

# **SECURITY ASSESSMENT REPORT**

## **ITSECGAMES.COM**

**Ragila V V – Security Officer Trainee (Applicant)**

**14/09/2025**

## Executive Summary

I performed a focused, non-destructive security review of <http://itsecgames.com> to evaluate the public-facing web service for common risks and misconfigurations.

The review found several issues that deserve prompt attention. The web server is running an older Apache release (2.4.29) that is associated with known security problems (for example, privilege-escalation vulnerabilities). The site's TLS certificate also does not match the hostname—browsers will flag this and secure connections cannot be trusted until it is fixed. In addition, a number of recommended HTTP security controls are missing (notably HSTS and a Content-Security-Policy), which increases exposure to client-side attacks. I also observed the OPTIONS method enabled and a /downloads/ directory that exists but is access-restricted; while nothing sensitive was directly exposed during my testing, these are things that should be checked and cleaned up.

### Severity summary

- **High**
  - Outdated Apache (2.4.29) with known CVEs (e.g., privilege escalation).
  - TLS certificate hostname mismatch (breaks trust / allows MITM warnings).
- **Medium**
  - Missing security headers (HSTS, CSP, etc.).
  - OPTIONS method enabled (information disclosure risk).
- **Low**
  - Presence of a /downloads/ directory (403) — confirm no sensitive files.
  - Server banner reveals Apache (information disclosure).

## Scope & Methodology

The scope of this assessment was limited to the publicly accessible endpoint <http://itsecgames.com>. No authentication credentials, source code, or internal systems were provided, so all testing was performed from an external perspective, simulating what an attacker on the internet could attempt.

The assessment followed a structured process:

### 1. Information Gathering

- a. Identified domain/IP ownership, DNS records, and server banners.
- b. Fingerprinted technologies in use (e.g., Apache web server).

### 2. Network and Service Scanning

- a. Used Nmap to identify open ports (22/SSH, 80/HTTP, 443/HTTPS).
- b. Captured service versions for CVE lookup.

### 3. Web Application Enumeration

- a. Ran Gobuster to discover accessible directories and files.
- b. Queried common files (e.g., robots.txt, phpinfo.php, config.php).

### 4. Vulnerability Testing

- a. Checked server version (Apache 2.4.29) against known CVEs using Searchsploit.
- b. Evaluated SSL/TLS configuration with SSLyze and testssl.sh.
- c. Checked HTTP methods, security headers, and error handling.

### 5. Manual Verification

- a. Reviewed HTTP responses, error messages, and banner information.
- b. Attempted limited misconfiguration checks (e.g., OPTIONS, directory listing).

All tools used (Nmap, Nikto, Gobuster, SSLyze, testssl.sh, curl) were run with safe options only. No destructive exploitation was performed.

## Detailed Findings

### Finding 1 – Outdated Apache Web Server (Apache 2.4.29)

- **Severity:** High
- **Description:** The server is running Apache 2.4.29, which is an outdated version. Multiple CVEs are associated with versions prior to 2.4.38, including privilege escalation and denial-of-service vulnerabilities.
- **Impact:** Attackers may be able to exploit known vulnerabilities to gain unauthorized access, crash the service, or execute code.
- **Evidence:**
  - Nmap service detection showing Apache/2.4.29.
  - searchsploit apache 2.4.29 listing multiple CVEs and exploits.

```
(ragila@kali)-[~]
$ nmap -sS -T4 -p 22,80,443 -sV -oA nmap_basic itsecgames.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 05:35 EDT
Nmap scan report for itsecgames.com (31.3.96.40)
Host is up (0.073s latency).
rDNS record for 31.3.96.40: web.mmebvba.com

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 (protocol 2.0)
80/tcp    open  http     Apache httpd
443/tcp   open  ssl/http Apache httpd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.36 seconds
```

```
(ragila@kali)-[~]
$ nmap -p 80,443 --script http-headers,http-methods,ssl-enum-ciphers -oA nmap_http itsecgames.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 05:37 EDT
Nmap scan report for itsecgames.com (31.3.96.40)
Host is up (0.051s latency).
rDNS record for 31.3.96.40: web.mmebvba.com

PORT      STATE SERVICE
80/tcp    open  http
| http-headers:
|   Date: Sat, 13 Sep 2025 09:36:30 GMT
|   Server: Apache
|   Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT
|   ETag: "e43-5d7959bd3c800"
|   Accept-Ranges: bytes
|   Content-Length: 3651
|   Vary: Accept-Encoding
|   Connection: close
|   Content-Type: text/html
|_ (Request type: HEAD)
| http-methods:
|_ Supported Methods: POST OPTIONS GET HEAD
443/tcp   open  https
| http-headers:
|   Date: Sat, 13 Sep 2025 09:36:30 GMT
|   Server: Apache
|   Expires: Sun, 19 Nov 1978 05:00:00 GMT
|   Cache-Control: no-cache, must-revalidate
|   X-Content-Type-Options: nosniff
|   Content-Language: en
|_ X-Frame-Options: SAMEORIGIN
```

```
(ragila@kali)-[~]
$ nmap --script vuln -p 80,443 -oA nmap_vuln itsecgames.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 05:49 EDT
Nmap scan report for itsecgames.com (31.3.96.40)
Host is up (0.18s latency).
rDNS record for 31.3.96.40: web.mmebvba.com

PORT      STATE SERVICE
80/tcp    open  http
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|   State: LIKELY VULNERABLE
|   IDs:  CVE:CVE-2007-6750
|   Slowloris tries to keep many connections to the target web server open and hold
|   them open as long as possible. It accomplishes this by opening connections to
|   the target web server and sending a partial request. By doing so, it starves
|   the http server's resources causing Denial Of Service.
|
|   Disclosure date: 2009-09-17
|   References:
|     http://ha.ckers.org/slowloris/
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
443/tcp    open  https
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
```

```
(ragila@kali)-[~]
$ searchsploit apache 2.4.29
```

Exploit Title	Path
Apache < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution	php/remote/29290.c
Apache < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner	php/remote/29316.py
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation	linux/local/46676.php
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service	multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow	unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)	unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal	linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing	multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal	unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)	multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)	windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)	jsp/webapps/42956.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)	linux/dos/36906.txt
WebFroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution	linux/remote/34.pl

```
Shellcodes: No Results
```

- **Recommendation:** Upgrade Apache to the latest stable release (2.4.58 or later). Regular patch management should be enforced.

## Finding 2 – SSL/TLS Certificate Issues

- **Severity:** High
- **Description:** The SSL certificate presented by itsecgames.com does not match the domain name. It is issued for mmebv.be and related domains. This leads to a hostname mismatch.
- **Impact:** Users may see browser warnings. Attackers could exploit this with man-in-the-middle attacks. Trust is reduced significantly.
- **Evidence:**
  - sslyze and testssl.sh results showing CN = mmebv.be instead of itsecgames.com.
  - **Browser warning:**



- **sslyze output snippet:**

```

Server extended key usage TLS Web Server Authentication, TLS Web Client Authentication
Serial 06E468197E9A3EF3332D35A842F858AF9E9C (OK: length 18)
Fingerprints SHA1 18049AA19AFDD1F91DA0F2386907BE12DD45BFA8
SHA256 66865FC2565018A5FC7A53F8AA7CF7478B129A5F3A4B20DB01331C2CCA60A
Common Name (CN) mmebv.be (CN in response to request w/o SNI: web.mmebvba.com )
subjectAltName (SAN) mmebv.be mmebv.com mmebvba.com mmesec.be mmesec.com www.mmebv.be www
Trust (hostname) certificate does not match supplied URI (same w/o SNI)
Chain of trust OK
EV cert (experimental) no
Certificate Validity (UTC) 51 ≥ 30 days (2025-08-06 09:47 → 2025-11-04 09:46)
ETS/"eTLS", visibility info not present
Certificate Revocation List http://r10.c.lencr.org/29.crl

```

- **Recommendation:** Obtain and install a valid SSL/TLS certificate that matches the domain itsecgames.com.

### Finding 3 – Missing Security Headers

- **Severity:** Medium
- **Description:** The server response is missing critical HTTP security headers such as:
  - Strict-Transport-Security (HSTS)
  - Content-Security-Policy (CSP)
  - X-XSS-Protection
- **Impact:** Increases risk of XSS, clickjacking, and downgrade attacks.
- **Evidence:**
  - curl -I http://itsecgames.com response showing only limited headers (X-Frame-Options, X-Content-Type-Options)

```

(ragila@kali)-[~]
$ curl -I http://itsecgames.com

HTTP/1.1 200 OK
Date: Sun, 14 Sep 2025 04:10:28 GMT
Server: Apache
Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT
ETag: "e43-5d7959bd3c800"
Accept-Ranges: bytes
Content-Length: 3651
Vary: Accept-Encoding
Content-Type: text/html

```

- **Recommendation:** Configure Apache to include missing security headers. Example:

Header set Strict-Transport-Security "max-age=31536000; includeSubDomains"

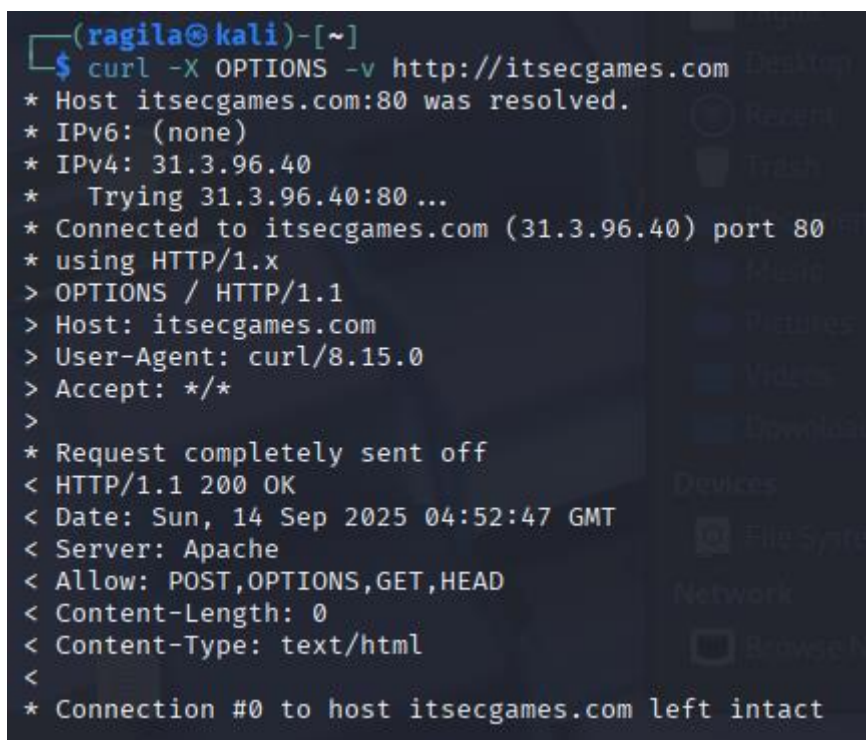
Header set Content-Security-Policy "default-src 'self'"

Header set X-XSS-Protection "1; mode=block"



## Finding 4 – Allowed HTTP Methods

- **Severity:** Low
- **Description:** The server allows the OPTIONS method in addition to GET, POST, and HEAD. While not directly exploitable, OPTIONS may provide attackers with information about supported methods.
- **Impact:** Information disclosure.
- **Evidence:**
  - curl -X OPTIONS -v http://itsecgames.com showing Allow: POST,OPTIONS,GET,HEAD.



```
(ragila@kali)-[~]
$ curl -X OPTIONS -v http://itsecgames.com
* Host itsecgames.com:80 was resolved.
* IPv6: (none)
* IPv4: 31.3.96.40
* Trying 31.3.96.40:80 ...
* Connected to itsecgames.com (31.3.96.40) port 80
* using HTTP/1.x
> OPTIONS / HTTP/1.1
> Host: itsecgames.com
> User-Agent: curl/8.15.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Sun, 14 Sep 2025 04:52:47 GMT
< Server: Apache
< Allow: POST,OPTIONS,GET,HEAD
< Content-Length: 0
< Content-Type: text/html
<
* Connection #0 to host itsecgames.com left intact
```

- **Recommendation:** Restrict HTTP methods to only what is required (usually GET and POST).

## Finding 5 – SSL/TLS Configuration Weaknesses

- **Severity:** Medium
- **Description:** The server supports only TLS 1.2, which is good, but TLS 1.3 is not enabled. Additionally, compression is enabled, which may lead to BREACH attacks if sensitive data is served.



- **Impact:** Attackers could exploit BREACH if secrets are included in compressed responses. Lack of TLS 1.3 reduces modern security guarantees.
- **Evidence:**
  - testssl.sh results showing TLS 1.2 only, BREACH risk, TLS 1.3 missing.

```
on kali:/tmp/testssl.sh/bin/openssl.Linux.x86_64
Testing all IPv4 addresses (port 443): 31.3.96.40

Start 2025-09-14 01:01:01 —> 31.3.96.40:443 (itsecgames.com) <—

rDNS (31.3.96.40): --
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN

SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      not offered
TLS 1.1    not offered
TLS 1.2    offered (OK)
TLS 1.3    not offered and downgraded to a weaker protocol
QUIC       not offered or timed out
```

```
ROBOT
Secure Renegotiation (RFC 5746)      Server does not support any cipher suites that use RSA key transport supported (OK)
Secure Client-Initiated Renegotiation not vulnerable (OK)
CRIME, TLS (CVE-2012-4929)            not vulnerable (OK)
BREACH (CVE-2013-3587)                potentially NOT ok, "gzip" HTTP compression detected. - only supplied "/" tested
                                      Can be ignored for static pages or if no secrets in the page
POODLE, SSL (CVE-2014-3566)           not vulnerable (OK), no SSLv3 support
TLS_FALLBACK_SCSV (RFC 7507)         No fallback possible (OK), no protocol below TLS 1.2 offered
SWEET32 (CVE-2016-2183, CVE-2016-6329) not vulnerable (OK)
FREAK (CVE-2015-0204)                not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703) not vulnerable on this host and port (OK)
```

```
Rating (experimental)

Rating specs (not complete)  SSL Labs's 'SSL Server Rating Guide' (version 2009r from 2025-05-16)
Specification documentation  https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
Protocol Support (weighted)  0 (0)
Key Exchange (weighted)     0 (0)
Cipher Strength (weighted)   0 (0)
Final Score                  0
Overall Grade                 M
Grade cap reasons             Grade capped to M. Domain name mismatch
Grade warning                 TLS 1.3 is not supported

Done 2025-09-14 01:07:08 [ 376s ] —> 31.3.96.40:443 (itsecgames.com) <—
```

- **Recommendation:** Enable TLS 1.3 in Apache configuration and disable HTTP compression for sensitive content.

## Information Disclosure Analysis

### Error Message Handling

- A request to a non-existent page (curl -I http://itsecgames.com/doesnotexist.php) returned a standard 404 Not Found response.
- No stack traces or sensitive debugging information were disclosed.
- Server banner (Apache) is still visible in the header, which increases fingerprinting risk.

## Input Handling

- A malformed query (curl -I "http://itsecgames.com/index.php?id=") also returned 404 Not Found with no SQL error or debug output.
- This suggests some filtering is in place, but the banner leakage remains.

## Directory Access

- Directory /downloads/ returned 403 Forbidden, confirming access restrictions are in place.
- Attempted file access (index.html) resulted in 404 Not Found.
- No sensitive files such as .env, config.php, or backup.sql were identified during testing.

**Finding:** Information disclosure is limited, but Apache banners and missing security headers provide attackers with useful reconnaissance data.

## Prioritized Findings Report

Severity	Finding	Evidence	Recommendation
High	Outdated Apache 2.4.29 (known CVEs, e.g., CVE-2019-0211)	nmap -sV + searchsploit apache 2.4.29	Upgrade Apache to latest stable version.
High	Certificate domain mismatch (issued to mmebv.be, not itsecgames.com)	sslyze --certinfo / testssl.sh	Install a valid certificate matching itsecgames.com.
Medium	TLS1.3 not supported (only TLS1.2 offered)	testssl.sh	Enable TLS1.3 for modern security compliance.
Medium	BREACH vulnerability risk due to HTTP compression	testssl.sh	Disable compression or ensure no secrets in compressed responses.
Medium	Missing security headers (HSTS, CSP, X-XSS-Protection)	curl -I	Add missing headers in Apache config.
Low	OPTIONS method enabled	curl -X OPTIONS -v	Restrict methods to only those required (GET, POST, HEAD).
Low	Apache banner exposed in error pages and headers	curl -I / 404 page	Disable server signature and banner exposure in Apache config.

## Conclusion

The assessment of itsecgames.com revealed multiple areas of concern:

- The server is running Apache 2.4.29, an outdated version with several high-severity CVEs.
- SSL/TLS implementation is misconfigured, with a certificate mismatch and no support for TLS1.3.
- Several security headers are missing, reducing client-side protection.
- Minor findings, such as enabled OPTIONS method and server banner exposure, provide additional attack surface.

Overall Risk: High

Immediate remediation is recommended for Apache upgrade and SSL certificate replacement. Secondary actions include enabling TLS1.3, applying modern headers, and restricting HTTP methods.