Penetration Test Report

Prepared for: Client Company Ltd.

Prepared by: CyberSec Consulting

Date: 2 July 2025

Table of Contents

Contents

1 Introduction

This document presents the results of a penetration test performed by CyberSec Consulting for Client Company Ltd.. The objective of this engagement was to assess the security posture of the client's systems, identify vulnerabilities, and provide actionable remediation recommendations.

2 Executive Summary

The penetration test identified the following key findings:

- X critical vulnerabilities
- Y high-severity issues
- Z medium/low-severity issues

Overall risk exposure: **[Insert risk level: Low / Medium / High]**

3 Scope

3.1 In-Scope Assets

- Web Application: `https://example.com`
- Internal Network Range: `192.168.0.0/24`
- External IPs: `203.0.113.10 - 203.0.113.20`

3.2 Out-of-Scope Assets

- Employee personal devices
- Third-party APIs

3.3 Testing Methodology

Testing was performed using a combination of manual and automated techniques, based on the OWASP Testing Guide and the PTES methodology.

4 Findings

1. ## Finding Title 1

   Severity: Critical
   Affected Asset: `https://example.com/login`
   Description: SQL Injection vulnerability in login form input.

   Evidence:

   ‘ OR ‘1’=’1

   Impact: An attacker could bypass authentication and access sensitive user data.

   Recommendation: Implement parameterised queries using prepared statements and validate all user input.

2. ## Finding Title 2

   Severity: Medium **Affected Asset**: `192.168.0.25` **Description**: SMBv1 enabled on internal host. **Impact**: Increased risk of exploitation via known vulnerabilities (e.g. EternalBlue). **Recommendation**: Disable SMBv1 protocol and apply all security patches.

5 Risk Summary

Severity	Count
Critical	1

Severity	Count
High	2
Medium	3
Low	

6 Conclusion

The test uncovered a number of security issues that require immediate attention. Addressing critical and high-severity findings should be prioritised. A follow-up validation test is recommended after remediation.

7 Appendix

7.1 Tools Used

- Nmap
- Burp Suite Pro
- Nikto
- Metasploit
- Custom Scripts

7.2 Definitions

Severity Ratings follow the CVSS v3.1 scoring system.

- Critical: CVSS 9.0 - 10.0
- High: CVSS 7.0 - 8.9
- Medium: CVSS 4.0 - 6.9
- Low: CVSS 0.1 - 3.9

This report is confidential and intended solely for Client Company Ltd..