AccuKnox Security Assessment Report

Vulnerability and SSL/TLS Analysis of

`www.itsecgames.com`

Contents

1. Methodology and Tools

Non-destructive reconnaissance and automated scanning were conducted on the publicly hosted endpoint `http://www.itsecgames.com/`. The objective was to identify potential vulnerabilities, misconfigurations, outdated software, and SSL/TLS issues.

Tools used (with raw outputs preserved as evidence) include:

- **Nikto** – Web server vulnerability scanning.
- **Nmap** – Network and port enumeration.
- **Gobuster** – Directory and file discovery.
- **curl** – HTTP header and banner inspection.
- **SSL Labs / testssl.sh** – Certificate and TLS analysis.

All command outputs, timestamps, and logs are preserved in the `evidence/` directory.

2. Prioritized Findings (Summary Table)

ID	Finding	Severity	Evidence (Tool & Snippet)	Mitigation
F1	Missing `X-Frame-Options` Header	Medium	Nikto: "GET /: The anti-clickjacking X-Frame-Options header is not present."	Add header in Apache: `Header always set X-Frame-Options "DENY"` and reload the server.
F2	Discovery of `/.hta` and `/.htpasswd` (403)	Medium	Gobuster: '/.hta (Status: 403)" and /.htpasswd (Status: 403)"	Move credential files outside webroot, ensure server denies access, enforce strict permissions.
F3	ETag Header Leaking Inode Metadata	Low (Info)	Nikto: "Server may leak inodes via ETags... CVE-2003-1418."	Disable ETags in Apache: `FileETag None`.
F4	Default Apache Icons README Exposed	Low (Info)	Nikto: "GET /icons/README: Apache default file found."	Remove default files or deny access to `/icons/`.
F5	Presence of `archive.cer` File and Drupal Headers	Medium	Nikto detected response at `/archive.cer` referencing Drupal 7 headers (HTTP 403 Forbidden when manually tested).	Remove leftover files; patch or upgrade Drupal if used; hide `X-Generator`.
F6	Missing "X-Content-Type-Options" Header	Medium/Low	Nikto: "GET /: The X-Content-Type-Options header is not set."	Add: `Header always set X-Content-Type-Options "nosniff"`.

Table 1: Prioritized summary of findings for `http://www.itsecgames.com/`.

3. Detailed Explanation of Findings

This section provides a concise yet detailed explanation of each vulnerability identified during the assessment of `http://www.itsecgames.com/`. Each issue is described in terms of its technical background, potential security impact, and recommended remediation. The objective is to provide clear insight into how these findings could be exploited and what preventive measures are appropriate.

F1. Missing `X-Frame-Options` Header

The absence of the `X-Frame-Options` HTTP header allows the web application to be embedded within external sites via iframes. Attackers can exploit this weakness to perform **clickjacking attacks**, where users unknowingly interact with maliciously hidden elements. Implementing the header with the value `DENY` or `SAMEORIGIN` ensures that pages cannot be framed by untrusted sources, thereby protecting users from UI redressing attacks.

F2. Discovery of `/.hta` and `/.htpasswd` Files

The directory brute-forcing scan revealed access-controlled files `/.hta` and `/.htpasswd` returning HTTP 403 responses. Although direct access is restricted, the mere presence of these files within the webroot indicates potential exposure if permissions are ever weakened. It is recommended to store these files outside the web-accessible directory and strictly enforce permission rules.

F3. ETag Header Leaking Inode Metadata

The ETag (Entity Tag) header is used for caching optimization but may unintentionally reveal sensitive file metadata such as inode numbers, modification timestamps, or file sizes. This information leakage can aid attackers in performing file enumeration or cache-based inference attacks.

F4. Default Apache Icons README Exposed

The exposure of the default Apache `/icons/README` file indicates that default configuration files remain accessible on the production server. Such files often disclose directory structure, server version, or internal path information. While not directly exploitable, this weakens the server's overall security posture

F5. Presence of `archive.cer` File and Drupal Headers

A downloadable `archive.cer` file and the detection of Drupal-specific headers suggest remnants of a previous CMS installation or misconfigured virtual host. Exposure of CMS metadata such as `X-Generator: Drupal 7` enables targeted attacks against known vulnerabilities in that version. Drupal 7 has reached end-of-life status, and any existing deployment should be upgraded or isolated. Hidden CMS headers should be disabled to reduce fingerprinting risk.

F6. Missing `X-Content-Type-Options` Header

Without the `X-Content-Type-Options: nosniff` directive, browsers may attempt to interpret files as a different MIME type than declared by the server. This could lead to the unintentional execution of scripts and cross-site scripting (XSS) payloads if a file is misclassified. Enforcing this header prevents content type sniffing and ensures safer client-side rendering behavior.

4. SSL/TLS Security Assessment Report

A comprehensive SSL/TLS configuration analysis was conducted using the SSL Labs online assessment platform. The following findings summarize major weaknesses and their corresponding recommendations.

Finding	Description	Recommendation
Expired SSL Certificate	Certificate for `web.mmebvba.com` (`https://www.itsecgames.com/`) expired on 22 May 2025 and is self-signed, causing untrusted warnings.	Renew and install a valid CA-signed certificate; automate renewal.
Self-Signed Certificate	The server certificate is issued by itself (`web.mmebvba.com`).	Obtain a trusted CA certificate to prevent MITM attacks.
Unsupported Protocols	Supports deprecated TLS 1.0/1.1; lacks TLS 1.3.	Disable TLS 1.0/1.1 and enable TLS 1.3 with modern cipher suites.
Forward Secrecy Not Enforced	Only partial FS support across browsers.	Reconfigure to enforce ECDHE key exchanges globally.
HSTS Not Enabled	No HSTS header; vulnerable to SSL stripping.	Add HSTS header to enforce HTTPS.
OCSP Stapling Disabled	Revocation checking handled inefficiently.	Enable OCSP Stapling for performance and privacy.
No DNS CAA Record	No CAA record restricting CA issuance.	Add DNS CAA record specifying authorized CA.
Outdated Key Exchange	RSA 2048-bit key still used; minimal by current standards.	Migrate to RSA 4096-bit or ECDSA 256-bit.

Table 2: Summary of SSL/TLS Configuration Vulnerabilities and Recommendations

4.1. Overall SSL/TLS Security Rating

SSL Labs rated the host as **T (untrusted)**, with a potential rating of **B** if certificate trust issues were ignored. The main contributors to the low score were the expired self-signed certificate, outdated TLS support, and incomplete forward secrecy.

4.2. Conclusion

The SSL/TLS configuration for `www.itsecgames.com` exhibits significant weaknesses that compromise confidentiality and authenticity. It is strongly advised to replace the certificate with a CA-signed one, enable TLS 1.3, configure secure cipher suites, enforce HSTS, and verify the presence of DNS CAA and OCSP Stapling for robust transport security.

5. Appendix: Evidence Files and Attachments

- `evidence/nikto-itsecgames.txt`
- `evidence/nmap.nmap` and `evidence/nmap.xml`
- `evidence/gobuster.txt`
- `evidence/curl-http-headers.txt`
- `evidence/icons_README.txt`
- SSL Labs screenshot