Suite.
- Modified user_id parameter manually to access unauthorized data.
- Confirmed unauthorized data access.

Cross-Site Request Forgery (CSRF)

CWE: CWE-352
OWASP Category: A08:2021 - Software and Data Integrity Failures

Description:
Allows attackers to trick users into executing unwanted actions.

Business Impact:
- Unauthorized account modifications
- Loss of user control over accounts
- Fraudulent transactions

Detection Method:
- Created a malicious HTML form mimicking a password change request.
- Tricked a logged-in user into submitting the form.
- Confirmed execution without authentication.

Security Misconfiguration

CWE: CWE-16
OWASP Category: A05:2021 - Security Misconfiguration

Description:
Default credentials, debug mode enabled, and exposed configuration files.

Business Impact:
- Increased attack surface
- Exposure of sensitive system information
- Unauthorized administrative access

Detection Method:

- Used default admin credentials (bee/bug) to log in.
- Found exposed /phpinfo.php revealing server configurations.
- Identified sensitive .bak and .txt files through brute-forcing.