COMPREHENSIVE VULNERABILITY ASSESSMENT REPORT

Target: www.itsecgames.com (31.3.96.40)

Prepared By:
Malagundla Manjunath
Cybersecurity Analyst / Student

Tools Used:
Nmap 7.94SVN | OWASP ZAP D-2025-09-18 | testssl.sh

Assessment Date: 28th September 2025

Nmap Vulnerability Assessment Report

Target: www.itsecgames.com (31.3.96.40)
Scan Type: TCP SYN scan (-sS), Service Version (-sV), OS Detection (-O), Default & Safe NSE scripts
Scan Date: 2025-09-27
Scan Tool: Nmap 7.94SVN

Summary :

Open Port	Service	Version	Risk Level	Notes
22/tcp	SSH	OpenSSH 6.7p1	**Critical**	Multiple known vulnerabilities; exploits available
80/tcp	HTTP	Apache httpd	**Medium**	HTTP headers incomplete; no HSTS; user-agent tester allowed
443/tcp	HTTPS	Apache httpd	**Medium**	No mobile version; missing HSTS; potential SSL misconfigurations

OS Guess: Oracle VirtualBox / QEMU gateway (not exact)
Filtered Ports: 997 (no response)

1. SSH (Port 22) CVEs

CVE	Description	Risk	Mitigation
CVE-2015-5600	OpenSSH integer overflow in xmalloc allows remote attackers to cause a denial-of-service (crash).	**High**	Update OpenSSH to latest version; ensure proper memory management; monitor SSH logs.
CVE-2016-1908	OpenSSH “roaming” feature enabled sensitive data exposure (private keys) if client used roaming.	**Critical**	Upgrade OpenSSH; disable roaming in client (UseRoaming no); audit SSH keys.

CVE	Description	Risk	Mitigation
CVE-2023-38408	Multiple issues in OpenSSH leading to privilege escalation and DoS.	**Critical**	Patch OpenSSH to latest stable release; enforce key-based authentication; restrict root login.
Other Exploits (Metasploit/GitHub)	Various remote code execution, brute force vulnerabilities.	**Critical**	Use firewall to restrict SSH; fail2ban; strong passwords; key-based authentication only.

Detected Service: OpenSSH 6.7p1

Additional Mitigation Steps for SSH:

1. Disable password authentication in /etc/ssh/sshd_config:
2. PasswordAuthentication no
3. Disable root login:
4. PermitRootLogin no
5. Use non-standard port (optional but reduces automated attacks).
6. Regularly monitor /var/log/auth.log for suspicious login attempts.

---

2. HTTP / HTTPS / Apache CVEs

While your Nmap scan did not show exact CVE numbers for Apache, using Apache httpd older versions can expose you to common CVEs:

CVE	Description	Risk	Mitigation
CVE-2017-3167	Apache HTTP Server mod_proxy allows request smuggling attacks via invalid headers.	**Medium**	Upgrade Apache to latest stable; disable unnecessary modules; validate input headers.

CVE	Description	Risk	Mitigation
CVE-2019-0211	Apache HTTP Server privilege escalation via mod_lua.	**High**	Apply patches; minimize enabled modules; use least privilege for Apache user.
CVE-2021-41773	Path traversal and file disclosure in Apache 2.4.49-2.4.50.	**High**	Upgrade Apache to >=2.4.51; enable security modules (mod_security).

Mitigation Steps for Web Services:

1. **Upgrade Apache** to latest version (>=2.4.55 or current stable).
2. **Enable Security Modules:** mod_security, mod_evasive.
3. **Disable Unnecessary Modules:** Only enable what is required.
4. **Configure Security Headers:**
   - X-Frame-Options: SAMEORIGIN
   - X-Content-Type-Options: nosniff
   - Content-Security-Policy: default-src 'self'
   - Strict-Transport-Security: max-age=31536000; includeSubDomains
5. **Limit HTTP Methods:** Allow only GET and POST.

---

3. SSL / TLS CVEs (if older versions detected)

Common CVEs if SSL/TLS versions are weak:

CVE	Description	Risk	Mitigation
CVE-2014-3566 (POODLE)	SSLv3 vulnerability leading to decryption attacks.	**High**	Disable SSLv3; use TLS 1.2+ only.
CVE-2015-0204 (FREAK)	Weak export-grade cipher vulnerability.	**High**	Disable weak ciphers; use strong cipher suites like AES-GCM.

CVE	Description	Risk	Mitigation
CVE-2016-2107	Padding oracle in CBC mode in OpenSSL.	**Medium**	Upgrade OpenSSL to latest stable; disable CBC if possible.

Mitigation Steps for TLS/SSL:

1. Enforce TLS 1.2/1.3.
2. Disable weak ciphers (DES, 3DES, RC4).
3. Enable HSTS and proper certificate management.
4. Run periodic scans using testssl.sh to detect SSL/TLS vulnerabilities.

✅ **Summary:**

- **SSH CVEs are critical:** Update OpenSSH, restrict root, enforce key-based login, use firewalls.
- **Apache CVEs are medium to high:** Upgrade Apache, configure security headers, minimize modules.
- **SSL/TLS CVEs are high:** Disable SSLv3, weak ciphers; enforce TLS 1.2+, 1.3; HSTS enabled.

OWASP ZAP Vulnerability Assessment Report

Target: www.itsecgames.com (http://www.itsecgames.com)
Scan Type: Passive + Active Web Application Scan (Spidering, Passive Analysis, Active Scan, User-Agent Fuzzing, Scripting Plugins)
Tools / Components Used: OWASP ZAP (Zed Attack Proxy) — Version **D-2025-09-18** (Checkmarx distribution); ZAP Spider; Passive Scanner; Active Scanner; Alerts/Report generator
Scan Date: 2025-09-27
Report File: zap_report.html (exported HTML)

1. Content Security Policy (CSP) Header Not Set

- **Risk:** Medium
- **CWE:** 693 (Protection Mechanism Failure)
- **OWASP References:** A05:2021 – Security Misconfiguration
- **Description:** CSP headers are missing. Without CSP, your site is more vulnerable to **XSS attacks** and content injection.
- **CVEs:** CSP misconfiguration itself doesn't map to a specific CVE, but many XSS CVEs exploit sites lacking CSP, e.g., **CVE-2020-1350** (for Windows DNS server) demonstrates how improper configurations lead to attacks, although not exactly CSP.
- **Mitigation:**
    1. Implement CSP headers on all pages. Example:
    2. Content-Security-Policy: default-src 'self'; script-src 'self' https://trusted.cdn.com; object-src 'none';
    3. Test using online tools like CSP Evaluator.
    4. Update CSP policies regularly and monitor violations via report-uri.

---

2. Sub Resource Integrity (SRI) Attribute Missing

- **Risk:** Medium
- **CWE:** 345 (Insufficient Verification of Data Authenticity)
- **Description:** External scripts/styles lack integrity attributes. Attackers modifying third-party resources can inject malicious code.

- **CVEs:** No direct CVE, but SRI absence can enable exploits such as **CVE-2018-12404** (malicious script injection via CDN).
- **Mitigation:**
    1. Add SRI hashes for all third-party scripts:
    2. <script src="https://cdn.example.com/lib.js" integrity="sha384-xyz" crossorigin="anonymous"></script>
    3. Verify hashes each time the library updates.
    4. Serve critical scripts from trusted sources or locally.

---

3. Missing Anti-Clickjacking Header

- **Risk:** Medium
- **CWE:** 1021 (Improper Restriction of Rendered UI Layers)
- **Description:** Page can be framed by other sites, allowing **clickjacking attacks**.
- **CVEs: CVE-2018-9206** shows clickjacking risk on improperly framed web applications.
- **Mitigation:**
    1. Use **X-Frame-Options** header:
    2. X-Frame-Options: SAMEORIGIN
    3. Or use **CSP frame-ancestors** directive:
    4. Content-Security-Policy: frame-ancestors 'self';
    5. Test framing prevention using online tools or browser developer tools.

---

4. Insufficient Site Isolation Against Spectre

- **Risk:** Low
- **CWE:** 693
- **Description:** Cross-Origin-Resource-Policy header missing, which mitigates Spectre-like attacks via side channels.
- **CVEs: CVE-2018-3639** (Speculative Store Bypass / Spectre variant 4)
- **Mitigation:**
    1. Set Cross-Origin-Resource-Policy:

2. Cross-Origin-Resource-Policy: same-origin
3. Consider Cross-Origin-Opener-Policy for top-level site isolation:
4. Cross-Origin-Opener-Policy: same-origin
5. Keep browsers and servers updated to mitigate microarchitectural attacks.

---

5. Permissions Policy Header Not Set

- **Risk:** Low
- **CWE:** 693
- **Description:** Without this header, browsers may allow access to sensitive APIs like camera, microphone, etc.
- **CVEs:** No direct CVE, but misconfigurations could enable attacks using **CVE-2022-0609** (web API abuse).
- **Mitigation:**
    1. Add Permissions-Policy header:
    2. Permissions-Policy: camera=(), microphone=(), geolocation=()
    3. Restrict features to only necessary origins.
    4. Audit API usage and browser support.

---

6. X-Content-Type-Options Header Missing

- **Risk:** Low
- **CWE:** 693
- **Description:** Allows MIME type sniffing, which can lead to XSS or content injection.
- **CVEs: CVE-2019-6340** (Drupal module exploitation involved content sniffing), **CVE-2018-7600** (Drupalgeddon 2)
- **Mitigation:**
    1. Add header to all responses:
    2. X-Content-Type-Options: nosniff
    3. Ensure correct Content-Type headers for all files.
    4. Test legacy browsers and modern browsers for behavior.

7. Storable and Cacheable Content

- **Risk:** Informational
- **CWE:** 524 (Information Exposure Through Caching)
- **Description:** Sensitive content may be cached by proxies or browsers, potentially exposing user data.
- **CVEs:** Rare, more configuration risk; improper caching can indirectly lead to CVEs in session hijacking scenarios.
- **Mitigation:**
  1. Add cache control headers for sensitive pages:
  2. Cache-Control: no-cache, no-store, must-revalidate
  3. Pragma: no-cache
  4. Expires: 0
  5. Avoid caching authentication responses or user-specific data.
  6. Regularly review caching policies.

---

8. User Agent Fuzzer

- **Risk:** Informational
- **Description:** Tests site responses to various User-Agent headers; may reveal content differences.
- **CVEs:** None directly, but differences can expose hidden endpoints.
- **Mitigation:**
  1. Normalize responses regardless of User-Agent.
  2. Avoid revealing sensitive or debug content for specific agents.
  3. Monitor logs for abnormal access patterns.

SSL/TLS Security Assessment Report – www.itsecgames.com

Tool: testssl

SSL/TLS Assessment Summary

1️⃣ Protocols Supported

Protocol	Status	Notes
SSLv2	Not offered	OK
SSLv3	Not offered	OK
TLS 1.0	Offered	Deprecated – weak, should be disabled
TLS 1.1	Offered	Deprecated – weak, should be disabled
TLS 1.2	Offered	OK
TLS 1.3	Not offered	Modern protocol missing, upgrade recommended

Risk: TLS 1.0/1.1 are deprecated and vulnerable to attacks like BEAST.

2️⃣ Cipher Suites

- Strong ciphers with Forward Secrecy are offered ✅
- Weak/deprecated CBC ciphers exist in TLS 1.0/1.1
- No NULL, anonymous, or export ciphers ✅

Risk: Weak CBC ciphers make TLSv1.0/1.1 sessions potentially vulnerable (BEAST, LUCKY13).

3️⃣ Certificate Details

Item	Status/Issue
Common Name (CN)	web.mmebvba.com (mismatch)
SAN (Subject Alt Name)	Missing (NOT OK)
Validity	Expired (2025-05-22)
Chain of Trust	Self-signed (NOT OK)
OCSP/CRL	Not offered
Public Key Size	2048 bits (OK)

Item	**Status/Issue**
Signature Algorithm	SHA256 with RSA (OK)

Risk: Expired, self-signed certificate and CN mismatch make HTTPS connections untrusted. Critical vulnerability.

4️⃣ HTTP Headers & Security Features

- **Strict Transport Security (HSTS):** Not offered
- **Public Key Pinning:** Not implemented
- **Server Banner:** Apache
- **Cookies:** None issued at root

Risk: Missing HSTS and security headers makes site more prone to SSL stripping and other attacks.

5️⃣ Vulnerability Testing

Vulnerability	**Status**
Heartbleed (CVE-2014-0160)	Not vulnerable
POODLE (SSLv3)	Not vulnerable
BEAST (TLSv1)	Vulnerable
LUCKY13 (CBC ciphers)	Potentially vulnerable
TLS_FALLBACK_SCSV	Supported (OK)
FREAK, DROWN, ROBOT, etc.	Not vulnerable

Risk: BEAST and CBC-related vulnerabilities affect older protocols (TLS 1.0/1.1).

6️⃣ Browser Compatibility

- Modern browsers (Chrome, Firefox, Edge, Safari, Android/iOS) mostly use TLS 1.2 → Forward Secrecy OK
- Older browsers (IE8, Java 7) using TLS 1.0 → vulnerable

Overall SSL/TLS Rating

- **Grade:** T (Testssl.sh experimental rating)
- **Reason:** Certificate expired, self-signed, CN mismatch, missing TLS 1.3, weak/deprecated protocols.

7️⃣ Recommendations

1. **Renew Certificate** with a trusted CA (Let’s Encrypt or commercial CA).
2. **Enable TLS 1.3** and disable TLS 1.0/1.1.
3. **Remove weak CBC ciphers** from the server configuration.
4. **Implement HSTS** to enforce HTTPS connections.
5. **Add SAN to certificate** to avoid CN mismatch warnings.
6. **Enable OCSP stapling** for revocation checking.
7. **Review server headers** and minimize information disclosure (remove Apache version, etc.).