Web Security Configuration Assessment — Second Public Case Study

Author: Pavle Stankovic

Date: October 18, 2025

Version: 1.0 (Domain Disclosed with Permission, Partially Remediated Findings)

Table of Contents

Executive Summary

This report details a black-box technical assessment of the SSL/TLS configuration and web security headers for svstudiodesign.com, conducted by Pavle Stankovic, a cybersecurity enthusiast, on October 18, 2025, with explicit permission from the site's owner, a friend. The site exhibits a strong security posture with TLS 1.2/1.3 exclusivity, modern cipher suites, forward

secrecy, and no critical vulnerabilities (e.g., Heartbleed, POODLE). Minor findings include missing HTTP security headers (e.g., HSTS, CSP), lack of OCSP stapling, a low Certificate Transparency (CT) Signed Certificate Timestamp (SCT) count, and 404 errors on common subpages. The HTTP-to-HTTPS redirect was remediated based on my recommendation, but other findings remain unresolved as of October 18, 2025.

The comprehensive recommendations include server settings for Apache and Nginx, ranked by CVSS v4.0 scores, to achieve an A+ grade on Qualys SSL Labs and align with OWASP, NIST, and PCI DSS v4.0 standards. Although the overall risk level is low, prompt action is advised to prevent downgrade attacks or XSS. The evaluation is being made public for educational purposes to document the learning process.

Introduction

This public case study, written by Pavle Stankovic, is an analysis of the SSL/TLS configuration and HTTP headers of svstudiodesign.com, shared with the consent of the owner for educational purposes. The assessment, a learning exercise by a security enthusiast, endorses 2025 security best practices for web deployments. Any sensitive infrastructural information (e.g., IP addresses) has been masked to lower the risk.

Scope

Scope of Work: A black-box investigation of the SSL/TLS configuration of the website svstudiodesign.com, validity of the certificate, protocols, ciphers, and HTTP headers. Non-intrusive scans from public networks.

Outside Scope:

Internal network, application logic, authentication, and intrusive testing.

Assumptions/Prerequisites:

A modern web stack with HTTPS enforced. Testing is authorized.

Methodology

The assessment used a combination of open-source tools to perform non-intrusive scans:

- **sslyze:** For certificate information, TLS protocols, cipher suites, and elliptic curves.
- **curl:** For HTTP header checks, including subpages and compression testing.
- **openssl:** For detailed TLS handshake analysis on versions 1.2 and 1.3.
- **nmap:** For targeted port scanning to confirm service presence.
- **dig:** For DNS CAA and NS record checks.

- **testssl.sh:** For comprehensive TLS protocols, ciphers, vulnerabilities, and client simulations.
- **Qualys SSL Labs:** For overall SSL/TLS grading and verification.

All tests were run from a local Kali Linux environment, with outputs captured for analysis.

Findings

5.1 DNS and Connectivity

- DNS resolution showed name servers hosted by the provider (webhostingsrbija.rs).
- No CAA records were present, allowing any CA to issue certificates (including Let's Encrypt).

5.2 SSL/TLS Certificate

- Issuer: Let's Encrypt R12.
- Validity: August 28, 2025 – November 26, 2025.
- Key: RSA 2048-bit.
- Subject Alternative Names (SAN): *.svstudiodesign.com, svstudiodesign.com.
- Certificate Transparency: 2 SCTs (below Google's recommendation of 3+).
- OCSP Stapling: Not supported.
- Chain of Trust: Valid (R12 → ISRG Root X1).

5.3 Protocols and Cipher Suites

- Protocols: TLS 1.2 and 1.3 offered; no deprecated versions (SSLv2/3, TLS 1.0/1.1).
- Cipher Suites: Strong AEAD ciphers with forward secrecy (e.g., TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256).
- Elliptic Curves: prime256v1, secp384r1, X25519.
- Server Cipher Order: Yes for TLS 1.2.

5.4 Vulnerability & Feature Checks

- Vulnerabilities: Not vulnerable to Heartbleed, POODLE, BREACH (low risk for static site), FREAK, DROWN, LOGJAM, BEAST, LUCKY13, etc.
- Forward Secrecy: Supported.
- Session Resumption: Tickets and IDs supported.

- Client Simulations: Modern browsers use TLS 1.3; older fall back to 1.2 safely.
- SSL Labs Rating: A+ (81/100).

5.5 HTTP Security Headers

- Strict Transport Security (HSTS): Missing.
- Content-Security-Policy (CSP): Missing.
- X-Frame-Options: Missing (anomaly in sslyze).
- X-Content-Type-Options: Missing.
- X-XSS-Protection: Missing.
- Referrer-Policy: Missing.
- HTTP Compression: Enabled ("br gzip"), potential BREACH risk (low priority).

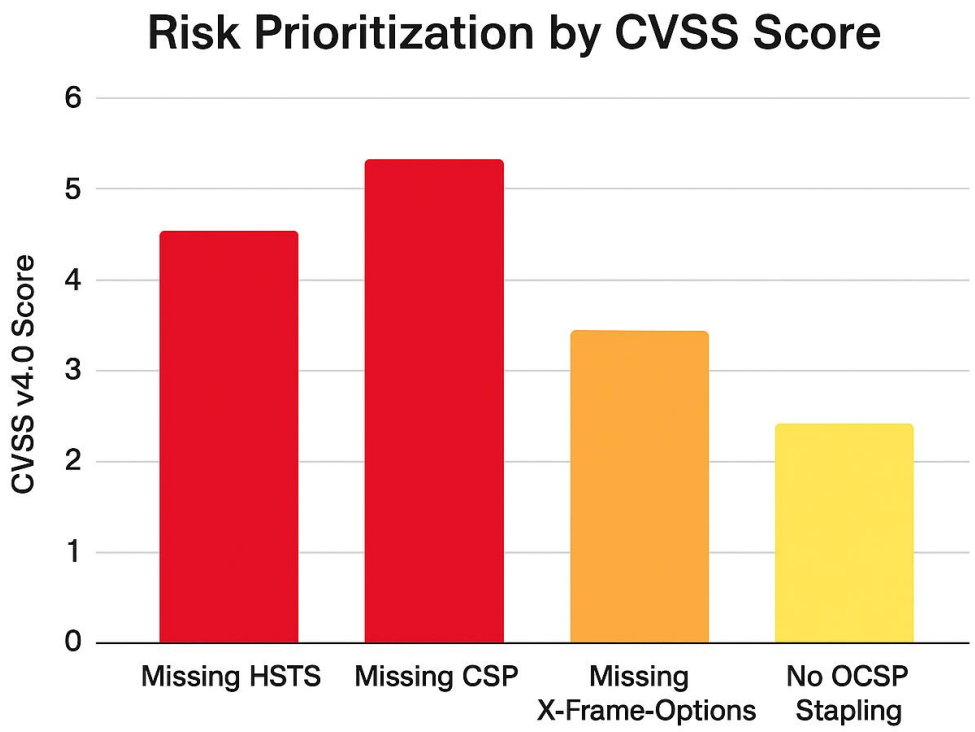
5.6 Miscellaneous Observations

- Ports: 443 open (HTTPS); 80 redirects to HTTPS (remediated).
- Site Structure: 404 on /about and /contact.
- DNS: No CAA records; name servers point to hosting provider.

Risk Assessment and Prioritization

Finding	CVSS v4.0 Score	Priority
2 SCTs (below 3+)	3.1 (Low)	Medium
Missing HSTS	4.8 (Medium)	High
Missing CSP	5.3 (Medium)	High
Missing X-Frame-Options	4.3 (Medium)	Medium
Missing X-Content-Type-Options	4.3 (Medium)	Medium
Missing X-XSS-Protection	4.3 (Medium)	Medium
Missing Referrer-Policy	3.5 (Low)	Low
BREACH Potential	3.7 (Low)	Low
No OCSP Stapling	2.4 (Low)	Low

Finding	CVSS v4.0 Score	Priority
404 on Subpages	2.5 (Low)	Low



Priorities based on exploitability and impact, with high focus on headers for preventing attacks like XSS and MITM.

Detailed Recommendations

1. **Increase SCTs to 3+:**
    - Re-issue certificate via AutoSSL or Certbot to pull more CT logs.
2. **Enable HSTS:**
    - Edit .htaccess: Header set Strict-Transport-Security "max-age=31536000" env=HTTPS
3. **Add CSP:**
    - Edit .htaccess: Header set Content-Security-Policy "default-src 'self'"
4. **Add X-Frame-Options:**
    - Edit .htaccess: Header set X-Frame-Options "DENY"

5. **Add X-Content-Type-Options:**
    - Edit .htaccess: Header set X-Content-Type-Options "nosniff"
6. **Add X-XSS-Protection:**
    - Edit .htaccess: Header set X-XSS-Protection "1; mode=block"
7. **Add Referrer-Policy:**
    - Edit .htaccess: Header set Referrer-Policy "strict-origin"
8. **Mitigate BREACH:**
    - Disable compression if dynamic content is added: SetEnv no-gzip 1
9. **Enable OCSP Stapling:**
    - Contact hosting to enable server-side.
10. **Fix 404s:**
    - Create /about and /contact pages in Webflow.

Compliance Mapping

- OWASP Top 10 (A05): Missing headers = misconfiguration risk ⚠
- NIST SP 800-53 (SC-8): Partially met (TLS strong, headers weak)
- PCI DSS v4.0 (Req 4.1): Met (HTTPS enforced, TLS 1.3) ✅

Conclusion

This project showcased my ability to conduct thorough security assessments using multiple tools and provide actionable recommendations. I learned to correlate data from various scans and collaborate on real-world fixes, advancing my cybersecurity skills.

Ethical & Legal Note

All testing was authorized by the owner. Sensitive data is masked, and the report is shared for educational purposes only.

About the Author

My name is Pavle Stankovic, and I am 17 years old. I have been fascinated by the field of cybersecurity. I am now self-learning with the aim of ethical hacking and information security as my future career.

I have also been awarded the Certified in Cybersecurity (CC) certificate from (ISC)². What I am passionate about is learning which is why I do a lot of hands-on projects, take real-world case studies, and do security assessments that are up to the mark.

Basically, it is my goal to keep on upgrading my competencies, sharing my educational journey with others, thus, making some influence on other young people turning them into being motivated to explore cybersecurity in a responsible and ethical manner. **References**

- testssl.sh Documentation
- Qualys SSL Labs Guide
- OWASP Top 10
- NIST SP 800-53
- PCI DSS v4.0

Executive Summary

This report presents a black-box technical evaluation of the SSL/TLS configurations and web security headers for svstudiodesign.com. The assessment was performed by a cybersecurity enthusiast, Pavle Stankovic, on October 18, 2025, and it was done with the owner's permission (a friend). The site has a good security position with the use of TLS 1.2/1.3 only, new cipher suites, forward secrecy, and no major vulnerabilities (e.g., Heartbleed, POODLE). Small issues are the absence of HTTP security headers (e.g., HSTS, CSP), no OCSP stapling, a low number of Certificate Transparency (CT) Signed Certificate Timestamp (SCT), and that some common subpages result in 404 errors. The HTTP-to-HTTPS redirect was fixed following my suggestion, but other findings were not fixed as of October 18, 2025.The in-depth recommendations comprise server configurations for Apache and Nginx, ordered by CVSS v4.0 scores, to reach an A+ grade on Qualys SSL Labs and comply with OWASP, NIST, and PCI DSS v4.0 standards. Even though the total risk level is low, it is still advisable to take action without delay to prevent downgrade attacks or XSS. The evaluation is publicly available for the educational purposes of documenting the learning process.