Vulnerability Scan Report

Target: **http://example.com**

Scan ID: 95693a9b-8ab7-4bbc-bfbc-dc742fb000d1

Executive Summary

This report presents the findings of a vulnerability scan conducted on **http://example.com**. The scan was performed on 2025-05-04 04:30:03 using security tools including Sqlmap, Nikto, Zap, Nessus.

Total Vulnerabilities	5
Risk Level	**High**
Scan Date	2025-05-04 04:30:03
Tools Used	Sqlmap, Nikto, Zap, Nessus

Vulnerability Overview

Vulnerability Severity Distribution

Critical: 0 **High: 2** **Medium: 0** **Low: 3** **Informational: 0**

Detailed Findings

Time-based Blind SQL Injection

Severity: High (CVSS: 8.6)

Detection Tool: SQLMap

Description:

Time-based blind SQL injection vulnerability detected in the "category" parameter.

Remediation

Use parameterized queries, input validation, and ORM frameworks.

SQL Injection

Severity: High (CVSS: 8.6)

Detection Tool: SQLMap

Description:

Potential SQL Injection vulnerability detected in the "id" parameter.

Remediation

Use parameterized queries, input validation, and ORM frameworks.

Severity: Low (CVSS: 2.0)

Detection Tool: Nikto

Description:

Potentially dangerous HTTP methods (e.g., TRACE, DELETE) enabled on example.com

Remediation

Review server configuration and update software.

Content Security Policy (CSP) Missing

Severity: Low (CVSS: 2.5)

Detection Tool: OWASP ZAP (Simulated)

Description:

No Content Security Policy detected, increasing risk of XSS attacks.

Remediation

Review ZAP findings and implement appropriate security controls.

Potentially Unnecessary Open Ports

Severity: Low (CVSS: 3.8)

Detection Tool: Nessus

Description:

example.com has several ports that may be unnecessarily exposed

Remediation

Update affected software and review configuration.

Report generated on: 2025-05-04 04:30:03