Security Assessment Report: itsecgames.com

Candidate: Damarapati Jashwanth
Email: damarapatijashwanth@gmail.com
Phone: +91 9000542152
Position: Security Officer Trainee
Assessment Date: September 21-22, 2025

Executive Summary

A comprehensive security assessment was conducted on itsecgames.com (IP: 31.3.96.40) to evaluate its security posture and identify potential vulnerabilities. The assessment revealed **8 significant findings** ranging from high-severity SSL/TLS misconfigurations to medium-severity platform vulnerabilities.

Key Critical Issues Identified:

- SSL certificate hostname mismatch causing browser security warnings
- Multiple unnecessary network services exposed (FTP, RTSP, PPTP)
- End-of-life Drupal 7 platform with known security vulnerabilities
- Missing modern security headers (HSTS, CSP)

Risk Rating: HIGH - Immediate remediation required for critical SSL and platform vulnerabilities.

Assessment Scope and Authorization

Target: itsecgames.com
Authorization: Security Officer Trainee assessment as per job requirement
Methodology: External security assessment using industry-standard tools
Testing Window: September 21-22, 2025

Problem Statement: Evaluate the security posture of itsecgames.com endpoint, identify vulnerabilities including misconfigurations, outdated software, CVEs, assess SSL/TLS configuration, and highlight exposed information that could aid attackers.

Reconnaissance and Information Gathering

Domain Intelligence

- **Domain:** itsecgames.com
- **IP Address:** 31.3.96.40
- **rDNS:** web.mmebvba.com
- **Country:** Netherlands (NL)
- **Registrar:** GoDaddy.com, LLC
- **Created:** May 21, 2012
- **Expires:** May 21, 2027

- **Name Servers:** NS53.DOMAINCONTROL.COM, NS54.DOMAINCONTROL.COM

Technology Stack Identification

- **Web Server:** Apache HTTP Server
- **CMS Platform:** Drupal 7 (End-of-Life)
- **JavaScript Libraries:** jQuery 1.5 (Outdated)
- **SSL/TLS:** Enabled but misconfigured

Port Scan and Service Enumeration

Open Ports and Services

```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
554/tcp  open  rtsp
1723/tcp open  pptp
```

Analysis: The server exposes 6 open ports, several of which are unnecessary for a web application and increase the attack surface. FTP (21), RTSP (554), and PPTP (1723) services should be evaluated for necessity.

Web Application Analysis

Technology Detection

WhatWeb identified the following components:

- **Primary Site (HTTP):** bWAPP (Intentionally vulnerable web application)
- **Primary Site (HTTPS):** MME Security Audits & Training
- **Framework:** Drupal 7 with jQuery 1.5
- **Contact Email:** info@mmesec.com

HTTP Security Headers Analysis

HTTPS Response Headers:

```
Server: Apache
X-Generator: Drupal 7 (http://drupal.org)
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
Content-Language: en
```

Security Assessment:

- ✅ X-Content-Type-Options: nosniff (Good)
- ✅ X-Frame-Options: SAMEORIGIN (Good)
- ❌ Missing Strict-Transport-Security (HSTS)
- ❌ Missing Content-Security-Policy (CSP)
- ❌ Server header reveals technology stack

Detailed Security Findings

HIGH SEVERITY FINDINGS

[H01] SSL/TLS Certificate Hostname Mismatch

Evidence: Nikto scan and SSL certificate validation
Description: The SSL certificate presented by the server is issued for "mmebv.be" but the domain accessed is " itsecgames.com". This mismatch causes browsers to display security warnings and prevents secure connections.

Impact:

- Users see certificate error warnings
- Increased risk of man-in-the-middle attacks
- Loss of user trust and potential abandonment
- Automated clients may fail to connect

Recommendation:

1. Obtain and install a valid SSL certificate for itsecgames.com
2. Ensure Subject Alternative Name (SAN) includes itsecgames.com
3. Consider using Let's Encrypt for free, valid certificates
4. Validate installation using SSL Labs test

[H02] Multiple Unnecessary Network Services

Evidence: Nmap port scans (nmap_all_ports.txt, nmap_quick.txt)
Description: The server exposes multiple network services that are not required for web application functionality, including FTP (21), RTSP (554), and PPTP (1723).

Impact:

- Increased attack surface
- Potential for lateral movement if services are compromised
- Additional maintenance overhead
- Unnecessary resource consumption

Recommendation:

1. Audit all running services for business necessity
2. Disable and close unused ports (FTP, RTSP, PPTP)

3. Implement network firewall rules to restrict access
4. Consider moving SSH (22) to non-standard port
5. Regular port scanning for monitoring

MEDIUM-HIGH SEVERITY FINDINGS

[M01] Drupal 7 End-of-Life CMS Platform

Evidence: X-Generator header, Nikto scans, WhatWeb analysis
Description: The website runs on Drupal 7, which reached end-of-life status and no longer receives regular security updates. This version has known vulnerabilities and is actively targeted by attackers.

Impact:

- Known security vulnerabilities remain unpatched
- No official security support from Drupal project
- High risk of exploitation through published CVEs
- Compliance issues for regulated industries

Recommendation:

1. **Immediate:** Conduct vulnerability assessment of current Drupal installation
2. **Short-term:** Apply any available extended security updates
3. **Long-term:** Migrate to Drupal 10+ or alternative secure CMS
4. **Ongoing:** Implement Web Application Firewall (WAF) as temporary protection

MEDIUM SEVERITY FINDINGS

[M02] Missing Critical Security Headers

Evidence: Nikto scans (nikto_https.txt, nikto_http.txt)
Description: The application is missing several important security headers that provide defense-in-depth protection against common web attacks.

Missing Headers:

- Strict-Transport-Security (HSTS)
- Content-Security-Policy (CSP)
- Referrer-Policy
- Permissions-Policy

Recommendation:

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline'
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
```

[M03] Exposed Installation and Configuration Files

Evidence: Nikto HTTPS scan revealing accessible robots.txt entries
Description: Multiple Drupal installation and configuration files are accessible through direct requests, potentially exposing sensitive information about the system configuration.

Accessible Files:

- /INSTALL.sqlite.txt
- /INSTALL.mysql.txt
- /INSTALL.pgsql.txt
- /install.php
- /MAINTAINERS.txt
- /UPGRADE.txt
- /LICENSE.txt
- /xmlrpc.php

Recommendation:

1. Remove installation files from production servers
2. Restrict access to configuration files via .htaccess rules
3. Review and clean up robots.txt entries
4. Implement proper file permissions

[M04] Information Disclosure via Server Headers

Evidence: WhatWeb scan and HTTP response headers
Description: The server reveals detailed technology stack information through HTTP headers, which aids attackers in fingerprinting and targeting specific vulnerabilities.

Disclosed Information:

- Apache web server
- Drupal 7 platform
- jQuery 1.5 library
- Server architecture details

Recommendation:

1. Configure Apache ServerTokens to "Prod"
2. Remove or obfuscate X-Generator headers
3. Implement header filtering at load balancer level
4. Regular review of information disclosure

LOW SEVERITY FINDINGS

[L01] Inconsistent Security Headers Between Protocols

Evidence: Comparison of Nikto HTTP vs HTTPS scans
Description: Security headers implementation differs between HTTP and HTTPS versions of the site, creating inconsistent security posture.

Recommendation:
Ensure all security headers are consistently applied across both HTTP and HTTPS protocols.

[L02] Apache Default Files Accessible

Evidence: Nikto HTTP scan
Description: Default Apache documentation files remain accessible on the server.

Recommendation:
Remove default Apache documentation and example files from the web root.

Risk Assessment Matrix

Finding	Likelihood	Impact	Risk Level
H01 - SSL Certificate Mismatch	High	High	**Critical**
H02 - Multiple Open Services	Medium	High	**High**
M01 - Drupal 7 EOL	High	Medium	**High**
M02 - Missing Security Headers	Medium	Medium	**Medium**
M03 - Exposed Config Files	Low	Medium	**Medium**
M04 - Information Disclosure	Medium	Low	**Medium**
L01 - Inconsistent Headers	Low	Low	**Low**
L02 - Default Apache Files	Low	Low	**Low**

Remediation Priorities

Immediate Actions (0-7 days)

1. **Fix SSL certificate** - Obtain and install valid certificate for itsecgames.com
2. **Close unnecessary ports** - Disable FTP, RTSP, and PPTP services
3. **Implement HSTS header** - Prevent protocol downgrade attacks

Short-term Actions (1-4 weeks)

1. **Security headers implementation** - Deploy comprehensive security headers
2. **Remove exposed files** - Clean up installation files and default content
3. **Web Application Firewall** - Implement WAF for Drupal protection

Long-term Actions (1-6 months)

1. **Platform migration** - Upgrade from Drupal 7 to supported version
2. **Security monitoring** - Implement continuous security monitoring
3. **Security training** - Staff training on secure development practices

Positive Security Controls Identified

The assessment also identified several positive security controls:

- ✅ X-Content-Type-Options: nosniff header prevents MIME sniffing attacks
- ✅ X-Frame-Options: SAMEORIGIN provides clickjacking protection
- ✅ HTTPS protocol available (despite certificate issues)
- ✅ No SQL injection vulnerabilities found in initial testing

Tools and Methodology

The assessment utilized industry-standard security testing tools:

- **Nmap 7.95** - Port scanning and service enumeration
- **Nikto v2.5.0** - Web vulnerability scanning
- **WhatWeb** - Technology fingerprinting
- **SSL Labs** - SSL/TLS configuration analysis
- **Gobuster** - Directory enumeration
- **Manual verification** - HTTP header analysis

Conclusion

The security assessment of itsecgames.com revealed significant security concerns that require immediate attention. The **SSL certificate mismatch and multiple open services present immediate risks** that should be addressed as priority items.

The use of **end-of-life Drupal 7 platform represents a substantial long-term risk** that requires strategic planning for migration or extended security measures.

Overall Security Posture: POOR - Requires immediate remediation of critical issues and comprehensive security improvement program.

Next Steps:

1. Implement immediate fixes for SSL and port exposure
2. Develop migration plan from Drupal 7
3. Establish ongoing security monitoring and maintenance procedures
4. Consider engaging security professionals for comprehensive security review

This assessment was conducted by Damarapati Jashwanth as part of Security Officer Trainee evaluation. All testing was performed in accordance with authorized scope and ethical hacking principles.

Report Generated: September 23, 2025
Classification: Confidential - For recruitment evaluation purposes only