Protecting Your Web Server

Using Secure Configuration and Encryption

Xavier Belanger – October 2022

What is a “Secure” Server?

- Running proper code and applications.
- Applying patches and updates.
- Controlled access to the data.
- Backups. Backups. Backups.
- Hardened operating system.
- Authorized network traffic.
- And more…

Configuration Hardening

- Follow the recommendations from the Center for Internet Security; use the CIS Benchmarks for your operating system and web server.
- Documentation is free, registration is required.
- Two levels of configuration are provided for each item when possible.
- Not every single configuration item may be needed.

`https://www.cisecurity.org/cis-benchmarks/`

Using HTTPS

- Hypertext Transfer Protocol Secure; using TCP/443 by default.
- Provide confidentiality (network encryption) and authenticity.
- Requires a security certificate.
- Use the most recent Transport Layer Security protocol version: TLS 1.2 and TLS 1.3.
- Web servers default configuration doesn’t always provide a good security level.

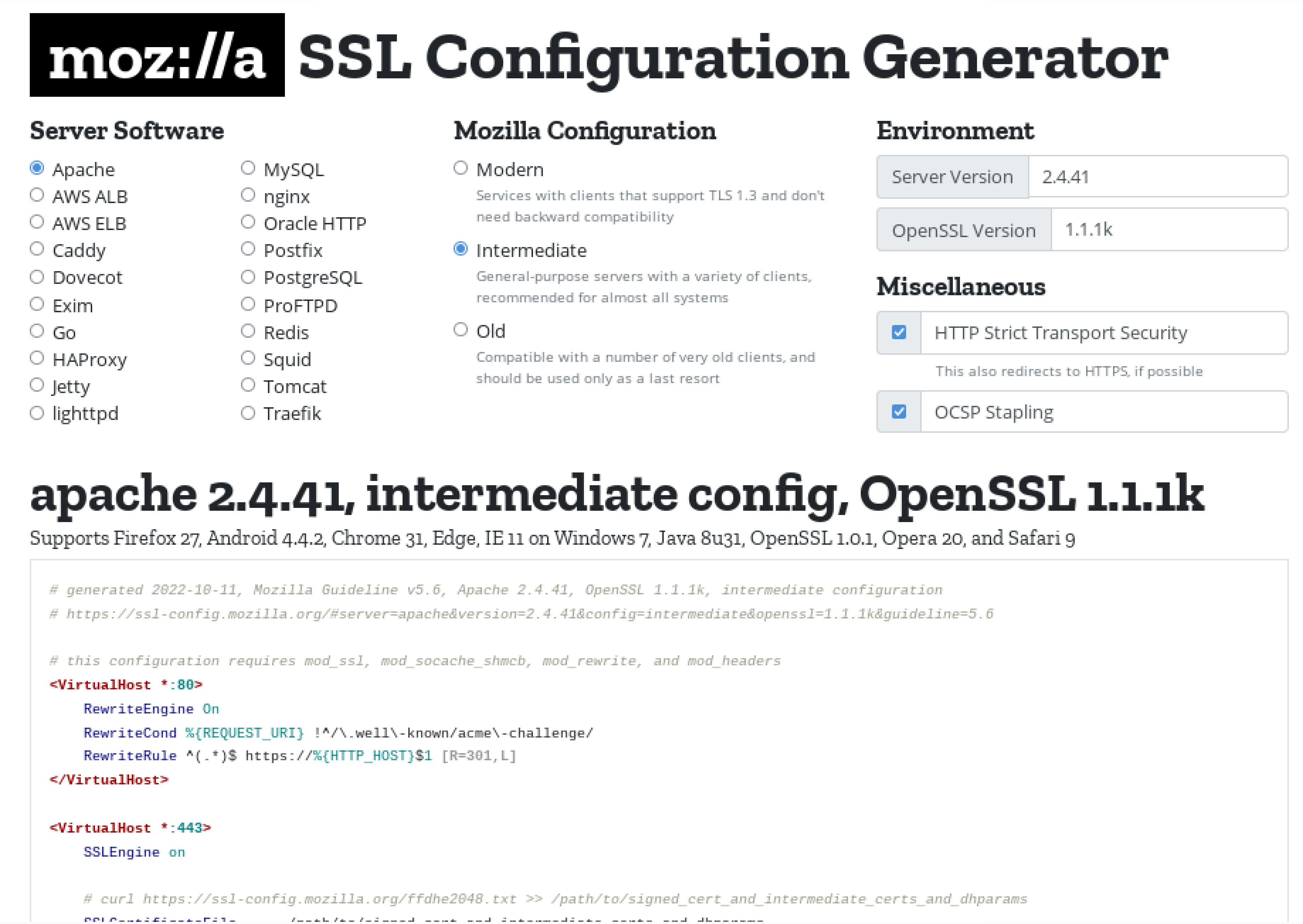
HTTPS Configuration Tools

- Adjust your configuration using the Mozilla SSL Configuration Generator.

  `https://ssl-config.mozilla.org/`

- Check the results with the Qualys SSL Labs Server Test.

  `https://www.ssllabs.com/ssltest/index.html`



moz://a SSL Configuration Generator

Server Software

● Apache
○ AWS ALB
○ AWS ELB
○ Caddy
○ Dovecot
○ Exim
○ Go
○ HAProxy
○ Jetty
○ lighttpd
○ MySQL
○ nginx
○ Oracle HTTP
○ Postfix
○ PostgreSQL
○ ProFTPD
○ Redis
○ Squid
○ Tomcat
○ Traefik

Mozilla Configuration

○ Modern
Services with clients that support TLS 1.3 and don't need backward compatibility

● Intermediate
General-purpose servers with a variety of clients, recommended for almost all systems

○ Old
Compatible with a number of very old clients, and should be used only as a last resort

Environment

Server Version: 2.4.41

OpenSSL Version: 1.1.1k

Miscellaneous

☑ HTTP Strict Transport Security
This also redirects to HTTPS, if possible

☑ OCSP Stapling

apache 2.4.41, intermediate config, OpenSSL 1.1.1k

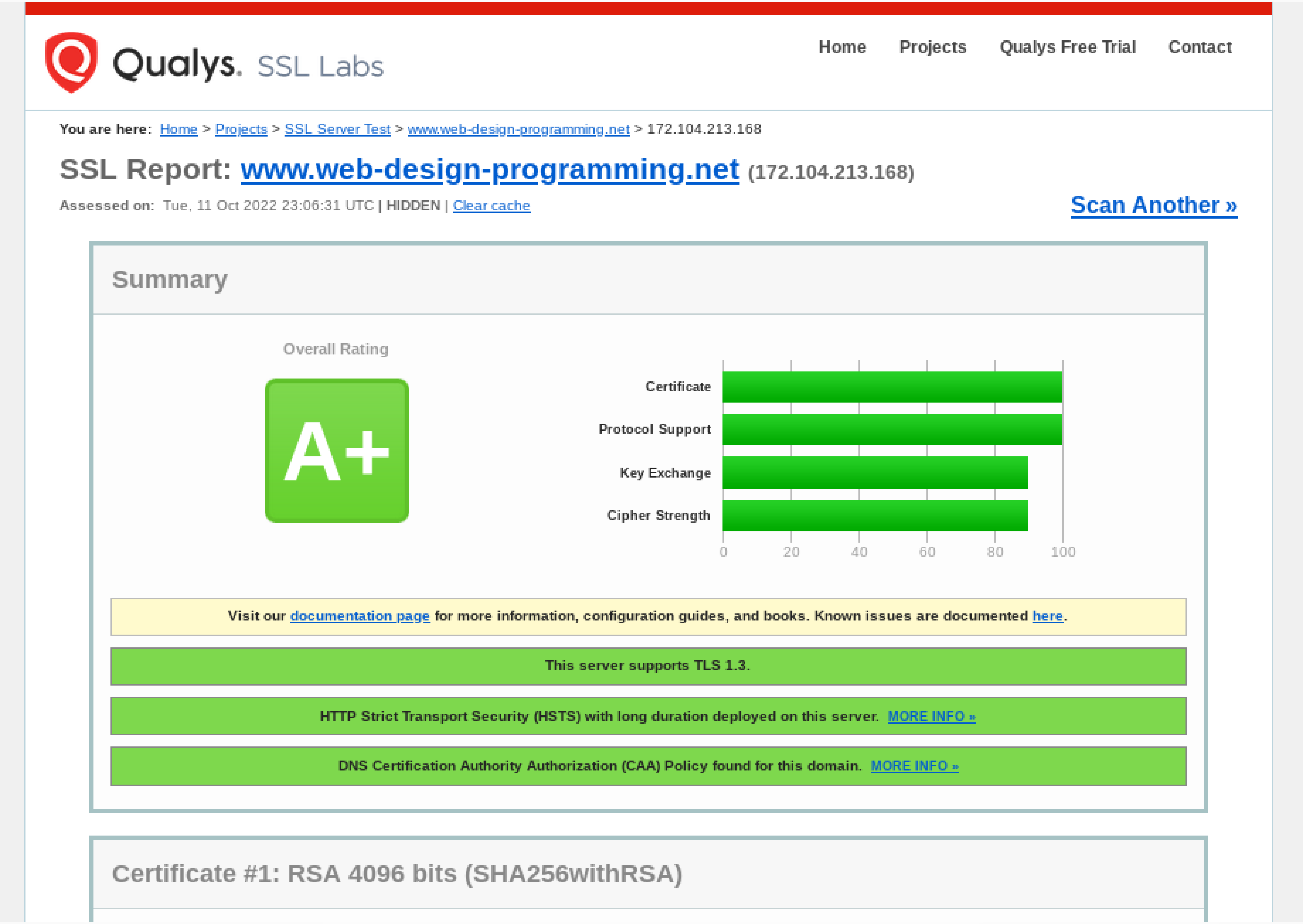
Supports Firefox 27, Android 4.4.2, Chrome 31, Edge, IE 11 on Windows 7, Java 8u31, OpenSSL 1.0.1, Opera 20, and Safari 9

```
# generated 2022-10-11, Mozilla Guideline v5.6, Apache 2.4.41, OpenSSL 1.1.1k, intermediate configuration
# https://ssl-config.mozilla.org/#server=apache&version=2.4.41&config=intermediate&openssl=1.1.1k&guideline=5.6

# this configuration requires mod_ssl, mod_socache_shmcb, mod_rewrite, and mod_headers
<VirtualHost *:80>
    RewriteEngine On
    RewriteCond %{REQUEST_URI} !^/\.well\-known/acme\-challenge/
    RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=301,L]
</VirtualHost>

<VirtualHost *:443>
    SSLEngine on

    # curl https://ssl-config.mozilla.org/ffdhe2048.txt >> /path/to/signed_cert_and_intermediate_certs_and_dhparams
    SSLCertificateFile      /path/to/signed_cert_and_intermediate_certs_and_dhparams
```



You are here: Home > Projects > SSL Server Test > www.web-design-programming.net > 172.104.213.168

SSL Report: www.web-design-programming.net (172.104.213.168)

Assessed on: Tue, 11 Oct 2022 23:06:31 UTC | HIDDEN | Clear cache

Scan Another »

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

Certificate #1: RSA 4096 bits (SHA256withRSA)

Checking a Private Server

- For a server not publicly visible on the Internet, you can use nmap to get similar results:

```
$ nmap -p T:443 -sV -sC www.example.net
```

```
$ nmap -p T:443 --script ssl-enum-ciphers www.example.net
```

https://nmap.org/

Thank you for your attention.

Time for questions and discussion.