Security Vulnerability Assessment Report

Target Application: http://192.168.10.10:3000
Scan Date: August 2025
Total Vulnerabilities Found: 12 unique vulnerability types

Executive Summary

This security assessment identified multiple vulnerabilities across the target web application, ranging from high-severity security misconfigurations to informational findings. The most critical issues include missing security headers, session management weaknesses, and vulnerable JavaScript libraries that require immediate attention.

Detailed Vulnerability Findings

1. Content Security Policy (CSP) Header Not Set

- **Alert Type:** Security Misconfiguration
- **Risk:** Medium
- **Severity:** Medium
- **Confidence:** High
- **Location:** http://192.168.10.10:3000
- **CWE ID:** CWE-693
- **WASC ID:** 15
- **OWASP Category:** A05:2021 - Security Misconfiguration
- **Evidence:** Missing CSP header in HTTP response
- **Root Cause:** Web server/application server lacks proper CSP header configuration
- **Remediation:** Configure Content-Security-Policy header on web server, application server, or load balancer to prevent XSS and data injection attacks

2. Session ID in URL Rewrite

- **Alert Type:** Session Management
- **Risk:** Medium
- **Severity:** High
- **Confidence:** High

- **Location:** http://192.168.10.10:3000/socket.io/?EIO=4&transport=polling&t=PYAxZ05&sid=yHq0Kfa8h7GBla2HAAFx
- **CWE ID:** CWE-598
- **WASC ID:** 13
- **OWASP Category:** A01:2021 - Broken Access Control
- **Evidence:** Session ID "yHq0Kfa8h7GBla2HAAFx" exposed in URL
- **Root Cause:** URL rewriting used for session tracking instead of secure cookies
- **Remediation:** Use secure cookies for session management instead of URL rewriting; consider combining cookie and URL rewrite for enhanced security

3. Cross-Domain Misconfiguration

- **Alert Type:** Access Control
- **Risk:** Medium
- **Severity:** Medium
- **Confidence:** Medium
- **Location:** http://192.168.10.10:3000
- **CWE ID:** CWE-264
- **WASC ID:** 14
- **OWASP Category:** A01:2021 - Broken Access Control
- **Evidence:** Access-Control-Allow-Origin: *
- **Root Cause:** CORS misconfiguration allows cross-domain requests from any origin
- **Remediation:** Configure restrictive Access-Control-Allow-Origin header; whitelist specific trusted domains instead of using wildcard

4. Missing Anti-clickjacking Header

- **Alert Type:** UI Redressing
- **Risk:** Medium
- **Severity:** Medium
- **Confidence:** Medium
- **Location:** http://192.168.10.10:3000/socket.io/?EIO=4&transport=polling&t=PYAxZ05&sid=yHq0Kfa8h7GBla2HAAFx
- **CWE ID:** CWE-1021
- **WASC ID:** 15
- **OWASP Category:** A05:2021 - Security Misconfiguration
- **Evidence:** Missing X-Frame-Options header
- **Root Cause:** Application lacks clickjacking protection headers
- **Remediation:** Implement Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options header

5. Vulnerable JS Library

- **Alert Type:** Known Vulnerability
- **Risk:** Medium
- **Severity:** Medium
- **Confidence:** Medium
- **Location:** http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
- **CWE ID:** CWE-1395
- **WASC ID:** 15
- **OWASP Category:** A06:2021 - Vulnerable and Outdated Components
- **Evidence:** jQuery version 2.2.4 detected
- **Root Cause:** Application uses outdated jQuery library with known security vulnerabilities (CVE-2020-11023, CVE-2020-11022)
- **Remediation:** Upgrade to latest stable jQuery version; implement dependency scanning in CI/CD pipeline

6. Cross-Domain JavaScript Source File Inclusion

- **Alert Type:** Resource Inclusion
- **Risk:** Low
- **Severity:** Medium
- **Confidence:** Medium
- **Location:** http://192.168.10.10:3000
- **CWE ID:** CWE-829
- **WASC ID:** 15
- **OWASP Category:** A08:2021 - Software and Data Integrity Failures
- **Evidence:** `<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>`
- **Root Cause:** Loading JavaScript from third-party domains without integrity verification
- **Remediation:** Load JavaScript from trusted sources only; implement Subresource Integrity (SRI) for external scripts

7. Private IP Disclosure

- **Alert Type:** Information Disclosure
- **Risk:** Low
- **Severity:** Medium
- **Confidence:** Medium
- **Location:** http://192.168.10.10:3000/rest/admin/application-configuration
- **CWE ID:** CWE-497
- **WASC ID:** 13
- **OWASP Category:** A01:2021 - Broken Access Control
- **Evidence:** IP addresses 192.168.99.100:3000, 192.168.99.100:4200
- **Root Cause:** Application exposes internal network topology information

- **Remediation:** Remove private IP addresses from HTTP responses; use server/application comments instead of client-visible content

8. Timestamp Disclosure - Unix

- **Alert Type:** Information Disclosure
- **Risk:** Low
- **Severity:** Low
- **Confidence:** Low
- **Location:** http://192.168.10.10:3000
- **CWE ID:** CWE-497
- **WASC ID:** 13
- **OWASP Category:** A01:2021 - Broken Access Control
- **Evidence:** Unix timestamp 1650485437 (2022-04-20 16:10:37)
- **Root Cause:** Application unnecessarily exposes timestamp information
- **Remediation:** Verify timestamp data is not sensitive and cannot reveal exploitable patterns

9. X-Content-Type-Options Header Missing

- **Alert Type:** Security Header
- **Risk:** Low
- **Severity:** Medium
- **Confidence:** Medium
- **Location:** http://192.168.10.10:3000/socket.io/?EIO=4&transport=polling&t=PYAxZYr
- **CWE ID:** CWE-693
- **WASC ID:** 15
- **OWASP Category:** A05:2021 - Security Misconfiguration
- **Evidence:** Missing X-Content-Type-Options: nosniff header
- **Root Cause:** Server lacks MIME-sniffing protection configuration
- **Remediation:** Set X-Content-Type-Options header to 'nosniff' for all web pages to prevent MIME-sniffing attacks

10. Information Disclosure - Suspicious Comments

- **Alert Type:** Information Disclosure
- **Risk:** Informational
- **Severity:** Low
- **Confidence:** Low
- **Location:** http://192.168.10.10:3000/main.js
- **CWE ID:** CWE-615
- **WASC ID:** 13
- **OWASP Category:** A01:2021 - Broken Access Control
- **Evidence:** Pattern "\bQUERY\b" detected in comments referencing OWASP

- **Root Cause:** Suspicious comments in source code may provide information to attackers
- **Remediation:** Remove comments containing sensitive information; implement code review process

11. Modern Web Application

- **Alert Type:** Informational
- **Risk:** Informational
- **Severity:** Medium
- **Confidence:** Medium
- **Location:** http://192.168.10.10:3000
- **Evidence:** Modern web application detected with AJAX functionality
- **Root Cause:** Not a vulnerability - informational finding
- **Remediation:** No action required - consider using AJAX Spider for more comprehensive scanning

12. Retrieved from Cache

- **Alert Type:** Informational
- **Risk:** Informational
- **Severity:** Medium
- **Confidence:** Medium
- **Location:** http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
- **Evidence:** Content retrieved from cache (Age: 653483)
- **Root Cause:** HTTP/1.1 compliant caching in use
- **Remediation:** Validate cached content doesn't contain sensitive information; consider cache control headers