Vulnerability Assessment Report — itsecgames.com

Prepared by: Harish Senthilnathan

Assessment date: 2025-10-06

Scope & Tools

Target: http://www.itsecgames.com/ (31.3.96.40)

Scope: Publicly hosted web endpoint (ports 80 and 443)

Tools used: curl, nikto, nmap, whatweb, sslscan

Executive summary (Technical)

This report outlines the results of a vulnerability assessment conducted on the publicly accessible web application itsecgames.com. The objective of the assessment was to identify potential vulnerabilities and misconfigurations through passive and non-destructive testing techniques. The scope of work included endpoint enumeration, manual validation of scanner results, evaluation of TLS/SSL configurations, and review of error-handling and information disclosure mechanisms.

No instances of remote code execution (RCE) vulnerabilities were identified during the assessment. However, several configuration-related weaknesses were observed that may impact the application's overall security posture. These include an **expired SSL certificate, absence of critical HTTP security headers, ETag information leakage, minor exposure of default files, and non-enforcement of HTTPS connections**.

Objective 1 – Identifying Vulnerabilities

Aim: To discover services, technologies and potential weakness using passive reconnaissance.

Commands Used:

- whatweb http://www.itsecgames.com/ → identify platform & server

- nslookup www.itsecgames.com → DNS resolution

- curl -I http://www.itsecgames.com/ → initial headers

- nikto -h http://www.itsecgames.com/ → automated scan (7 findings)

- nmap -sV -p 80,443 --script=vuln 31.3.96.40 → Checks service version and also checks for vulnerability scripts.

Objective 2 – Validation of findings and detecting potential vulnerabilities

Aim: Validate each finding from the automated scan and map to real risk / CVEs.

Finding: Missing **X-Frame-Options**

Command Used: curl -sS -D - -o /dev/null http://www.itsecgames.com/ | grep -i "X-Frame-Options"

Interpretation: The scan returned no output, indicating that the security header is absent. This missing header could expose the application to clickjacking attacks.

Mitigation: Add Header always append X-Frame-Options "SAMEORIGIN" in Apache security.conf

Finding: Missing **X-Content-Type-Options**

Command Used: curl -sS -D - -o /dev/null http://www.itsecgames.com/ | grep -i "X-Content-Type-Options"

Interpretation: The scan returned no output, which means the browser can override declared MIME types and interpret content incorrectly which can enable cross-site-scripting (XSS)

Mitigation: Add Header always set X-Content-Type-Options "nosniff"

Finding: ETag info leak (Nikto → CVE-2003-1418 mapping)

Command Used: curl -sS -D - -o /dev/null http://www.itsecgames.com/ | grep -i "ETag"

Interpretation: The token contains file inode, modification time, and size information, confirming the presence of a vulnerability. Apache generates ETags based on file metadata, which can be exploited for cache fingerprinting and minor information disclosure.

Mitigation: Disable ETag in Apache, then reload after modification

Finding: Allowed HTTP methods

Command Used: curl -sI -X OPTIONS http://www.itsecgames.com/

Interpretation: This confirms that the server only permits safe methods. However, exposing OPTIONS might be a potential information to the attacker.

Mitigation: Restrict HTTP methods if not required

Finding: Apache default file /icons/README

Command Used: curl -sI http://www.itsecgames.com/icons/README

Interpretation: HTTP response showed 200 OK, confirming the file exists and is publicly reachable. Default Apache example directories should not be visible externally.

Mitigation: Restrict access or remove directory.

Findings: Drupal 7 was identified via the x-generator header– False Positive

Commands Used:

curl -sI http://www.itsecgames.com/archive.gz

curl -sS http://www.itsecgames.com/archive.gz | head -n 30

curl -sS -D - -o /dev/null http://www.itsecgames.com/archive.gz | grep -i “x-generator”

Interpretation: Nikto scanner reported that Drupal 7 was detected through the file /archive.gz. All the commands gave 404 error which is likely to be false positive.

Mitigation: No security risk as of now. But it’s better to remove archive or zip files if any.

Findings: Drupal Link Header found under /archive.gz – False Positive

Command Used: curl -sS -D - -o /dev/null http://www.itsecgames.com/archive.gz | grep -i "Link:"

Interpretation: No Link appeared in the response header. Likely a false positive

Mitigation: None required. Continue regular scan.

Objective 3 - Assess SSL/TLS configuration and certificate health.

Aim: Verify TLS protocol, cipher strength and certificate health

Commands Used:

- curl -vk https://www.itsecgames.com/ → View SSL handshake, TLS Version

- nmap --script ssl-enum-ciphers -p 443 itsecgames.com → Checks which type of secure connection and encryption methods are allowed.

- curl -I http://www.itsecgames.com/ → Check if HTTP automatically redirects to HTTPS

- openssl s_client -connect itsecgames.com:443 -servername itsecgames.com → Verify certificate expiry and issuer info.

Result:

Check	**Observation**
TLS handshake	Negotiated TLSv1.2 / ECDHE_RSA_AES_256_GCM_SHA384
Protocol versions	TLS 1.2 supported, TLS 1.3 not shown
Certificate	Expired May 2025; issued for www.mmebvba.com
Hostname check	CN does not match www.itsecgames.com
Redirect test	HTTP (port 80) did not redirect to HTTPS
HTTPS header	Not present

Interpretation and Conclusion:

- From the table, we can see that the TLS handshake uses a strong encryption mechanism (TLS 1.2 / ECDHE_RSA_AES_256_GCM_SHA384).
- While TLS 1.2 is secure, it can be upgraded to TLS 1.3 for stronger security.
- The SSL certificate which is used is expired and also has a hostname mismatch. The certificate's Common Name **(**CN**)** and the domain name do not match.
- The CN on the certificate is www.mmebvba.com, while the domain accessed is www.itsecgames.com.
- This mismatch causes browsers to show a certificate error and prevents secure trust establishment.
- The site still allows HTTP access and does not automatically redirect users to the HTTPS version, which enables unencrypted communication.

Objective 4 - Exposed Information, Error Messages & Headers

Aim: To find any information disclosure via error message, robots, backups, directory listings, HTTP methods.

Server Banner and Error Page Exposure

Command Used: curl -sS -D - http://www.itsecgames.com/invalidtestpage -o /tmp/serverbanner.html && sed -n '1,60p' /tmp/ serverbanner.html

Interpretation: The 404-error page is a default error page and it does not leak any sensitive information. Although the server banner is visible which can be mitigated by making server signature off in security.conf file of Apache.

robots.txt and sitemap.xml information exposure

Commands used:

curl -sS http://www.itsecgames.com/robots.txt || echo "no robots"

curl -sS http://www.itsecgames.com/sitemap.xml || echo "no sitemap"

Interpretation: Both gave 404 page which means it both robots.txt and sitemap.xml does not reveal sensitive information.

Backup or Sensitive File Exposure

Interpretation: Created a shell script file which checks hidden and left over files such as /backup.tar /backup.zip /site.zip /wwwitsecgames.tar /.git/config /.env /phpinfo.php and got 404 page, meaning no sensitive files were left publicly accessible

Directory Listing Check

Commands Used:

curl -sS -D - http://www.itsecgames.com/uploads/ -o /tmp/uploadscheck.html && sed -n '1,40p' /tmp/uploadscheck.html

curl -sS -D - http://www.itsecgames.com/images/ -o /tmp/imagecheck.html && sed -n '1,40p' /tmp/imagecheck.html

Interpretation: /uploads return 404 page and /images returned 403 forbidden page which means directory listing is disabled.

HTTP Methods

Commands Used:

curl -sI -X OPTIONS http://www.itsecgames.com/

curl -sI -X TRACE http://www.itsecgames.com/

Interpretation: OPTION request returned allow: GET, HEAD, POST, OPTIONS whereas TRACE request returned 405 error method not allowed. This means only safe methods are allowed and TRACE is disabled.