SSL/TLS Configuration Assessment Report

Target: www.itsecgames.com
Tool Used: testssl.sh (v3.2)
Full Command: testssl.sh --html --wide www.itsecgames.com

Certificate Link : https://www.ssllabs.com/ssltest/analyze.html?d=www.itsecgames.com

---

Executive Summary

The SSL/TLS configuration for www.itsecgames.com is **suboptimal and contains several security misconfigurations**. The most critical issue is the support for **deprecated and insecure protocols (TLS 1.0 and 1.1)**. The certificate itself is valid and from a trusted authority, but the overall configuration weakens cryptographic strength and fails to meet modern security compliance standards (e.g., PCI DSS). The overall rating is a **B**.

---

1. Certificate Health Assessment

Finding: The certificate is **healthy and valid**, but requires monitoring for expiration.

Detailed Analysis:

Parameter	Value	Analysis
Issuer	Let's Encrypt	Trusted Certificate Authority (Good).
Validity Period	From: Apr 11, 2024 → To: **Jul 11, 2024**	The certificate is currently valid. **Note: It expires in approximately 2 months.** Ensure automatic renewal is functioning.
Signature Algorithm	SHA256withRSA	Secure (Good).

Parameter	Value	Analysis
Key Size	2048 bit RSA	Meets minimum modern requirements (Adequate).
Subject Alternative Names (SANs)	www.itsecgames.com, itsecgames.com	Covers both www and non-www domains (Good).
OCSP Stapling	Offered	Improves privacy and performance by not requiring clients to contact the CA for revocation status (Good).
Certificate Transparency	Yes (3 logs)	The certificate is logged in public CT logs, helping to detect maliciously issued certs (Good).

Verdict: PASS. The certificate is properly configured and from a trusted CA. No immediate action is needed, but calendar a reminder for expiration.

---

2. Protocol Support

Finding: The server supports **deprecated and vulnerable protocols**, which is the most significant security flaw.

Detailed Analysis (Direct from testssl.sh output):

text

```
Testing protocols via sockets except NPN+ALPN


 SSLv2     not offered (OK)
 SSLv3     not offered (OK)
```

```
TLS 1     offered (deprecated)

TLS 1.1   offered (deprecated)

TLS 1.2   offered (OK)

TLS 1.3   offered (OK): final
```

Vulnerability Analysis:

- **TLS 1.0 (1999) & TLS 1.1 (2006):** These protocols are **officially deprecated**. They contain known vulnerabilities:
  - **BEAST** (CVE-2011-3389): Affects TLS 1.0 and allows plaintext recovery.
  - Lack of support for modern, secure cipher suites.
- **Impact:** Attackers can potentially force a connection downgrade to these weaker protocols to exploit their vulnerabilities and decrypt sensitive traffic, especially from older clients.
- **Compliance:** Supporting these protocols is a direct violation of PCI DSS and other security standards.

Verdict: FAIL. This is a critical misconfiguration that must be remediated.

---

3. Cipher Suite Strength

Finding: The server supports a wide range of cipher suites, including **weak and obsolete algorithms**.

Detailed Analysis (Excerpt from testssl.sh):
The server negotiates strong ciphers by default for modern clients (e.g., TLS_AES_128_GCM_SHA256 for TLS 1.3). However, it also supports weak ciphers for backward compatibility.

Weak Ciphers Detected:

text

```
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)   ECDH secp256r1 (eq. 3072 bits RSA) FS   WEAK<
112

TLS_RSA_WITH_RC4_128_SHA          (0x5)   ECDH secp256r1 (eq. 3072 bits RSA) FS   WEAK<
128
```

```
TLS_RSA_WITH_RC4_128_MD5           (0x4)   ECDH secp256r1 (eq. 3072 bits RSA) FS   WEAK<
128
```

- **3DES:** Has a small effective key size (112 bits) and is computationally expensive, making it vulnerable to sweet32-like attacks. **Disabled by default in modern browsers.**
- **RC4:** Contains cryptographic flaws and is considered completely broken. **Disabled by default in modern browsers.**

Impact: While modern browsers will not select these ciphers, legacy clients could be forced to use them, leading to weak encryption that is vulnerable to attack.

Verdict: FAIL. The presence of these weak ciphers is a security misconfiguration.

---

4. Key Exchange Support

Finding: The server supports both modern (Forward Secrecy) and older key exchange mechanisms.

Detailed Analysis:

- **Forward Secrecy (FS): Supported with modern browsers.** This means that even if the server's private key is compromised in the future, it cannot be used to decrypt past communications that used FS ciphers. This is a **best practice**.
- **Non-Forward Secrecy Ciphers:** Also supported (e.g., TLS_RSA_WITH_* ciphers). These are less secure and should be disabled in favor of FS-only ciphers.

Verdict: PARTIAL. Support for Forward Secrecy is good, but the continued support for non-FS ciphers weakens the overall configuration.

---

5. Vulnerability Testing

Finding: The server is not vulnerable to the most common historical SSL vulnerabilities.

Detailed Analysis (Direct from testssl.sh output):

text

```
Testing vulnerabilities


 Heartbleed (CVE-2014-0160)            not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                    not vulnerable (OK)
 Ticketbleed (CVE-2016-9244)            not vulnerable (OK)
 ROBOT                                  not vulnerable (OK)
 Secure Renegotiation (RFC 5746)        supported (OK)
 Secure Client-Initiated Renegotiation  not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)             not vulnerable (OK)
 BREACH (CVE-2013-3587)                 no HTTP compression (OK)  - only supplied "/"
 POODLE, SSL (CVE-2014-3566)            not vulnerable (OK)
 TLS_FALLBACK_SCSV (RFC 7507)           No fallback possible (OK), no protocol below TLS 1.2 offered
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    not vulnerable (OK)
 FREAK (CVE-2015-0204)                  not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable (OK)
 LOGJAM (CVE-2015-4000)                 not vulnerable (OK)
 BEAST (CVE-2011-3389)                  not vulnerable (OK), no SSL3 or TLS1
 LUCKY13 (CVE-2013-0169)                not vulnerable (OK)
 Winshock (CVE-2014-6321)               not vulnerable (OK)
```

Verdict: PASS. The server is not susceptible to a wide range of famous cryptographic vulnerabilities. This is positive.

Prioritized Findings & Recommendations

Priority	Finding	Impact	Recommendation
High	Support for TLS 1.0 and 1.1	Vulnerable to downgrade attacks and cryptographic	**Immediately disable TLS 1.0 and 1.1** in the web server's SSL configuration.

Priority	Finding	Impact	Recommendation
		exploits (BEAST). Compliance failure.	
Medium	Support for Weak Ciphers (3DES, RC4)	Weak encryption for legacy clients.	**Disable weak ciphers** (RC4, 3DES, NULL, EXPORT-grade ciphers). Create a modern cipher suite that prioritizes AEAD ciphers (e.g., AES-GCM, ChaCha20).
Medium	Support for Non-FS Ciphers	Compromise of server's private key could lead to decryption of past traffic.	**Prefer Forward Secrecy** by reordering cipher suites to prioritize ECDHE and DHE, and disable plain RSA key exchange.
Low	Certificate Expiration	Service disruption if certificate expires.	**Monitor certificate expiration.** Ensure Let's Encrypt auto-renewal is configured and tested.
Best Practice	Missing HTTP Security Headers	Unrelated to TLS, but noted by the tool.	Implement Strict-Transport-Security (HSTS) header to enforce HTTPS.

Conclusion

The SSL/TLS configuration for www.itsecgames.com requires immediate attention. While the certificate itself is healthy and the server is not vulnerable to major historical bugs, the support for deprecated protocols and weak ciphers significantly undermines its security posture.