Middleton Remediation Report

Date Created: 06-15-2023

Overall Score 672 / 850

Website Security: 672 | Email Security: 594 | Network Security: 221 | Phishing Score: 937 | 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: HTTP does not redirect to HTTPS

Why is it risky:

Susceptible to man-in-the-middle attacks

Description:

The domain is still accessible over HTTP. All HTTP requests should be redirected to HTTPS.

Issue #3: DMARC policy not found

Why is it risky:

Emails can be fraudulently sent

Description:

DMARC policy was not found. This makes it easier for attackers to send email from this domain. A DMARC policy should be deployed for this domain.

Issue #4: Hostname does not match SSL certificate

Why is it risky:

Susceptible to man-in-the-middle attacks

Description:

The site's hostname does not match the SSL certificate. The domain name should be added to the certificate, either as a Subject Alternative Name or as the Common Name.

Issue #5: SPF not enabled

Why is it risky:

Emails can be fraudulently sent

Description:

Sender Policy Framework (SPF) record is not present. This may allow spammers to send messages with forged addresses using this domain. The DNS record for the domain should be modified to include an SPF record.

Issue #6: 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 #7: 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 #8: 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 #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: 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 #11: 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 #12: 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 #13: 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 #14: Domain registrar or registry deletion protection not enabled

Why is it risky:

Domain at risk of being hijacked

Description:

Domain is not protected from unsolicited deletion requests with the registrar or registry. The domain should have clientDeleteProhibited or serverDeleteProhibited set.

Issue #15: SPF policy uses ?all

Why is it risky:

Emails can be fraudulently sent

Description:

Sender Policy Framework (SPF) record is too lenient as to which domains are allowed to send email on the domain's behalf. When DMARC is not being enforced, the SPF record should use -all to instruct mail receivers to reject messages from unauthorised sources.

Issue #16: 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 #17: WordPress version exposed

Why is it risky:

WordPress misconfiguration issues found

Description:

Ensuring the WordPress version is not exposed can make it harder for attackers to find exploits against your site

Issue #18: 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 #19: 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 #20: Domain registrar or registry update protection not enabled

Why is it risky:

Domain at risk of being hijacked

Description:

Domain is not protected from unsolicited update requests with the registrar or registry. The domain should have clientUpdateProhibited or serverUpdateProhibited set.

Issue #21: 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 #22: WordPress plugin versions exposed

Why is it risky:

WordPress misconfiguration issues found

Description:

Ensuring WordPress plugin versions are not exposed can make it harder for attackers to find exploits against your site.

Issue #23: 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 #24: Microsoft Exchange Server 15.2.986.37 has potential vulnerabilities

Why is it risky:

Vulnerabilities

Description:

Microsoft Exchange Server 15.2.986.37 has vulnerablities which might be exploitable under certain conditions. Affected domains should be checked to determine which vulnerabilities might pose a risk.

Issue #25: 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 #26: 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 #27: '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 #28: 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.
