

Sample Pentest Report

Security Assessment Findings Report

Project: Sample Pentest Report

Date: 2024-01-01

Reporter: John Doe

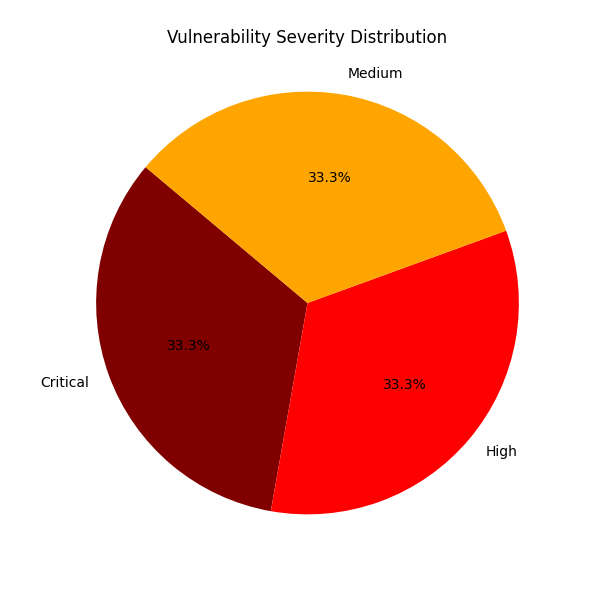
**Table of Contents**

# Executive Summary

The application was tested thoroughly and 3 vulnerabilities were identified, leading to complete takeover of the system.

# Technical Summary

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Findings** | | | | | |
| **Critical** | **High** | **Medium** | **Low** | **Informational** | **Total** |
| 1 | 1 | 1 | 0 | 0 | 3 |



# Vulnerabilities

## 1. SQL Injection

**Severity: High**

**URL/Vulnerable component:** http://example.com/login

**Description:** SQL injection vulnerability in login form.

**Impact:** Access to all user data.

**Remediation:** Use parameterized queries.

**PoC:** Use this to bypass authentication.

## 2. Cross-Site Scripting

**Severity: Medium**

**URL/Vulnerable component:** http://example.com/comment

**Description:** Reflected XSS in comment section.

**Impact:** Stealing session cookies.

**Remediation:** Sanitize user input.

**PoC:** <script>alert("XSS")</script>

## 3. SSTI

**Severity: Critical**

**URL/Vulnerable component:** http://example.com/comment

**Description:** SSTI in order placing.

**Impact:** Remote Code Execution.

**Remediation:** Sanitize user input.

**PoC:** {{7\*7}}