**Danvers MA (207.38.77.139)**

Overall Score: 829 / 950

Website Security: 763 / 950

-------------------------------------------------------------------------------------------------------------

# Issue #1 (+12)

Insecure SSL/TLS versions available (#1 most common vulnerability across 44 municipalities)

#Why it's an issue?

Susceptible to man-in-the-middle attacks

How to Resolve?

Identify your web server software (Apache, Nginx, IIS, etc.)

Back up your current server configuration.

Modify your server's SSL/TLS configuration to disable SSL and any versions of TLS older than 1.2.

Ensure that your server supports and is configured to prioritize newer, secure protocols like TLS 1.2 and TLS 1.3.

-------------------------------------------------------------------------------------------------------------

# Issue #2 (+18)

CAA not enabled. (#2 most common vulnerability across 44 municipalities)

#Why it's an issue?

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.

How to Resolve?

1. Identify your DNS provider: Determine which DNS provider you are using for your domain. This information is typically provided by the company where you registered your domain or where you manage your DNS settings.
2. Access your DNS management interface: Log in to your DNS provider's website or access the DNS management interface provided by your domain registrar.
3. Locate the CAA record settings: Look for an option to manage DNS records or specifically CAA records. The exact location and terminology may vary depending on your DNS provider.
4. Add a CAA record: Create a new CAA record for your domain. You will need to provide the following information:
   * Name/Host: Enter your domain name or the subdomain for which you want to add the CAA record (e.g., "danversma.gov").
   * Flag: Set the flag to 0 (zero), which indicates a critical CAA record.
   * Tag: Set the tag to "issue".
   * Value: Specify the Certification Authority (CA) that you authorize to issue certificates for your domain. You can list multiple CAs by separating them with semicolons (;). For example, if you trust Let's Encrypt and Sectigo, you can set the value to "letsencrypt.org;sectigo.com".
5. Save the changes: Once you have entered the necessary information, save the CAA record.
6. Verify the CAA record: Wait for the DNS changes to propagate, which can take some time (usually up to 24 hours). You can use online DNS lookup tools to verify that the CAA record is correctly set up for your domain.
7. Repeat the process for other domains: If you have multiple domains triggering the CAA risk, follow the same steps for each domain.

-------------------------------------------------------------------------------------------------------------

# Issue #3 (+0)

Only weak cipher suites supported in TLS 1.2 (Provisional) (#3 most common vulnerability across 44 municipalities)

#Why it's an issue?

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.

#How to Resolve?

1. Identify the web server software: Determine which web server software you are using, such as Apache HTTP Server, Nginx, Microsoft IIS, etc.
2. Update the web server software: Ensure that your web server software is up to date with the latest version, as newer versions often include security enhancements and stronger cipher suites.
3. Disable weak cipher suites: In your web server's configuration file, disable the weak cipher suites and only enable secure and strong cipher suites. Remove or comment out any cipher suites that are considered weak or vulnerable.

Enable Perfect Forward Secrecy (PFS): Perfect Forward Secrecy ensures that even if an attacker gains access to the server's private key, they cannot decrypt past communications. Enable PFS by configuring your web server to use cipher suites that support it.

1. Enable TLS 1.3: If your web server and client support it, consider enabling TLS 1.3, which is the latest version of the TLS protocol and provides enhanced security and performance benefits.
2. Obtain and install a valid SSL/TLS certificate: Ensure that you have a valid SSL/TLS certificate installed on your web server. Use a trusted certificate authority to obtain the certificate to establish secure connections with clients.
3. Test and verify the configuration: After making the necessary changes, thoroughly test your web server's configuration using online SSL/TLS testing tools or tools like Qualys SSL Labs. These tools can help identify any remaining vulnerabilities or misconfigurations.

--------------------------------------------------------------------------------------------------------------------------------------------------------