Penetration Test Report

Client: Example Corp

Date: 2025-11-06

Prepared by: Security Team

Executive Summary

This penetration testing assessment was conducted on 2025-11-06 for Example Corp. The assessment identified a total of 7 security findings across the tested infrastructure.

Key Findings:
• Critical Issues: 1
• High Severity Issues: 0
• Medium Severity Issues: 4

The findings indicate that immediate attention is required for critical and high-severity vulnerabilities to prevent potential security breaches.

Vulnerability Summary

Severity	Count	Percentage
Critical	1	14.3%
High	0	0.0%
Medium	4	57.1%
Low	2	28.6%
Informational	0	0.0%

Detailed Findings

1. [Critical] Web Vulnerability: /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute fo

Host	45.33.32.156
Port	80
Source	Nikto
Severity	Critical
CVEs	CVE-1999-0521, CVE-1999-0095, CVE-1999-0071, CVE-1999-0236

Description:
Method: GET, URI: /index /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html.

Remediation:
Restrict directory listings. Remove sensitive files from web root.

2. [Medium] Open Port: HTTP

Host	45.33.32.156
Port	80
Source	Nmap
Severity	Medium
CVEs	CVE-1999-1209, CVE-1999-0322, CVE-1999-0267, CVE-1999-0189, CVE-1999-1075

Description:
Port 80/tcp is open and running http

Remediation:
Review if http service on port 80 is necessary. Ensure it's properly configured and patched.

3. [Medium] Web Vulnerability: /: The anti-clickjacking X-Frame-Options header is not present.

Host	45.33.32.156
Port	80
Source	Nikto
Severity	Medium
CVEs	CVE-1999-1220

Description:
Method: GET, URI: / /: The anti-clickjacking X-Frame-Options header is not present.

Remediation:
Configure HTTP security headers (X-Frame-Options, CSP, etc)

4. [Medium] Web Vulnerability: /: The X-Content-Type-Options header is not set. This could allow the user agent to render the conte

Host	45.33.32.156
Port	80
Source	Nikto
Severity	Medium

Description:
Method: GET, URI: / /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.

Remediation:
Configure HTTP security headers (X-Frame-Options, CSP, etc)

5. [Medium] Web Vulnerability: /index: Uncommon header 'tcn' found, with contents: list.

Host	45.33.32.156
Port	80
Source	Nikto
Severity	Medium
CVEs	CVE-1999-0045, CVE-1999-0070, CVE-1999-0059, CVE-1999-1220, CVE-1999-0170

Description:
Method: GET, URI: /index /index: Uncommon header 'tcn' found, with contents: list.

Remediation:
Configure HTTP security headers (X-Frame-Options, CSP, etc)

6. [Low] Web Vulnerability: Apache/2.4.7 appears to be outdated (current is at least 2.4.57). Apache 2.2.34 is the EOL for the 2

Host	45.33.32.156
Port	80
Source	Nikto
Severity	Low
CVEs	CVE-1999-0071, CVE-1999-0236, CVE-1999-0107

Description:
Method: HEAD, URI: / Apache/2.4.7 appears to be outdated (current is at least 2.4.57). Apache 2.2.34 is the EOL for the 2.x branch.

Remediation:
Review and remediate per OWASP guidelines

7. [Low] Web Vulnerability: OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .

Host	45.33.32.156
Port	80
Source	Nikto
Severity	Low
CVEs	CVE-1999-0298, CVE-1999-1572

Description:
Method: OPTIONS, URI: / OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .

Remediation:
Review and remediate per OWASP guidelines

Recommendations

Based on the findings of this penetration test, the following high-level recommendations are provided:

1. **Immediate Actions:**
• Address all Critical and High severity vulnerabilities within 7 days
• Implement emergency patches for systems with known exploits
• Review and restrict unnecessary service exposure

2. **Short-term Actions (30 days):**
• Remediate Medium severity vulnerabilities
• Implement security hardening configurations
• Update security policies and procedures

3. **Long-term Actions:**
• Establish regular vulnerability scanning schedule
• Implement security awareness training
• Develop incident response procedures
• Conduct periodic penetration testing