

Vulnerability Report for http://testhtml5.vulnweb.com

Vulnerabilities Found:

Vulnerability: Missing Anti-clickjacking Header

Risk Level: Medium

URL: http://testhtml5.vulnweb.com/

Description: The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy or X-Frame-Options HTTP headers.

Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers.

Vulnerability: Content Security Policy (CSP) Header Not Set

Risk Level: Medium

URL: http://testhtml5.vulnweb.com/

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including drive-by-download attacks, cross-site scripting (XSS), and data injection attacks.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Vulnerability: Cross-Domain Misconfiguration

Risk Level: Medium

URL: http://testhtml5.vulnweb.com/

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration.

Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP addresses or other identifiers).

Vulnerability: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low

URL: http://testhtml5.vulnweb.com/

Description: The page includes one or more script files from a third-party domain.

Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can be audited.

Vulnerability: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low

URL: http://testhtml5.vulnweb.com/

Description: The page includes one or more script files from a third-party domain.

Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can be audited.

Vulnerability: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low

URL: http://testhtml5.vulnweb.com/

Description: The page includes one or more script files from a third-party domain.

Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can be audited.

Vulnerability: Cross-Domain JavaScript Source File Inclusion

Risk Level: Low

URL: http://testhtml5.vulnweb.com/

Description: The page includes one or more script files from a third-party domain.

Solution: Ensure JavaScript source files are loaded from only trusted sources, and the sources can be audited.

Vulnerability: Information Disclosure - Suspicious Comments

Risk Level: Informational

URL: http://testhtml5.vulnweb.com/

Description: The response appears to contain suspicious comments which may help an attacker. No action is required.

Solution: Remove all comments that return information that may help an attacker and fix any underlying issues.

Vulnerability: Modern Web Application

Risk Level: Informational

URL: http://testhtml5.vulnweb.com/

Description: The application appears to be a modern web application. If you need to explore it automatically, use a tool like Burp Suite.

Solution: This is an informational alert and so no changes are required.

Vulnerability: Server Leaks Version Information via "Server" HTTP Response Header Field

Risk Level: Low

URL: http://testhtml5.vulnweb.com/

Description: The web/application server is leaking version information via the "Server" HTTP response header field.