Security Assessment Report

Assessment Date: September 19, 2025

Assessment Time: 03:15 PM IST

Performed by: Smit S. Bhatt

Target Endpoint (Domain): itsecgames.com

Resolved Host/IP: web.mmebvba.com (31.3.96.40)

Authoritative DNS: 31.3.96.40

Scanning Host (Tester): Kali Linux VM (192.168.44.160)

DNS Resolver Used: 192.168.44.2

Objective: To evaluate the security posture of the target, identify vulnerabilities, and provide remediation recommendations.

Executive Summary

This assessment was performed to evaluate the security posture of the target endpoint. The primary objectives were to **identify vulnerabilities, analyze misconfigurations, assess SSL/TLS health**, and highlight any exposed information that could aid attackers.

The testing revealed **multiple critical and high-severity vulnerabilities**, including outdated software, missing security headers, and weak SSL/TLS configurations. If exploited, these issues could lead to remote code execution, sensitive data leakage, or unauthorized system access.

Methodology

1. **Information Gathering** – Collected metadata about the target (DNS, IP, hosting country, server banners).
2. **Service Enumeration** – Identified open ports and active services using Nmap and WhatWeb.
3. **Vulnerability Scanning** – Leveraged Nikto, Nmap scripts, and OWASP ZAP to detect weaknesses.
4. **Validation & Analysis** – Cross-referenced findings with CVEs, CWE entries, and OWASP guidelines.

5. **Reporting** – Consolidated vulnerabilities, ranked by severity, and provided remediation advice.

Identified Vulnerabilities

Service	Port	Vulnerability	Severity	CVE(s)
HTTP	80	Outdated Apache server version disclosure	Medium	CVE-2023-31122
HTTPS	443	TLS/SSL weak cipher support	High	CVE-2013-2566, CVE-2015-2808
General	-	Directory indexing enabled	Medium	-
General	-	Missing security headers (X-Frame-Options, CSP)	High	-
General	-	Potential outdated components	Medium	-
SSH	22	Outdated OpenSSH 6.7p1 with RCE flaws	High	CVE-2023-38408, CVE-2016-1908, CVE-2015-5600

Additional Findings

- **SSH (Port 22):** Running **OpenSSH 6.7p1**, which is outdated and vulnerable (CVE-2023-38408 – CVSS 9.8). Exploits exist for remote code execution.
- **HTTP (Port 80):** Apache redirects to HTTPS, but missing modern security headers. No XSS/CSRF detected in quick tests.
- **HTTPS (Port 443):** SSL certificate valid until May 22, 2025, but weak cipher suites supported. May allow downgrade attacks.
- **Host Metadata:** Target hosted in **Netherlands** (per WhatWeb results). Server leaks version and banner info.

Severity Ratings:

- **High:** Issues that could allow remote compromise (e.g., OpenSSH RCE, weak TLS).
- **Medium:** Issues that increase exposure but require chaining (e.g., directory listing, outdated software).
- **Low:** Informational disclosures with minimal risk.

Recommendations

1. **Upgrade OpenSSH** to the latest stable release to patch RCE vulnerabilities.
2. **Harden TLS/SSL configurations** by disabling weak ciphers and enabling TLS 1.2+ only.
3. **Apply security headers** (CSP, X-Frame-Options, X-Content-Type-Options) to prevent clickjacking, XSS, and MIME attacks.
4. **Patch Apache** and other backend components to mitigate known CVEs.
5. **Restrict directory indexing** and suppress version banners to reduce information leakage.
6. **Continuous Monitoring:** Implement SIEM logging and periodic vulnerability scans to detect future issues.

Conclusion:

The target endpoint demonstrates several **serious vulnerabilities** that could be exploited by attackers if left unpatched. Immediate focus should be placed on **OpenSSH and SSL/TLS misconfigurations**, followed by remediation of missing headers and software updates.

By addressing these findings, the organization can significantly strengthen its security posture and reduce the likelihood of compromise.