Danvers Remediation Report

Date Created: 06-15-2023

Overall Score 829 / 850

Website Security: 829 | Email Security: 763 | Network Security: 950 | Phishing Score: 949 | Brand Score: 950

Issue #1: SSL not available

Why is it risky:

Susceptible to man-in-the-middle attacks

Description:

SSL is the standard encryption method for browsing websites. Enabling SSL requires installing an SSL certificate on the site.

Issue #2: Server information header exposed

Why is it risky:

Vulnerabilities can be uncovered more easily

Description:

Exposing information about the server version increases the ability of attackers to exploit certain vulnerabilities. The website configuration should be changed to prevent version information being revealed in the 'server' header.

Issue #3: Vulnerable to CVE-2014-3566 (POODLE)

Why is it risky:

Vulnerabilities

Description:

The server supports SSLv3 and is therefore vulnerable to POODLE, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack.

Issue #4: HTTP Strict Transport Security (HSTS) not enforced

Why is it risky:

Susceptible to man-in-the-middle attacks

Description:

Without HSTS enforced, people browsing this site are more susceptible to man-in-the-middle attacks. The server should be configured to support HSTS.

Issue #5: CSP implemented unsafely

Why is it risky:

Vulnerable to cross-site attacks

Description:

The Content Security Policy may not restrict sources appropriately, or may contain 'unsafe-inline' without the use of a nonce or hash. This increases the risk of XSS attacks.

Issue #6: Only weak cipher suites supported in TLS 1.2 (Provisional)

Why is it risky:

Susceptible to man-in-the-middle attacks

Description:

Weak cipher suites can potentially be broken by a well resourced attacker, and should not be used where possible. This server also does not appear to support any secure cipher suites, which means clients will either not be able to make a secure connection, or only make a weak one.

Issue #7: HTTPS redirect not supported

Why is it risky:

Susceptible to man-in-the-middle attacks

Description:

HTTPS is the standard protocol for secure communication on the internet. All redirects should be performed over HTTPS.

Issue #8: Common Diffie-Hellman prime used in key exchange (Provisional)

Why is it risky:

Susceptible to man-in-the-middle attacks

Description:

Commonly used Diffie-Hellman primes smaller than 2048 bits are likely to have been broken by organized groups or nation-state actors, allowing passive eavesdropping on traffic. It is recommended to use a 2048 bit or stronger Diffie-Hellman prime.

Issue #9: Secure cookies not used

Why is it risky:

Susceptible to man-in-the-middle attacks

Description:

When secure cookies are not used, there is an increased risk of third parties intercepting information contained in these cookies. The website configuration should be changed so that all 'Set-Cookie' headers include 'secure'.

Issue #10: X-Frame-Options is not deny or sameorigin

Why is it risky:

Vulnerable to clickjacking attacks

Description:

Browsers may display this website's content in frames. This can lead to clickjacking attacks.

Issue #11: CSP allows insecure active sources

Why is it risky:

Vulnerable to cross-site attacks

Description:

The Content Security Policy on this site allows insecure active content.

Issue #12: Insecure SSL/TLS versions available

Why is it risky:

Susceptible to man-in-the-middle attacks

Description:

Any version of the SSL protocol, and TLS prior to version 1.2, are now considered insecure. The server should disable support for these old protocols.

Issue #13: CSP is not implemented

Why is it risky:

Vulnerable to cross-site attacks

Description:

No valid Content Security Policy is implemented. This increases the risk of XSS and clickjacking attacks.

Issue #14: HttpOnly cookies not used

Why is it risky:

Vulnerable to cross-site attacks

Description:

When HttpOnly cookies are not used, the cookies can be accessed on the client, which enables certain type of client-side attacks. The website configuration should be changed to enforce HttpOnly cookies.

Issue #15: Domain was not found on the HSTS preload list

Why is it risky:

Susceptible to man-in-the-middle attacks

Description:

The domain was not found on the HSTS preload list. Users who visit the website for the first time will be vulnerable to MITM attacks. The requirements for inclusion on the preload list are specified by hstspreload.org.

Issue #16: Use of ASP.NET exposed via header

Why is it risky:

Vulnerabilities can be uncovered more easily

Description:

Exposing the ASP.NET version header indicates that the site is built with ASP.NET, which makes it easier for attackers to exploit certain vulnerabilities. The website configuration should be changed to remove this header.

Issue #17: CSP contains unsafe-eval

Why is it risky:

Vulnerable to cross-site attacks

Description:

The Content Security Policy is implemented with unsafe-eval, reducing protection against XSS attacks.

Issue #18: Specific ASP.NET version exposed via header

Why is it risky:

Vulnerabilities can be uncovered more easily

Description:

Exposing a specific ASP.NET version in the ASP.NET version header makes it easier for attackers to exploit certain vulnerabilities. The website configuration should be changed to remove this header completely.

Issue #19: X-Content-Type-Options is not nosniff

Why is it risky:

Vulnerable to cross-site attacks

Description:

Browsers may interpret files as a different MIME type than what is specified in the Content-Type HTTP header. This can lead to MIME confusion attacks.

Issue #20: HSTS header does not contain includeSubDomains

Why is it risky:

Susceptible to man-in-the-middle attacks

Description:

The HTTP Strict Transport Security (HSTS) header does not contain the includeSubDomains directive. This directive instructs the browser to also enforce the HSTS policy over subdomains of this domain.

Issue #21: DNSSEC not enabled

Why is it risky:

DNS is susceptible to man-in-the-middle attacks

Description:

DNSSEC records prevent third parties from forging the records that guarantee a domain's identity. DNSSEC should be configured for this domain.

Issue #22: 'HTTP' port open

Why is it risky:

Unnecessary open ports

Description:

The 'HTTP' service is running and exposed to the internet. The configuration of the server should be reviewed and unnecessary ports closed.

Issue #23: CAA not enabled

Why is it risky:

Susceptible to man-in-the-middle attacks

Description:

The domain does not contain a valid Certification Authority Authorization (CAA) record. A CAA record indicates which Certificate Authorities (CAs) are authorized to issue certificates for a domain.

Issue #24: Weak cipher suites supported in TLS 1.2

Why is it risky:

Susceptible to man-in-the-middle attacks

Description:

Weak cipher suites can potentially be broken by a well resourced attacker, and should not be supported by the server unless very old devices or browsers must be supported.

Issue #25: Port 8010 is open

Why is it risky:

Unnecessary open ports

Description:

Port 8010 is open on this server, however no service was detected listening on this port. The configuration of the server should be reviewed and unnecessary ports closed.

Issue #26: 'HTTPS' port open

Why is it risky:

Unnecessary open ports

Description:

The 'HTTPS' service is running and exposed to the internet. The configuration of the server should be reviewed and unnecessary ports closed.

Issue #27: Unmaintained page detected

Why is it risky:

Vulnerabilities can be uncovered more easily

Description:

This domain appears to be unmaintained based on indicators like page content or status code. Unmaintained pages expand the attack surface for malicious actors.

Issue #28: Microsoft Internet Information Server 8.5 has potential vulnerabilities

Why is it risky:

Vulnerabilities

Description:

Microsoft Internet Information Server 8.5 has vulnerablities which might be exploitable under certain conditions. Affected domains should be checked to determine which vulnerabilities might pose a risk.
