Web Security Configuration Assessment — Public Case Study

Author: Pavle Stankovic

Date: October 17, 2025

Version: 1.7 (Domain Disclosed with Permission, Unremediated Findings)

Table of Contents

Executive Summary

This report details a black-box technical assessment of the SSL/TLS configuration and web security headers for mundo-gol.com, conducted by Pavle Stankovic, a cybersecurity enthusiast, on October 17, 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, ROBOT). Minor findings include missing HTTP security headers (e.g., HSTS, CSP), lack of OCSP stapling, and a low Certificate Transparency (CT) Signed Certificate Timestamp (SCT) count. These findings remain unremediated as of October 17, 2025.

The comprehensive recommendations are the server settings for Apache and Nginx, ranked by CVSS v4.0 scores, to get an A+ grade on Qualys SSL Labs and be in line with the OWASP, NIST, and PCI DSS v4.0 standards. Although the overall risk level is low, it is still better to take action without delay to prevent, for instance, downgrade attacks or XSS. The evaluation is being made public for the sole purpose of education as a way 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 mundo-gol.com, which was 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 mundo-gol.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

Based on NIST SP 800-115 and OWASP Testing Guide:

Steps:

1. Passive enumeration (DNS, connectivity).
2. SSL/TLS handshake analysis.
3. Cipher suite and protocol validation.
4. HTTP header inspection.
5. Manual verification and recommendations.

Tools:

- sslyze (TLS scanning)
- nmap (port/service enumeration)
- curl, openssl (header/handshake analysis)
- Browser DevTools (cross-platform validation)

Testing was non-destructive and ethical.

Findings

DNS and Connectivity

All subdomains of mundo-gol.com resolve to a production IP address. HTTPS is enforced via HTTP-to-HTTPS redirects (301).

Evidence: curl confirmed redirects.

SSL/TLS Certificate

Valid certificate from a trusted public CA, compatible with Android, iOS, Windows, macOS.

Issue (Low Severity): Two CT SCTs detected; three or more recommended.

Evidence: OpenSSL verified chain and expiration (valid beyond 2025).

Protocols and Cipher Suites

- Disabled: TLS 1.0, 1.1 (good).
- Supported: TLS 1.2, 1.3 (TLS 1.3 prioritized).
- Ciphers: AES-GCM, ChaCha20-Poly1305 (modern).
- Forward Secrecy: Enabled (ECDHE, DHE fallback).

Evidence: sslyze confirmed secure configuration.

Vulnerability & Feature Checks

- Heartbleed: Not vulnerable, No OpenSSL issues.
- ROBOT (RSA Key Exchange): Not vulnerable, RSA disabled.
- Session Renegotiation: Secure, Prevents DoS.
- TLS Compression: Disabled, Mitigates CRIME.
- OCSP Stapling: Not supported, Low severity, Recommended for performance.

Evidence: nmap, sslyze outputs.

HTTP Security Headers

Missing headers increases risks like downgrade attacks or XSS.

- Strict-Transport-Security: Missing, Medium severity, HTTP downgrade risk.
- X-Frame-Options: Missing, Low severity, Clickjacking exposure.
- X-Content-Type-Options: Missing, Low severity, MIME sniffing attacks.
- Content-Security-Policy: Missing, Medium severity, XSS/injection risks.

Evidence: curl -I showed absent headers.

Miscellaneous Observations

- No robots.txt (neutral security, minor SEO impact).

- HTTPS responses: 200 OK with valid certificate chain.

Risk Assessment and Prioritization

Findings rated using CVSS v4.0:

- Missing HSTS: CVSS Score 5.3, Medium severity, Vector String AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:L

- Missing CSP: CVSS Score 5.3, Medium severity, Vector String AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

- Missing X-Frame-Options: CVSS Score 4.2, Low severity, Vector String AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:N/SI:N/SA:L

- Missing X-Content-Type-Options: CVSS Score 4.2, Low severity, Vector String AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:N/SI:N/SA:L

- OCSP Stapling Not Supported: CVSS Score 3.1, Low severity, Vector String AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N

- Low SCT Count (2): CVSS Score 2.7, Low severity, Vector String AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N

Overall Posture: Low risk; remediation advised to address medium-severity issues.

Detailed Recommendations

Below are actionable steps to address the unremediated findings, prioritized by severity, with server configurations and verification methods.

1. Enable Strict-Transport-Security (HSTS) (Medium)

Issue: Missing HSTS risks HTTP downgrade attacks.

Impact: Attackers may intercept unencrypted traffic.

Recommendation:

- Enable HSTS with max-age of 1 year, including subdomains.

- Consider HSTS preload (https://hstspreload.org/) after testing.

Apache Configuration:

```
   <VirtualHost *:443>
       Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
   </VirtualHost>
```

Nginx Configuration:

```
   server {
       listen 443 ssl;
       add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
   }
```

Verification:

- Run: curl -s -D- https://mundo-gol.com | grep Strict
- Check: Strict-Transport-Security: max-age=31536000; includeSubDomains
- Use SSL Labs (https://www.ssllabs.com/ssltest/).

Priority: High (quick fix, significant impact).

2. Implement Content-Security-Policy (CSP) (Medium)

Issue: Missing CSP increases XSS/injection risks.

Impact: Malicious scripts could execute in browsers.

Recommendation:

- Apply restrictive CSP, refine for site needs.

Apache Configuration:

```
   <VirtualHost *:443>
       Header set Content-Security-Policy "default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self';"
   </VirtualHost>
```

Nginx Configuration:

```
   server {
        listen 443 ssl;
        add_header Content-Security-Policy "default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self';" always;
    }
```

Verification:

- Run: curl -s -D- https://mundo-gol.com | grep Content-Security-Policy
- Test with https://csp-evaluator.withgoogle.com/.

Priority: High (mitigates XSS).

3. Add X-Frame-Options (Low)

Issue: Missing header risks clickjacking.

Impact: Site could be embedded in malicious iframes.

Recommendation:

- Set to DENY.

Apache Configuration:

```
    <VirtualHost *:443>
        Header always set X-Frame-Options "DENY"
    </VirtualHost>
```

Nginx Configuration:

```
    server {
        listen 443 ssl;
        add_header X-Frame-Options "DENY" always;
    }
```

Verification:

- Run: curl -s -D- https://mundo-gol.com | grep X-Frame-Options

Priority: Medium.

4. Add X-Content-Type-Options (Low)

Issue: Missing header risks MIME sniffing.

Impact: Browsers may misinterpret content types.

Recommendation:

- Set to nosniff.

Apache Configuration:

```
<VirtualHost *:443>
    Header always set X-Content-Type-Options "nosniff"
</VirtualHost>
```

Nginx Configuration:

```
server {
    listen 443 ssl;
    add_header X-Content-Type-Options "nosniff" always;
}
```

Verification:

- Run: `curl -s -D- https://mundo-gol.com | grep X-Content-Type-Options`

Priority: Medium.

5. Enable OCSP Stapling (Low)

Issue: Not supported, slowing validation.

Impact: Increased latency for clients.

Recommendation:

- Enable OCSP stapling.

Apache Configuration:

```
<VirtualHost *:443>
    SSLUseStapling On
    SSLStaplingCache "shmcb:/path/to/ssl_stapling_cache(128000)"
```

```
        SSLStaplingReturnResponderErrors Off
    </VirtualHost>
```

Nginx Configuration:

```
    server {
        listen 443 ssl;
        ssl_stapling on;
        ssl_stapling_verify on;
        resolver 8.8.8.8;
    }
```

Verification:

- Run: openssl s_client -connect mundo-gol.com:443 -status

Priority: Low.

6. Increase CT SCTs to 3+ (Low)

Issue: Two SCTs; three or more recommended.

Impact: Limited CT logging reduces transparency.

Recommendation:

- Reissue certificate with 3+ SCTs.
- Use Certbot: certbot certonly --webroot -w /var/www/html -d mundo-gol.com --must-staple.

Verification:

- Run: openssl s_client -connect mundo-gol.com:443 | openssl x509 -noout -text
- Check: https://crt.sh/

Priority: Low.

7. General Best Practices

- Automate Renewals: Use Certbot (certbot renew --quiet).

- Monitor: Regular SSL Labs scans, Nagios for expiry.

- Post-Quantum Prep: Monitor NIST PQC standards (e.g., CRYSTALS-Kyber).

Compliance Mapping

- OWASP Top 10 (2021, applicable 2025): Addresses A05:2021 (Security Misconfiguration).

- NIST SP 800-52 Rev. 2: TLS 1.3 priority, cipher restrictions.

- PCI DSS v4.0: Requirement 4 (Encrypt transmission).

- GDPR/HIPAA: Encryption for data protection.

Conclusion

A student exercise audit by Pavle Stankovic of mundo-gol.com has verified a strong TLS configuration without any serious security issues. Still, the unremedied results (missing headers, OCSP stapling, low SCT count) should be fixed as soon as possible to be in line with 2025 best practices and get an A+ rating from Qualys SSL Labs.

Ethical & Legal Note

This case study features the domain mundo-gol.com. Permission was granted by the owner via email on October 17, 2025, a friend of the author, for the author's educational purposes only. The assessment was carried out as a learning exercise by a student, Pavle Stankovic, in October 2025. Testing was allowed, non-intrusive, and results were unremediated as of October 17, 2025. No sensitive infrastructure details (e.g., IP addresses) are revealed. Do not attempt to compromise vulnerabilities using this report.

About the Author

Pavle Stankovic, a cybersecurity enthusiast and student experimenting with web security assessments.

Contact:

- Email: stankovic.pavle16@gmail.com

- LinkedIn: linkedin.com/in/pavle-stanković-914694386

References

- Qualys SSL Labs: https://www.ssllabs.com/projects/best-practices/

- SSL.com TLS Best Practices: https://www.ssl.com/guide/ssl-best-practices/

- OWASP Top 10: https://owasp.org/www-project-top-ten/

- NIST SP 800-52: Guidelines for TLS Implementations