

# Security Assessment Report

**Target:** <http://www.itsecgames.com>

**Date of Assessment:** 15–16 Sept 2025

**Assessor:** Rakshit Agarwal

## 1. Executive Summary

A comprehensive security assessment of **itsecgames.com** was performed using manual analysis and publicly available tools (Snyk and SSL Labs).

The results indicate significant weaknesses:

- The site is available over **unencrypted HTTP** without enforced HTTPS redirection.
- The SSL/TLS certificate is **expired, self-signed, and not trusted**.
- Deprecated protocols (TLS 1.0/1.1) and weak ciphers are still supported.
- Several **critical security headers are missing**.
- The server discloses software details that could aid attackers.

These findings place the site at **high risk of exploitation**, including man-in-the-middle (MITM) attacks, spoofing, downgrade attacks, and client-side vulnerabilities.

### Overall Ratings:

- **Snyk:** Grade F (due to missing headers and no HTTPS enforcement)
- **SSL Labs:** Grade T (certificate not trusted, expired, hostname mismatch)

## 2. Findings

### 2.1 HTTP Security Headers (Snyk Scan)

#### Observations:


- Content-Security-Policy: Missing
- X-Frame-Options: Missing
- X-Content-Type-Options: Missing
- Referrer-Policy: Missing
- Permissions-Policy: Missing

**Severity:** High

**Impact:** Increases the risk of Cross-Site Scripting (XSS), clickjacking, MIME sniffing, and information leakage.

**Recommendation:** Implement the missing headers in the Apache configuration.

### Security Report Summary



Site:	<a href="http://www.itsecgames.com/">http://www.itsecgames.com/</a> - (Scan again over https)
IP Address:	31.3.96.40
Report Time:	15 Sep 2025 11:13:33 UTC
Headers:	<div><div>✗ Content-Security-Policy</div><div>✗ X-Frame-Options</div><div>✗ X-Content-Type-Options</div><div>✗ Referrer-Policy</div><div>✗ Permissions-Policy</div></div>
Warning:	Grade capped at A, please see warnings below.
Advanced:	Ouch, you should work on your security posture immediately: <a href="#">Start Now</a>

### Missing Headers

<b>Content-Security-Policy</b>	<a href="#">Content Security Policy</a> is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
<b>X-Frame-Options</b>	<a href="#">X-Frame-Options</a> tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
<b>X-Content-Type-Options</b>	<a href="#">X-Content-Type-Options</a> stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
<b>Referrer-Policy</b>	<a href="#">Referrer Policy</a> is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
<b>Permissions-Policy</b>	<a href="#">Permissions Policy</a> is a new header that allows a site to control which features and APIs can be used in the browser.

## 2.2 SSL/TLS and Certificates (SSL Labs Scan)

### Certificate Issues:

- Certificate expired on 22 May 2025.
- Self-signed certificate, not trusted by browsers.
- Hostname mismatch (issued for web.mmebvba.com, not itsecgames.com).
- No Certificate Transparency logs.
- No revocation information (OCSP/CRL).

### Protocol and Cipher Issues:

- TLS 1.0 and TLS 1.1 enabled (deprecated, insecure).
- TLS 1.2 supported; TLS 1.3 not supported.
- Weak ciphers (AES-CBC, CAMELLIA) allowed.
- No forward secrecy with reference browsers.

### Other SSL/TLS Issues:

- No HSTS (HTTP Strict Transport Security).
- No OCSP stapling.

- Vulnerable to BEAST attack (TLS 1.0 with AES-CBC).

**Severity:** Critical

**Impact:** Users cannot establish a trusted connection; attackers can exploit weak protocols and ciphers.

**Recommendation:** Deploy a valid CA-signed certificate, disable weak protocols/ciphers, and enable TLS 1.3 with strong cipher suites.



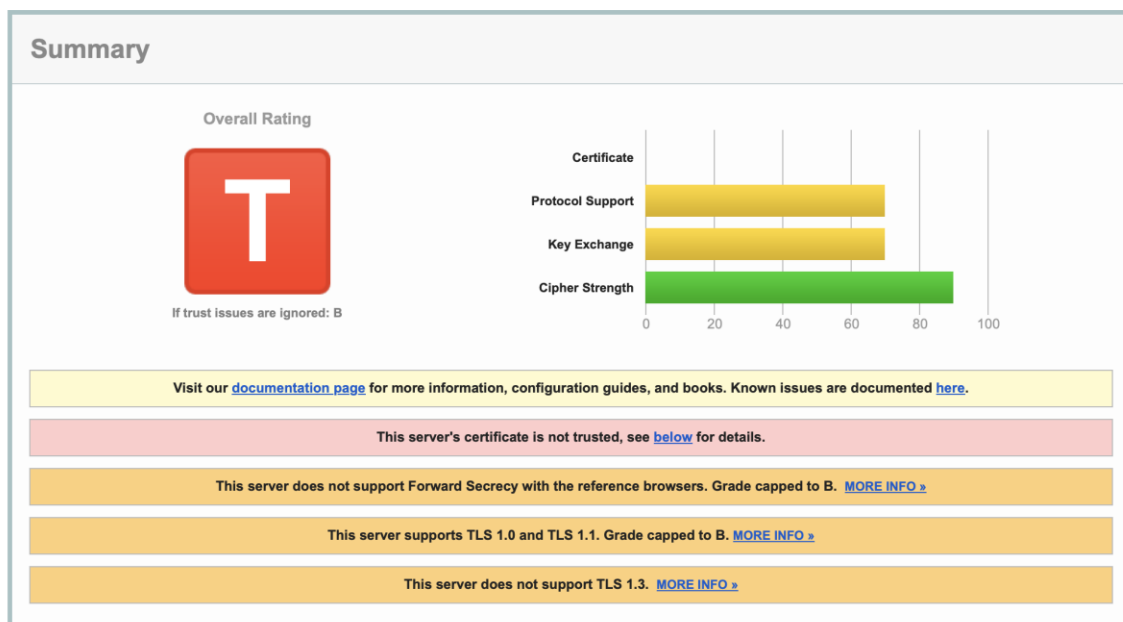
[Home](#) [Projects](#) [Qualys Free Trial](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.itsecgames.com

## SSL Report: www.itsecgames.com (31.3.96.40)

Assessed on: Mon, 15 Sep 2025 11:23:05 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)



## 2.3 DNS and Redirection (Manual Verification)

### Observations:

- <http://itsecgames.com> → responds with HTTP/1.1 200 OK (Apache).
- <https://itsecgames.com> → redirects to <https://mmebvba.com>.
- <https://mmebvba.com> → responds with headers (X-Frame-Options: SAMEORIGIN, X-Content-Type-Options: nosniff) but discloses CMS as **Drupal 7**, which is end-of-life as of January 2025.
- No CAA records found in DNS.

**Severity:** High

**Impact:** Redirection to another domain may confuse users and increase phishing risk; outdated CMS introduces known vulnerabilities.

**Recommendation:** Upgrade CMS to a supported version, add CAA records, and ensure HTTPS is served directly on itsecgames.com if intended for production.

```
Last login: Sat Sep 13 01:45:18 on console
[(base) rakshit@Rakshits-MacBook-Pro ~ % curl -I http://www.itsecgames.com/
HTTP/1.1 200 OK
Date: Mon, 15 Sep 2025 11:21:34 GMT
Server: Apache
Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT
ETag: "e43-5d7959bd3c800"
Accept-Ranges: bytes
Content-Length: 3651
Vary: Accept-Encoding
Content-Type: text/html

[(base) rakshit@Rakshits-MacBook-Pro ~ % curl -I https://www.itsecgames.com/ -k --max-time 10
HTTP/1.1 301 Moved Permanently
Date: Tue, 16 Sep 2025 10:16:03 GMT
Server: Apache
Location: https://www.mmebvba.com
Content-Type: text/html; charset=iso-8859-1

[(base) rakshit@Rakshits-MacBook-Pro ~ % curl -I https://www.mmebvba.com/
HTTP/1.1 200 OK
Date: Tue, 16 Sep 2025 10:30:28 GMT
Server: Apache
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
X-Generator: Drupal 7 (http://drupal.org)
Link: <https://www.mmebvba.com/>; rel="canonical",<https://www.mmebvba.com/>; rel="shortlink"
Content-Type: text/html; charset=utf-8

(base) rakshit@Rakshits-MacBook-Pro ~ % █
```

## 2.4 Server Banner Disclosure

### Observations:

- Server header reveals Apache.

**Severity:** Low

**Impact:** Discloses server software, which attackers may exploit using known vulnerabilities.

**Recommendation:** Hide server version using ServerTokens Prod and ServerSignature Off in Apache configuration.

### 3. Risk Analysis

Category	Severity	Impact
HTTP only (no HTTPS redirection)	Critical	Unencrypted traffic, MITM attacks
Expired, self-signed certificate	Critical	No trust, spoofing possible
TLS 1.0/1.1 enabled	Critical	Vulnerable to downgrade and BEAST attacks
Outdated CMS (Drupal 7)	High	Known unpatched vulnerabilities
Missing security headers	High	XSS, clickjacking, information leakage
Weak ciphers enabled	High	Reduced resistance to brute-force
No HSTS / OCSP stapling	Medium	Downgrade and revocation-checking issues
Server banner disclosure	Low	Information leakage

### 4. Recommendations

#### 4.1 SSL/TLS Hardening

- Deploy a valid CA-signed certificate for itsecgames.com.
- Enable TLS 1.2 and TLS 1.3; disable TLS 1.0 and TLS 1.1.
- Remove weak ciphers; prefer strong ECDHE-based suites.
- Enable Forward Secrecy, HSTS, and OCSP stapling.

#### 4.2 Security Headers

- Add the following headers:
  - Content-Security-Policy
  - X-Frame-Options
  - X-Content-Type-Options
  - Referrer-Policy
  - Permissions-Policy

#### 4.3 DNS and CMS

- Add CAA records to control certificate issuance.
- Upgrade CMS to a supported version (Drupal 10+).
- Ensure redirect to external domain (mmebvba.com) is intentional and documented.

#### 4.4 Server Configuration

- Update Apache to the latest stable version.
- Hide server version information.
- Periodically test with SSL Labs and header-checking tools.

## 5. Conclusion

The assessment of **itsecgames.com** revealed multiple critical security issues, including the absence of HTTPS enforcement, expired and untrusted certificates, insecure TLS protocols, missing headers, and outdated CMS software.

Without immediate remediation, the site remains vulnerable to interception, spoofing, downgrade attacks, and exploitation of known vulnerabilities.

**Final Risk Posture:** Insecure – Immediate remediation required.