Penetration Testing Report

Client: ACME Corp

Test Type: Web Application Pentest

Date: May 2025

Consultant: Sayyam Muhammad

Executive Summary

This assessment focused on identifying security vulnerabilities in ACME Corp's internal and external-facing web applications. Several critical and high-risk findings were discovered and are documented below.

Methodology

The test was conducted using OWASP Top 10 methodology including Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Reporting.

Findings Snapshot

- SQL Injection (Critical)
- Stored Cross-Site Scripting (High)
- Insecure Direct Object Reference (IDOR)
- Missing HTTP Security Headers

Remediation Recommendations

Input validation should be enforced on all user-supplied data. Implement WAF policies and sanitize user inputs. Add HTTP security headers and conduct regular vulnerability scans.