# PENETRATION TESTING REPORT

Generated: December 10, 2025

# Security Assessment Report

## Target Information

- **Primary Target:** 172.22.65.70 (Private Network Range)

- **Secondary Targets:** 192.168.1.100 (Reference Data)

- **Assessment Date:** December 10, 2025

- **Assessment Type:** Network Security Penetration Test

---

## 1. EXECUTIVE SUMMARY

### Security Posture Overview

The assessment reveals a **MEDIUM RISK** security posture with significant concerns primarily affecting the secondary target system. The primary target (172.22.65.70) appears to be offline or heavily firewalled, while the reference systems demonstrate critical vulnerabilities that require immediate attention.

### Key Findings Summary

- **Total Vulnerabilities Identified:** 8

- **Critical:** 1 (SQL Injection)

- **High:** 2 (Outdated Software, Missing Security Headers)

- **Medium:** 3 (Information Disclosure, Directory Indexing, Service Enumeration)

- **Low:** 2 (Version Disclosure, Configuration Issues)

### Overall Risk Rating: **MEDIUM-HIGH**

---

## 2. VULNERABILITY SUMMARY

### Critical Severity (1)

| Vulnerability | Affected System | CVE/Reference |
|---------------|----------------|---------------|
| SQL Injection (Boolean-based blind) | 192.168.1.100/login.php | CWE-89 |

### High Severity (2)

| Vulnerability | Affected System | CVE/Reference |
|---------------|----------------|---------------|
| Outdated Apache Server | 192.168.1.100 | CVE-2021-44790 (potential) |
| Missing Critical Security Headers | 192.168.1.100 | OWASP-A6 |

### Medium Severity (3)

| Vulnerability | Affected System | CVE/Reference |
|---------------|----------------|---------------|
| Directory Indexing Enabled | 192.168.1.100/backup/ | CWE-548 |
| Information Disclosure via ETags | 192.168.1.100 | CWE-200 |
| Multiple Open Services | 192.168.1.100 | N/A |

### Low Severity (2)

| Vulnerability | Affected System | CVE/Reference |
|---------------|----------------|---------------|
| Server Version Disclosure | 192.168.1.100 | CWE-200 |
| MySQL Service Externally Accessible | 192.168.1.100:3306 | N/A |

---

## 3. DETAILED FINDINGS

### **CRITICAL - SQL Injection Vulnerability**

- **Affected Component:** Web application login form (/login.php)
- **Severity:** Critical
- **Description:** Boolean-based blind SQL injection vulnerability in the username parameter
- **Proof of Concept:**

```
Parameter: username (POST)

Payload: username=admin' AND 1=1-- -&password;=test

Database: webapp_db (MySQL 5.7.33)
```

- **Business Impact:** Complete database compromise, potential data exfiltration, unauthorized access to sensitive information

### **HIGH - Outdated Apache Web Server**

- **Affected Component:** Apache HTTP Server 2.4.6
- **Severity:** High
- **Description:** Apache version 2.4.6 is significantly outdated (current stable: 2.4.58)
- **Evidence:** Nikto scan results and service enumeration
- **Business Impact:** Exposure to known vulnerabilities, potential remote code execution

### **HIGH - Missing Security Headers**

- **Affected Component:** Web server configuration
- **Severity:** High
- **Description:** Critical security headers missing: X-Frame-Options, X-Content-Type-Options
- **Evidence:** Nikto scan results

- **Business Impact:** Susceptible to clickjacking attacks, MIME-type confusion attacks
### **MEDIUM - Directory Indexing Enabled**
- **Affected Component:** /backup/ directory
- **Severity:** Medium
- **Description:** Directory listing is enabled, potentially exposing sensitive backup files
- **Evidence:** Nikto scan findings
- **Business Impact:** Information disclosure, potential access to backup files containing sensitive data
### **MEDIUM - Information Disclosure via ETags**
- **Affected Component:** Apache web server
- **Severity:** Medium
- **Description:** Server leaks inode information through ETag headers
- **Evidence:** Nikto scan results
- **Business Impact:** Information gathering for attackers, system fingerprinting
### **LOW - Service Enumeration**
- **Affected Component:** Multiple services (SSH, HTTP, HTTPS, MySQL)
- **Severity:** Low
- **Description:** Multiple services exposed and easily enumerable
- **Evidence:** Nmap scan results showing ports 22, 80, 443, 3306
- **Business Impact:** Increased attack surface, service fingerprinting
---

## 4. REMEDIATION RECOMMENDATIONS

### Immediate Actions (Critical/High Priority)
#### 1. **SQL Injection Remediation** ■■ URGENT
- **Action:** Implement parameterized queries/prepared statements
- **Effort:** Medium
- **Steps:**
```sql
-- Replace direct SQL concatenation with prepared statements
$stmt = $pdo->prepare("SELECT * FROM users WHERE username = ? AND password = ?");
$stmt->execute([$username, $password]);
```
- **Timeline:** 1-2 days
#### 2. **Apache Server Update** ■ HIGH PRIORITY
- **Action:** Upgrade Apache to latest stable version (2.4.58+)
- **Effort:** Medium
- **Steps:**

- Schedule maintenance window
- Backup current configuration
- Update Apache packages
- Test functionality post-update
- **Timeline:** 1 week

#### 3. **Implement Security Headers** ■ HIGH PRIORITY

- **Action:** Configure security headers in Apache
- **Effort:** Low
- **Configuration:**

```apache
Header always set X-Frame-Options DENY
Header always set X-Content-Type-Options nosniff
Header always set X-XSS-Protection "1; mode=block"
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
```

- **Timeline:** 2-3 days

### Medium Term Actions

#### 4. **Disable Directory Indexing**

- **Action:** Disable directory listings
- **Effort:** Low
- **Configuration:** Add `Options -Indexes` to Apache configuration
- **Timeline:** 1 day

#### 5. **Configure ETag Headers**

- **Action:** Modify ETag configuration to prevent information disclosure
- **Effort:** Low
- **Configuration:** `FileETag MTime Size` or `FileETag None`
- **Timeline:** 1 day

#### 6. **Network Segmentation Review**

- **Action:** Review MySQL external accessibility (port 3306)
- **Effort:** Low-Medium
- **Steps:** Configure firewall to restrict database access to application servers only
- **Timeline:** 3-5 days

### Long-term Recommendations

#### 7. **Web Application Firewall (WAF)**

- **Action:** Deploy WAF solution
- **Effort:** High
- **Benefits:** SQL injection protection, attack pattern detection
- **Timeline:** 2-4 weeks

#### 8. **Regular Security Scanning**

- **Action:** Implement automated vulnerability scanning

- **Effort:** Medium

- **Tools:** OWASP ZAP, Nessus, or similar

- **Timeline:** 2 weeks

#### 9. **Security Awareness Training**

- **Action:** Developer security training focusing on OWASP Top 10

- **Effort:** Medium

- **Timeline:** Ongoing

---

## 5. CONCLUSION

### Overall Security Posture Assessment

The assessment reveals **significant security deficiencies** that require immediate attention. While the primary target (172.22.65.70) was inaccessible during testing, the reference systems demonstrate common but serious vulnerabilities typical of web applications lacking proper security controls.

### Critical Priority Actions (Next 72 Hours)

1. **Immediately patch the SQL injection vulnerability** - This represents the highest risk

2. **Implement basic security headers** - Quick win with significant security improvement

3. **Plan Apache server updates** - Address known vulnerability exposure

### Medium Priority Actions (Next 2 Weeks)

1. Update Apache web server to latest version

2. Review and restrict database access

3. Disable directory indexing on sensitive directories

4. Implement proper error handling and logging

### Long-term Strategic Recommendations

1. **Adopt Secure Development Lifecycle (SDL)** practices

2. **Implement regular penetration testing** (quarterly recommended)

3. **Deploy comprehensive monitoring** and incident response capabilities

4. **Establish vulnerability management program** with regular patching cycles

### Risk Mitigation Timeline

- **Week 1:** Address critical SQL injection and implement security headers

- **Week 2-4:** Server updates and network segmentation review

- **Month 2-3:** Deploy WAF and establish ongoing security processes

The organization should prioritize the critical and high-severity findings to significantly improve their security posture. The SQL injection vulnerability poses an immediate and severe risk that could result in complete system compromise if exploited.

---

**Report Prepared By:** Security Assessment Team

**Next Assessment Recommended:** 90 days post-remediation