Wenham Remediation Report

Date Created: 06-15-2023

Overall Score 801 / 850

Website Security: 801 | Email Security: 823 | Network Security: 475 | Phishing Score: 908 | Brand Score: 950

Issue #1: 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 #2: 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 #3: 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 #4: 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 #5: 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. This record should preferably not use the ~all mechanism, as this does not instruct the mail receiver to reject messages from unauthorised sources. When DMARC is not being enforced, -all should be used on the SPF record.

Issue #6: 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 #7: 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.
