Penetration Testing Report

Client: Demo Web Application (Lab Environment)

Tester: Sam Jabr

Date: [Insert Date]

Scope: Web Application vulnerabilities (OWASP Top 10 focus)

Environment: TryHackMe Lab – OWASP Top 10 2021

# 1. Executive Summary

This penetration test was performed against a controlled lab environment to simulate real-world attacks.   
Four major vulnerabilities were identified, including Broken Access Control, Injection, Authentication Failures,   
and Security Misconfiguration. These findings highlight common OWASP Top 10 issues and demonstrate how they could   
be exploited by attackers to compromise sensitive data and system integrity.

# 2. Findings Overview

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerability | Severity | Impact | Recommendation |
| Broken Access Control (IDOR) | High | Unauthorized data access | Enforce authorization checks |
| Injection (SQLi / Command Injection) | Critical | Full system compromise | Use parameterized queries |
| Authentication Failures | High | Account takeover | Implement MFA, lockout policies |
| Security Misconfiguration | Medium | Information leakage, easier exploitation | Harden configs, disable defaults |

# 3. Detailed Findings

## Broken Access Control (IDOR)

Attackers can bypass authorization controls and access data or functionality   
that should be restricted. This was demonstrated by accessing other users' data without proper authorization checks.   
Impact: Unauthorized access to sensitive information. Fix: Implement strict authorization checks.

## Injection (SQLi / Command Injection)

Unvalidated input was passed into database/system commands,   
allowing execution of arbitrary queries and system commands. Impact: Database dump, potential   
remote code execution. Fix: Use parameterized queries and input validation.

## Authentication Failures

Weak login mechanisms allowed brute-force and weak password exploitation.   
Impact: Account takeover, lateral movement. Fix: Enforce MFA, lockouts, and strong   
password policies.

## Security Misconfiguration

Default settings and verbose error messages exposed sensitive system details.   
Impact: Information leakage and easier exploitation. Fix: Apply security hardening,   
remove unnecessary features, and audit configurations regularly.

# 4. Disclaimer

This report is based on vulnerabilities identified in controlled lab environments (TryHackMe).   
No client or production systems were tested. This report is for demonstration and educational purposes only.