Topsfield Remediation Report

Date Created: 06-15-2023

Overall Score 804 / 850

Website Security: 804 | Email Security: 787 | Network Security: 504 | Phishing Score: 885 | 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: 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 #3: 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 #4: 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 #5: 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 #6: Port 465 is open and listening

Why is it risky:

Unnecessary open ports

Description:

Port 465 is open and an unidentified service was detected listening on this port. The configuration of the server should be reviewed and unnecessary ports closed.

Issue #7: 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 #8: 'MSA Outlook' port open

Why is it risky:

Unnecessary open ports

Description:

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

Issue #9: 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 #10: 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 #11: 'SSH' port open

Why is it risky:

Unnecessary open ports

Description:

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

Issue #12: 'SMTP' port open

Why is it risky:

Unnecessary open ports

Description:

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

Issue #13: 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 #14: 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 #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. 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 #16: 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 #17: 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 #18: 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 #19: 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 #20: OpenSSH 7.2p2 has potential vulnerabilities

Why is it risky:

Vulnerabilities

Description:

OpenSSH 7.2p2 has vulnerablities which might be exploitable under certain conditions. Affected domains should be checked to determine which vulnerabilities might pose a risk.

Issue #21: '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 #22: 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.
