

Report

Target: <http://www.itsecgames.com>

Date: October 2025

Performed by: Aakash Dagadu Patil

It includes:

- Objective
- Tools used
- Scan findings (Nmap, Nikto, ZAP, Netcraft, Headers)
- CVE Mapping
- SSL/TLS analysis
- Prioritized list of findings
- Mitigation recommendations
- Video demo script

1. Objective

To evaluate the security posture of the publicly hosted endpoint

<http://www.itsecgames.com>.

Tasks include identifying vulnerabilities, outdated software, SSL/TLS configuration issues, and providing mitigation recommendations.

2. Tools Used

Tool	Purpose
Nmap	Network and service enumeration
Nikto	Web server vulnerability scanning
OWASP ZAP	Web application security scanning
SearchSploit	CVE mapping for detected versions
Netcraft	SSL/TLS and hosting information
Smart Scanner	Automated vulnerability analysis

curl / whois / dig	Header and DNS information gathering
---------------------------	--------------------------------------

3. Target Information

Attribute	Details
Domain	itsecgames.com
IP Address	31.3.96.40
Hosting Provider	team.blue, Netherlands
Web Server	Apache HTTPD
Framework	Drupal 7 (identified by Nikto)
DNSSEC	Not enabled
Registrar	GoDaddy
Certificate Common Name	mmebv.be (Mismatch with itsecgames.com)

4. Nmap Scan Summary

Command Used:

```
nmap -Pn -sS -sV -p- --min-rate=1000 itsecgames.com
```

Port	State	Service	Version	Risk
22/tcp	open	ssh	OpenSSH 6.7p1	Outdated – CVE-2018-15473
80/tcp	open	http	Apache httpd	Exposed headers, no HTTPS redirect
443/tcp	open	https	Apache httpd	Certificate mismatch

Observation:

Server exposes outdated OpenSSH and Apache versions, increasing the risk of RCE and information disclosure.

5. Nikto Scan Findings

Command Used:

```
nikto -h http://itsecgames.com
```

Finding	Description	Severity
Missing X-Frame-Options	No clickjacking protection	Medium
Missing X-Content-Type-Options	MIME-sniffing possible	Medium
ETag header exposed	Information disclosure (CVE-2003-1418)	Low
Apache default file /icons/README	Default directory accessible	Low
Drupal 7 detected	Outdated CMS with known CVEs	High

6. OWASP ZAP Findings

Risk	Alert	Description	CWE
Medium	Content Security Policy (CSP) Header Not Set	Increases XSS risk	CWE-693
Medium	Missing Anti-Clickjacking Header	Frame injection possible	CWE-1021
Low	X-Content-Type-Options Header Missing	MIME sniffing risk	CWE-693
Informational	User-Agent Fuzzer	Passive scan info	-

Summary:

Web app lacks critical security headers, increasing exposure to XSS and Clickjacking.

7. CVE Mapping (SearchSploit Results)

Apache HTTP Server

CVE	Description	Severity
CVE-2021-41773	Path Traversal & RCE in Apache 2.4.49	High
CVE-2019-10092	mod_proxy Cross-Site Scripting	Medium
CVE-2019-10098	mod_rewrite Open Redirect	Medium
CVE-2016-1546	mod_http2 DoS	Medium

OpenSSH

CVE	Description	Severity
CVE-2018-15473	Username Enumeration (2.3 – 7.7)	Medium

8. SSL/TLS & Certificate Analysis (Netcraft Report)

Attribute	Finding	Risk
Common Name	mmebv.be	✗ Mismatch
Validity	Oct 2025 – Jan 2026	Short term
Protocol	TLSv1.2 (No TLSv1.3)	Outdated
Perfect Forward Secrecy	Enabled	✓ Secure
DNSSEC	Not enabled	✗ Moderate
OCSP / Stapling	Not configured	Minor

9. HTTP Header & DNS Reconnaissance

Header	Observation	Risk
Server	Apache	Version disclosure
Security Headers	Missing CSP, XFO, XCTO	XSS & Clickjacking
HTTPS Redirect	Not enforced	Plaintext communication
DNSSEC	Not enabled	DNS spoofing possible

Recommendations:

ServerTokens Prod

ServerSignature Off










Header always set X-Frame-Options "SAMEORIGIN"

Header always set X-Content-Type-Options "nosniff"

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

10. Prioritized List of Findings & Mitigation

Recommendations

Priority	Finding	Description	Mitigation
 High	Outdated Apache HTTP Server	Vulnerable to RCE & Path Traversal (CVE-2021-41773)	Upgrade Apache \geq 2.4.58, disable unused modules
 High	Outdated OpenSSH 6.7p1	Username enumeration (CVE-2018-15473)	Update OpenSSH \geq 9.x, enable Fail2ban
 High	SSL Certificate Mismatch	CN = mmebv.be, allows MITM	Reissue valid certificate for itsecgames.com
 Medium	Missing Security Headers	XSS & Clickjacking risk	Add headers (CSP, XFO, XCTO)
 Medium	Outdated Drupal 7 CMS	End-of-life, multiple CVEs	Upgrade to Drupal 10 or newer
 Low	ETag Disclosure	Information leak	Disable with FileETag None
 Low	DNSSEC Disabled	DNS spoofing possible	Enable DNSSEC at registrar
 Low	HTTP Allowed	No HTTPS enforcement	Force redirect using .htaccess or Apache config
 Info	Server Info Disclosure	Aids recon	Hide version (ServerTokens Prod)

11. General Recommendations

1. **Patch Management:** Apply monthly updates for Apache, SSH, and CMS.
2. **TLS Hardening:** Disable TLS 1.0/1.1 and weak ciphers; prefer TLS 1.3.
3. **Web Hardening:** Apply headers and restrict directory listings.
4. **Monitoring:** Deploy host-based IDS (e.g., Wazuh or OSSEC).
5. **Access Control:** Restrict SSH by IP; use key-based authentication.
6. **Continuous Scanning:** Automate Nikto/ZAP every quarter.



12. Conclusion

The website `itsecgames.com` demonstrates multiple real-world vulnerabilities:

- Outdated Apache and OpenSSH versions
- Invalid SSL certificate
- Missing HTTP security headers
- DNSSEC not enabled

Implementing the listed mitigations will significantly strengthen the confidentiality, integrity, and availability of the system.