Technical Report: Test Secure Socket Layer (SSL) and Transport Layer Security (TLS) Configurations.

1.Introduction

Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), are cryptographic protocols that ensure secure communication over the Internet. Testing SSL/TLS configurations is crucial for identifying protocol vulnerabilities, weak cipher suites, expired certificates, and overall web server security posture. This report summarizes the SSL and TLS security testing for two websites to analyze their configuration, detect flaws, and provide mitigation strategies.

2. Tools Used

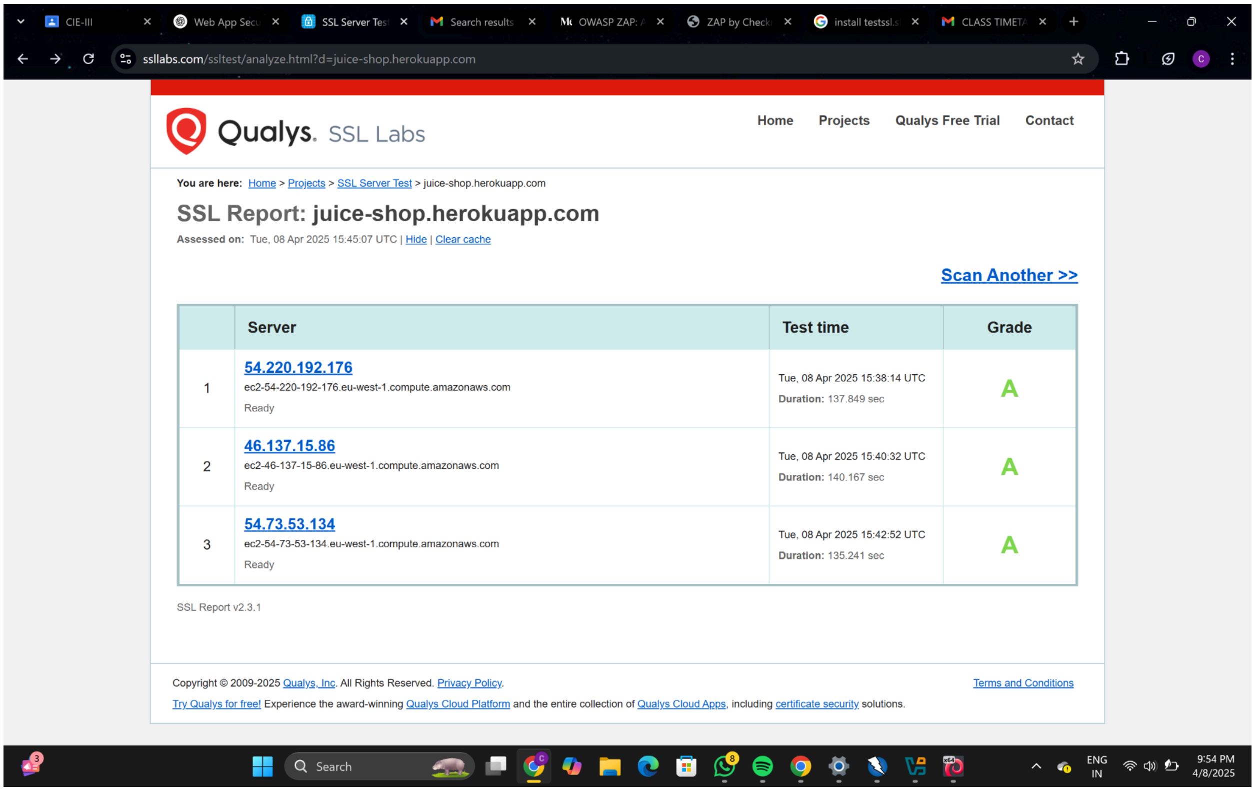
Qualys SSL Labs – SSL/TLS Server Test

- **Website:** https://www.ssllabs.com/ssltest
- **Purpose:** Scans websites for SSL/TLS implementation and grades their security.
- **Key Features:**
  - Protocol support check (SSL 2.0 to TLS 1.3)
  - Cipher suite strength
  - Certificate chain analysis
  - Forward Secrecy and HSTS check
  - Identifies vulnerabilities like POODLE, BEAST, FREAK, etc.

3. Step-by-Step Execution

- **Step 1: Launch SSL Labs Tool**

    - Visit: https://www.ssllabs.com/ssltest
    - Input URL of the website to test
- **Step 2: Perform Scan on Websites**
    - **Website 1: juice-shop.herokuapp.com**
        - Entered URL, scan started
        - Results include detailed TLS/SSL configuration



You are here: Home > Projects > SSL Server Test > juice-shop.herokuapp.com

SSL Report: juice-shop.herokuapp.com

Assessed on: Tue, 08 Apr 2025 15:45:07 UTC | Hide | Clear cache

Scan Another >>

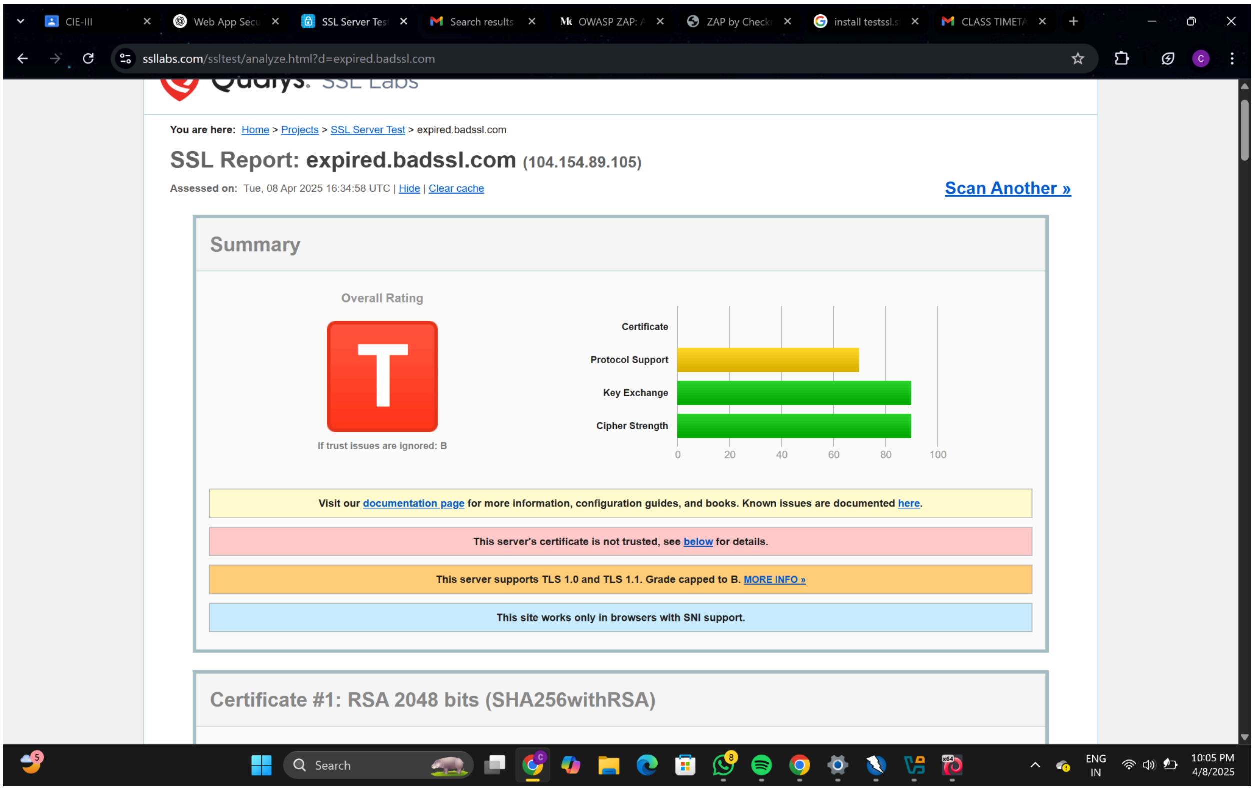
	Server	Test time	Grade
1	54.220.192.176 ec2-54-220-192-176.eu-west-1.compute.amazonaws.com Ready	Tue, 08 Apr 2025 15:38:14 UTC **Duration:** 137.849 sec	A
2	46.137.15.86 ec2-46-137-15-86.eu-west-1.compute.amazonaws.com Ready	Tue, 08 Apr 2025 15:40:32 UTC **Duration:** 140.167 sec	A
3	54.73.53.134 ec2-54-73-53-134.eu-west-1.compute.amazonaws.com Ready	Tue, 08 Apr 2025 15:42:52 UTC **Duration:** 135.241 sec	A

SSL Report v2.3.1

Copyright © 2009-2025 Qualys, Inc. All Rights Reserved. Privacy Policy. Terms and Conditions

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.

- Results include detailed TLS/SSL configurations
    - **Website 2: expired.badssl.com**
        - Entered URL, scan initiated
        - Results showed multiple issues



You are here: Home > Projects > SSL Server Test > expired.badssl.com

SSL Report: expired.badssl.com (104.154.89.105)

Assessed on: Tue, 08 Apr 2025 16:34:58 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

If trust issues are ignored: B

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

This server's certificate is not trusted, see below for details.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This site works only in browsers with SNI support.

Certificate #1: RSA 2048 bits (SHA256withRSA)

4. Findings & Analysis

Website 1: juice-shop.herokuapp.com

Test Category	Result
SSL Version Support	❌ SSL 2.0/3.0 Disabled (Good)
TLS Version Support	✅ TLS 1.2, ✅ TLS 1.3
Certificate	✅ Valid, not expired
Cipher Suites	✅ Strong (ECDHE, AES-GCM)
Forward Secrecy	✅ Enabled
HSTS (Strict Transport)	✅ Present
Compression & Renegotiation	✅ Secure
Vulnerabilities	❌ None Detected

SSL/TLS Grade (Qualys)	🟢 Grade: A

Website 2: expired.badssl.com

Test Category	**Result**
SSL Version Support	⚠️ Might still support SSL 3.0
TLS Version Support	❌ Only TLS 1.0, 1.1 supported
Certificate	❌ Expired Certificate
Cipher Suites	⚠️ Outdated, less secure
Forward Secrecy	❌ Not Enabled
HSTS (Strict Transport)	❌ Not Present
Vulnerabilities	⚠️ Possible protocol downgrade risks
SSL/TLS Grade (Qualys)	🔴 Grade: T (Trust issues)

5. Identified Authentication Vulnerabilities

- **juice-shop.herokuapp.com**
  - No major authentication vulnerabilities detected
  - Uses valid certificate, secure TLS, and strong encryption
- **expired.badssl.com**
  - **Expired Certificate:** Browser shows warning; not trustworthy
  - **Outdated TLS Protocols:** TLS 1.0 and 1.1 are deprecated
  - **Weak Cipher Suites:** Potential risk of downgrade attacks
  - **No Forward Secrecy or HSTS:** Makes it vulnerable to MITM attacks

6. Security Recommendations & Mitigation Strategies

Issue	**Recommendation**
Deprecated TLS/SSL Support	Disable SSL 3.0, TLS 1.0, and TLS 1.1
Expired Certificate	Renew certificates and implement auto-renewal
Weak Cipher Suites	Use only strong ciphers: AES-GCM, ECDHE, CHACHA20
No Forward Secrecy	Enable ECDHE for forward secrecy
No HSTS	Implement HSTS for downgrade prevention
No TLS 1.3 Support	Upgrade server to support TLS 1.3
Lack of Certificate Transparency Logs	Enable CT logging to improve trustworthiness

7. Conclusion

This SSL/TLS configuration test revealed that:

- juice-shop.herokuapp.com follows best practices for secure communication and passes all SSL/TLS compliance checks.

- expired.badssl.com fails critical security checks due to outdated protocols, expired certificates, and missing modern protections.

Regular audits of SSL/TLS configurations, automatic certificate renewals, and upgrading to the latest secure protocols (like TLS 1.3) are essential to ensure robust web application security.