PENETRATION TESTING REPORT

Generated: December 04, 2025

Security Assessment Report

Target: 192.168.1.100

Assessment Date: [Current Date]

Assessed By: Penetration Testing Team

---

1. EXECUTIVE SUMMARY

Security Posture Overview

The target system at 192.168.1.100 presents a **CRITICAL** security risk with multiple high-severity vulnerabilities that could lead to complete system compromise. The assessment identified significant weaknesses in the web application, server configuration, and security hardening practices.

Vulnerability Summary

- **Total Vulnerabilities Found:** 7

- **Overall Risk Rating:** CRITICAL

- **Critical Vulnerabilities:** 1

- **High Vulnerabilities:** 3

- **Medium Vulnerabilities:** 2

- **Low Vulnerabilities:** 1

Key Findings

The most concerning finding is a SQL injection vulnerability that allows complete database access. Combined with an exposed MySQL service and outdated software components, an attacker could achieve full system compromise.

---

2. VULNERABILITY SUMMARY

| Severity | Vulnerability | Affected Component | CVE |

|----------|---------------|--------------------|-----|

| **Critical** | SQL Injection (Boolean-based blind) | login.php | N/A |

| **High** | Exposed MySQL Service | Port 3306 | N/A |

| **High** | Outdated Apache Version | Apache 2.4.6 | CVE-2017-15710, CVE-2017-15715 |

| **High** | Directory Indexing Enabled | /backup/ directory | N/A |

| **Medium** | Missing Security Headers | Web Application | N/A |

| **Medium** | Information Disclosure via ETags | Apache Server | N/A |

| **Low** | SSH Service Exposed | Port 22 | N/A |

---

3. DETAILED FINDINGS

■ CRITICAL - SQL Injection Vulnerability

Description: A boolean-based blind SQL injection vulnerability exists in the username parameter of the login form.

Affected Component: `/login.php` - username parameter (POST method)

Severity Rating: Critical - Allows complete database compromise

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 and data exfiltration
- Potential privilege escalation to system level
- Loss of data confidentiality, integrity, and availability
- Regulatory compliance violations (GDPR, PCI-DSS)
- Reputation damage and financial losses

■ HIGH - Exposed MySQL Database Service

Description: MySQL database service is directly accessible from the network on port 3306.

Affected Component: MySQL 5.7.33 service

Severity Rating: High - Direct database access risk

Evidence: Port 3306/tcp open mysql MySQL 5.7.33

Business Impact:

- Direct database attacks and brute force attempts
- Potential data breach if weak credentials exist
- Bypass of application-layer security controls

■ HIGH - Outdated Apache Web Server

Description: Apache web server version 2.4.6 contains multiple known security vulnerabilities.

Affected Component: Apache HTTP Server 2.4.6

Severity Rating: High - Known exploitable vulnerabilities

Evidence: Multiple CVEs including CVE-2017-15710, CVE-2017-15715

Business Impact:

- Remote code execution potential
- Server compromise and lateral movement

- Service disruption and data theft

■ HIGH - Directory Indexing Enabled

Description: Directory listing is enabled on the `/backup/` directory, potentially exposing sensitive files.

Affected Component: `/backup/` directory

Severity Rating: High - Information disclosure

Evidence: Directory indexing enabled on /backup/

Business Impact:

- Exposure of sensitive backup files

- Information gathering for further attacks

- Potential access to configuration files and credentials

■ MEDIUM - Missing Security Headers

Description: Critical security headers are missing, leaving the application vulnerable to various client-side attacks.

Affected Component: Web application responses

Severity Rating: Medium - Client-side attack vectors

Evidence: Missing X-Frame-Options, X-Content-Type-Options headers

Business Impact:

- Clickjacking attacks

- MIME type confusion attacks

- Cross-site scripting (XSS) exploitation

■ MEDIUM - Information Disclosure via ETags

Description: Server leaks inode information through ETag headers.

Affected Component: Apache web server

Severity Rating: Medium - Information disclosure

Evidence: Server leaks inodes via ETags

Business Impact:

- Information gathering for targeted attacks

- Server fingerprinting and reconnaissance

■ LOW - SSH Service Exposure

Description: SSH service is accessible from the network, presenting a potential attack vector.

Affected Component: OpenSSH 7.4 on port 22

Severity Rating: Low - Standard service exposure

Evidence: 22/tcp open ssh OpenSSH 7.4

Business Impact:

- Brute force attack potential
- Credential stuffing attacks
---

4. REMEDIATION RECOMMENDATIONS

Priority 1 - IMMEDIATE ACTION REQUIRED
Critical: SQL Injection Vulnerability
- **Action:** Implement parameterized queries/prepared statements
- **Effort:** Medium
- **Timeline:** 24-48 hours
- **Prevention:**
- Input validation and sanitization
- Web Application Firewall (WAF) implementation
- Regular security code reviews
High: Disable MySQL External Access
- **Action:** Configure MySQL to bind only to localhost (127.0.0.1)
- **Effort:** Low
- **Timeline:** Immediate
- **Prevention:** Network segmentation and firewall rules
Priority 2 - SHORT TERM (1-2 weeks)
High: Update Apache Web Server
- **Action:** Update to latest stable Apache version (2.4.54+)
- **Effort:** Medium
- **Timeline:** 1 week
- **Prevention:** Implement automated patch management
High: Disable Directory Indexing
- **Action:** Add `Options -Indexes` directive to Apache configuration
- **Effort:** Low
- **Timeline:** Immediate
- **Prevention:** Secure Apache configuration baseline
Priority 3 - MEDIUM TERM (2-4 weeks)
Medium: Implement Security Headers
- **Action:** Configure security headers in web server/application
- **Effort:** Low
- **Timeline:** 1 week
- **Headers to implement:**
```
```

X-Frame-Options: DENY

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

Strict-Transport-Security: max-age=31536000

```

#### Medium: Fix ETag Information Disclosure

- **Action:** Configure Apache to use non-inode based ETags

- **Effort:** Low

- **Timeline:** 1 week

- **Configuration:** `FileETag MTime Size`

### Priority 4 - LONG TERM

#### Low: Secure SSH Access

- **Action:** Implement SSH hardening measures

- **Effort:** Low

- **Timeline:** 2 weeks

- **Recommendations:**

- Disable root login

- Implement key-based authentication

- Configure fail2ban

- Change default port if feasible

---

# 5. CONCLUSION

### Overall Security Posture Assessment

The target system presents a **CRITICAL** security risk that requires immediate attention. The combination of SQL injection vulnerability, exposed database service, and outdated software creates a perfect storm for system compromise.

### Immediate Priority Vulnerabilities

1. **SQL Injection** - Must be fixed within 24-48 hours

2. **MySQL External Access** - Should be disabled immediately

3. **Outdated Apache Server** - Update within one week

### Long-term Security Recommendations

#### Infrastructure Security

- Implement network segmentation

- Deploy Web Application Firewall (WAF)

- Establish automated patch management

- Configure comprehensive logging and monitoring

#### Application Security
```

- Conduct regular security code reviews
- Implement secure coding practices
- Perform periodic penetration testing
- Establish vulnerability management program

Operational Security

- Create incident response procedures
- Implement security awareness training
- Establish change management processes
- Regular security assessments and audits

Risk Acceptance

RECOMMENDATION: Do not accept current risk levels. The critical SQL injection vulnerability poses an unacceptable risk of data breach and should be remediated immediately before the system continues operation in a production environment.

Report Classification: CONFIDENTIAL

Next Assessment: Recommended within 30 days post-remediation