Vulunerability Assessment Report: www.itsecgames.com

Executive Summary

This report presents the findings of a security assessment performed on **www.itsecgames.com** using **OWASP ZAP** and **Qualys SSL Labs**. The assessment identified multiple security vulnerabilities and misconfigurations, including an **expired SSL certificate**, missing security headers, weak TLS configurations, and informational disclosures. The issues identified expose the site to risks such as man-in-the-middle attacks, clickjacking, cross-site scripting (XSS), and content injection attacks.

A total of **9 findings** were identified, categorized by severity (Critical, High, Medium, Low, Informational). Each finding includes a description, evidence, impact, and recommended mitigation steps.

Methodology

- **Tools Used**: OWASP ZAP (v2.16.1), Qualys SSL Labs Server Test
- **Scan Date**: September 15, 2025
- **Target**: http://www.itsecgames.com
- **Scope**: Web application and SSL/TLS configuration

Risk Rating Overview

Severity	Count
Critical	2
High	1
Medium	3
Low	2

Severity	Count
Informational	1

Detailed Findings

1. Expired SSL Certificate (Critical)

- **Description**: The server uses a self-signed certificate that expired on May 22, 2025.
- **Evidence**:
    - SSL Labs report: Valid until: Thu, 22 May 2025 09:07:54 UTC (expired)
    - Trusted: No
- **Impact**: Browsers will display security warnings, potentially preventing users from accessing the site. Loss of trust and increased risk of MITM attacks.
- **Recommendation**:
    - Replace the self-signed certificate with a valid certificate from a trusted Certificate Authority (e.g., Let's Encrypt).
    - Implement automatic certificate renewal.

---

2. Self-Signed Certificate (Critical)

- **Description**: The certificate is self-signed and not issued by a trusted Certificate Authority.
- **Evidence**:
    - SSL Labs: Issuer: web.mmebvba.com Self-signed
- **Impact**: Users will see security warnings, and modern browsers may block access. Not suitable for production use.
- **Recommendation**:
    - Obtain a certificate from a trusted CA.
    - Use ACME for automated certificate management.

---

3. Missing Content Security Policy (CSP) Header (High)

- **Description**: The CSP header is not set, leaving the site vulnerable to XSS and data injection attacks.
- **Evidence**:
    - ZAP Alert: Content Security Policy (CSP) Header Not Set (Risk: Medium, Confidence: High)
- **Impact**: Increased risk of cross-site scripting (XSS) and content injection attacks.
- **Recommendation**:
    - Implement a CSP header such as:

Content-Security-Policy: default-src 'self'; script-src 'self'; object-src 'none';

    - Use CSP Evaluator to validate the policy.

---

4. Missing Anti-Clickjacking Header (Medium)

- **Description**: The X-Frame-Options header is missing, making the site vulnerable to clickjacking attacks.
- **Evidence**:
    - ZAP Alert: Missing Anti-clickjacking Header (Risk: Medium, Confidence: Medium)
- **Impact**: Attackers could embed the site in an iframe and trick users into performing unintended actions.
- **Recommendation**:
    - Add the header:

X-Frame-Options: DENY

    - Alternatively, use CSP with frame-ancestors 'none'.

---

5. Weak TLS Configuration (Medium)

- **Description**: The server supports outdated protocols (TLS 1.0 and TLS 1.1) and weak cipher suites.
- **Evidence**:
    - SSL Labs: Supports TLS 1.0 and 1.1
    - Does not support TLS 1.3
    - Uses weak ciphers
- **Impact**: Vulnerable to downgrade attacks and weak encryption.
- **Recommendation**:
    - Disable TLS 1.0 and TLS 1.1.
    - Enable TLS 1.2 and TLS 1.3.
    - Prioritize forward-secret ciphers

---

6. Missing HSTS Header (Medium)

- **Description**: The Strict-Transport-Security header is not present.
- **Evidence**:
    - SSL Labs: Strict Transport Security (HSTS): No
- **Impact**: Users may be downgraded to HTTP, leading to MITM attacks.
- **Recommendation**:
    - Implement HSTS with a long max-age:

Strict-Transport-Security: max-age=31536000; includeSubDomains

---

7. Missing X-Content-Type-Options Header (Low)

- **Description**: The X-Content-Type-Options: nosniff header is missing.
- **Evidence**:
    - ZAP Alert: X-Content-Type-Options Header Missing (Risk: Low, Confidence: Medium)

- **Impact**: Older browsers may perform MIME-sniffing, leading to content-type misinterpretation.
- **Recommendation**:
    - Add the header:

X-Content-Type-Options: nosniff

---

8. No OCSP Stapling (Low)

- **Description**: OCSP stapling is not enabled.
- **Evidence**:
    - SSL Labs: OCSP stapling: No
- **Impact**: Slower SSL handshake and potential privacy issues.
- **Recommendation**:
    - Enable OCSP stapling in the web server configuration.

---

9. User Agent-Based Access Control (Informational)

- **Description**: The server returns a 403 Forbidden response when accessed with certain User-Agent strings (e.g., older IE).
- **Evidence**:
    - ZAP Alert: User Agent Fuzzer → 403 response for Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
- **Impact**: May indicate inconsistent access control or error handling.
- **Recommendation**:
    - Ensure consistent error handling and avoid user-agent-based blocking unless necessary.
    - Use proper authentication and authorization mechanisms instead.

Summary of Recommendations

Priority	Recommendation
Critical	Replace expired self-signed certificate with a trusted CA-signed certificate.
Critical	Obtain a valid certificate from a trusted CA (e.g., Let's Encrypt).
High	Implement Content Security Policy (CSP) header.
Medium	Add X-Frame-Options: DENY or CSP frame-ancestors directive.
Medium	Upgrade TLS configuration: disable TLS 1.0/1.1, enable TLS 1.3, use strong ciphers.
Medium	Implement HSTS header.
Low	Add X-Content-Type-Options: nosniff header.
Low	Enable OCSP stapling.
Info	Review user-agent-based access control logic.

Conclusion

The assessment revealed several critical and high-severity issues that require immediate attention. The most urgent issues are the **expired and self-signed SSL certificate**, which undermines user trust and exposes the site to MITM attacks. Additionally, the lack of security headers (CSP, X-Frame-Options, HSTS) increases the risk of XSS, clickjacking, and protocol downgrade attacks.

Implementing the recommended mitigations will significantly improve the security posture of **www.itsecgames.com** and ensure compliance with modern web security standards.

Appendix

Tools Used

- **OWASP ZAP**: Web application vulnerability scanner.
- **Qualys SSL Labs**: SSL/TLS configuration and certificate health checker.

References

- OWASP Secure Headers Project

Report Generated By: Sambit Kumar Sahoo
Date: September 15, 2025