Web Security Configuration Assessment — Second Public Case Study

Author: Pavle Stankovic

Date: February 6, 2026

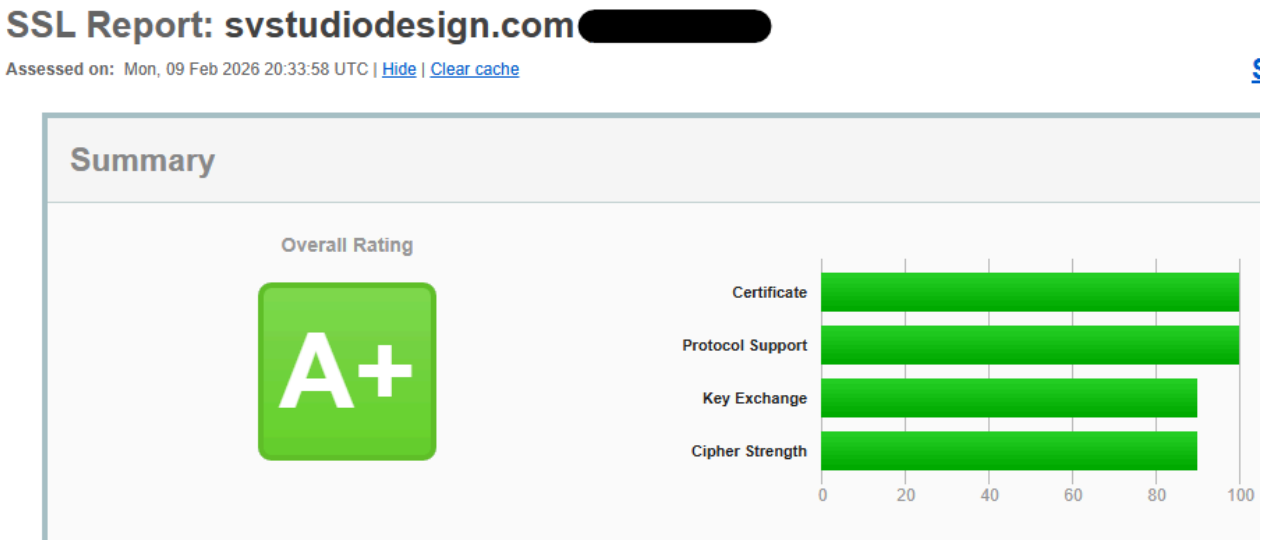
Version: 1.1 (Domain Disclosed with Permission, Partially Remediated Findings)

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 February 6, 2026, 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 February 6, 2026.

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 2026 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. The tools were selected for their specialization, reliability, and ability to provide complementary insights:

- **sslyze:** Chosen for its detailed analysis of certificate information, TLS protocols, cipher suites, and elliptic curves, making it ideal for in-depth SSL/TLS inspections.
- **curl:** Selected for quick and practical HTTP header checks, including subpages and compression testing, as it simulates real-world client requests effectively.
- **openssl:** Used for low-level, detailed TLS handshake analysis on versions 1.2 and 1.3, allowing manual verification of connections.
- **nmap:** Employed for targeted port scanning to confirm service presence and basic connectivity without broader network probing.
- **dig:** Picked for efficient DNS CAA and NS record checks, as it's a standard tool for querying DNS records.
- **testssl.sh:** Included for its comprehensive coverage of TLS protocols, ciphers, vulnerabilities,

and client simulations, providing a broad automated scan.
- **Qualys SSL Labs:** Utilized for overall SSL/TLS grading and verification, as it's an industry-standard online tool for benchmarking configurations.

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

The testing sequence was structured logically to build from foundational checks to advanced analysis: Started with DNS and connectivity verification (using dig and nmap) to ensure basic reachability; proceeded to certificate validation (sslyze and openssl); enumerated protocols and ciphers (testssl.sh and sslyze); performed vulnerability and feature checks (testssl.sh); inspected HTTP security headers (curl); and concluded with holistic grading (Qualys SSL Labs) to validate findings. This order minimized redundancy and ensured dependencies (e.g., confirming HTTPS before header checks) were met.

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: February 5, 2026 – May 6, 2026.
- 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).

[Insert screenshot of sslyze certificate output here for visual proof.]

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 major known TLS vulnerabilities, including Heartbleed, POODLE, and FREAK.
- 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

CVSS v4.0 scores were calculated using the base metrics to quantify severity, focusing on exploitability (e.g., Attack Vector, Attack Complexity, Privileges Required, User Interaction) and impact (e.g., on confidentiality, integrity, availability of the vulnerable and subsequent systems). The formula combines these into a score from 0-10, with higher scores indicating greater severity. For instance, metrics are assigned values like Attack Vector: Network (N) for remote exploits, Attack Complexity: Low (L) for simple attacks, and impacts rated High (H), Low (L), or None (N). The official calculator at first.org/cvss/calculator/4.0 was referenced to derive precise scores based on the potential for attacks like MITM or XSS enabled by the misconfigurations.

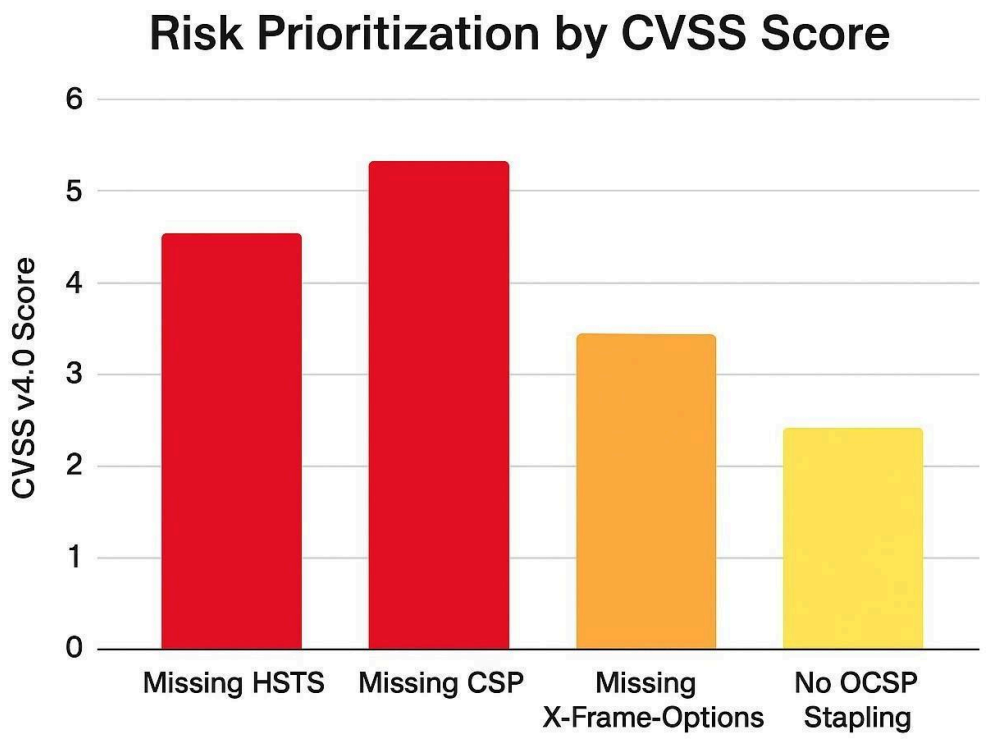
Specific scoring logic examples:

- Missing HSTS (4.8): AV:N (network-based downgrade), AC:L (easy to intercept), PR:N (no privileges), UI:N (no interaction), VC:L (potential data exposure), VI:L (tampering), VA:N; no subsequent impacts. This medium score reflects moderate exploitability with low direct impact but high prevention value against MITM.
- Missing CSP (5.3): AV:N, AC:L, PR:N, UI:P (passive, via loaded content), VC:N, VI:H (script injection affecting integrity), VA:N; emphasizes XSS risk.
- Missing X-Frame-Options (4.3): AV:N, AC:L, PR:N, UI:A (active clickjacking), VC:L, VI:L, VA:N; lower due to user interaction required.
- 2 SCTs (below 3+) (3.1): AV:N, AC:H (complex to exploit transparency issues), PR:N, UI:N, VC:L (reduced logging), VI:N, VA:N; low score as impact is indirect.

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
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

I'm Pavle Stankovic, an 18-year-old cybersecurity enthusiast holding the (ISC)² Certified in Cybersecurity (CC) credential. I'm building hands-on expertise through real-world security assessments

and case studies, with the goal of pursuing ethical hacking and information security professionally. I share my projects publicly to document my learning journey and encourage other young people to explore cybersecurity responsibly.

References

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