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: 0
- 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	0	0.0%
High	0	0.0%
Medium	4	57.1%
Low	3	42.9%
Informational	0	0.0%

Detailed Findings

1. [Medium] Web Vulnerability: /: Retrieved x-powered-by header: ASP.NET.

Host	44.238.29.244
Port	80
Source	Nikto
Severity	Medium

Description:
Method: GET, URI: / /: Retrieved x-powered-by header: ASP.NET.

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

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

Host	44.238.29.244

Port	80
Source	Nikto
Severity	Medium

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

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

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

Host	44.238.29.244
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)

4. [Medium] Web Vulnerability: /p574uSrP.ashx: Retrieved x-aspnet-version header: 2.0.50727.

Host	44.238.29.244
Port	80
Source	Nikto
Severity	Medium

Description:
Method: GET, URI: /p574uSrP.ashx /p574uSrP.ashx: Retrieved x-aspnet-version header: 2.0.50727.

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

5. [Low] Web Vulnerability: /: Cookie ASPSESSIONIDSCBSABCS created without the httponly flag.

Host	44.238.29.244
Port	80
Source	Nikto

Severity	Low

Description:
Method: GET, URI: / /: Cookie ASPSESSIONIDSCBSABCS created without the httponly flag.

Remediation:
Review and remediate per OWASP guidelines

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

Host	44.238.29.244
Port	80
Source	Nikto
Severity	Low

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

Remediation:
Review and remediate per OWASP guidelines

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

Host	44.238.29.244
Port	80
Source	Nikto
Severity	Low

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

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