Web Application Security Assessment Report – bWAPP

Sept. 2025

Prepared by: Sachin Mishra

Contents

1. Executive Summary

A comprehensive security assessment of itsecgames.com identified multiple critical and high-risk issues. The target is hosting **bWAPP (http://itsecgames.com)**, an intentionally vulnerable application designed for training purposes. If treated as a production asset, its security posture is Critical and susceptible to exploitation.

Key findings include:

- Outdated Drupal 7 CMS and OpenSSH 6.7p1 with known CVEs.
- Missing security headers such as CSP, X-Frame-Options, and X-Content-Type-Options.
- TLS configuration supporting only TLS 1.2, lacking TLS 1.3.
- Exposure of default Apache files and inconsistent responses to user-agents.

Remediation requires immediate isolation of bWAPP, upgrading outdated components, and enforcing modern security configurations.

Tools Used

- **Nmap:** Port scanning, service enumeration, SSH version detection
- **Nikto:** Web server misconfiguration and default file exposure
- **OWASP ZAP:** HTTP header analysis, XSS, clickjacking detection
- **SSLScan:** TLS version and cipher suite analysis
- **Manual Analysis:** Header inspection, CVE correlation, OWASP Top 10 mapping

2. Results

1	1	2	2	2
Critical	High	Medium	Low	Informational

Sr. No.	Vulnerabilities	CVSS Score	Risk Category
4.1	Exposed Vulnerable Application (bWAPP)	9.8	Critical
4.2	Outdated OpenSSH 6.7p1	8.1	High
4.3	Missing CSP Header	6.5	Medium
4.4	Missing Anti-Clickjacking Header	6.5	Medium
4.5	X-Content-Type-Options Missing	4.8	Low
4.6	Apache Default File Exposed (/icons/README)	4.3	Low
4.7	TLS 1.3 Disabled (TLS 1.2 only)	NA	Informational
4.8	User-Agent Fuzzer (Inconsistent Responses)	NA	Informational

Total Vulnerabilities Identified: 8

3. Methodology

Testing followed OWASP and PTES best practices:

1. Reconnaissance & Enumeration
   - Nmap for open ports and service versions
   - Curl for HTTP header inspection
2. Vulnerability Scanning
   - Nikto for web server misconfigurations
   - OWASP ZAP for OWASP Top 10 issues
3. SSL/TLS Analysis
   - SSLScan for supported protocols, ciphers, and certificates
4. Manual Verification
   - Correlation of results with CVE databases
   - OWASP Top 10 mapping

4. Findings

4.1 Outdated Drupal 7 Backend

- CVSS v3.1 Score/Vector: 9.8 (Critical) – AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- OWASP Top 10: A06:2021 – Vulnerable & Outdated Components

Description: Drupal 7 has reached end-of-life and is no longer supported with security patches. Numerous CVEs exist for Drupal 7, including remote code execution and SQL injection vulnerabilities.

Impact: Attackers can exploit known Drupal vulnerabilities to gain full system compromise, deface content, or exfiltrate sensitive data.

Evidence: Nikto scan revealed the header: X-Generator: Drupal 7.

```
sachin@sachin:~/Downloads$ nikto -h http://itsecgames.com -output nikto_report.txt
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          31.3.96.40
+ Target Hostname:    itsecgames.com
+ Target Port:        80
+ Start Time:         2025-09-08 20:42:41 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ Server leaks inodes via ETags, header found with file /, fields: 0xe43 0x5d7959b
d3c800
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ Uncommon header 'link' found, with contents: <http://nikto/>; rel="canonical",<h
ttp://nikto/>; rel="shortlink"
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'x-ua-compatible' found, with contents: IE=edge
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 1 error(s) and 9 item(s) reported on remote host
+ End Time:           2025-09-08 21:24:04 (GMT5.5) (2483 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Recommendation: Upgrade to a supported version (Drupal ≥ 9/10) or migrate to a modern CMS. Apply ongoing patch management.

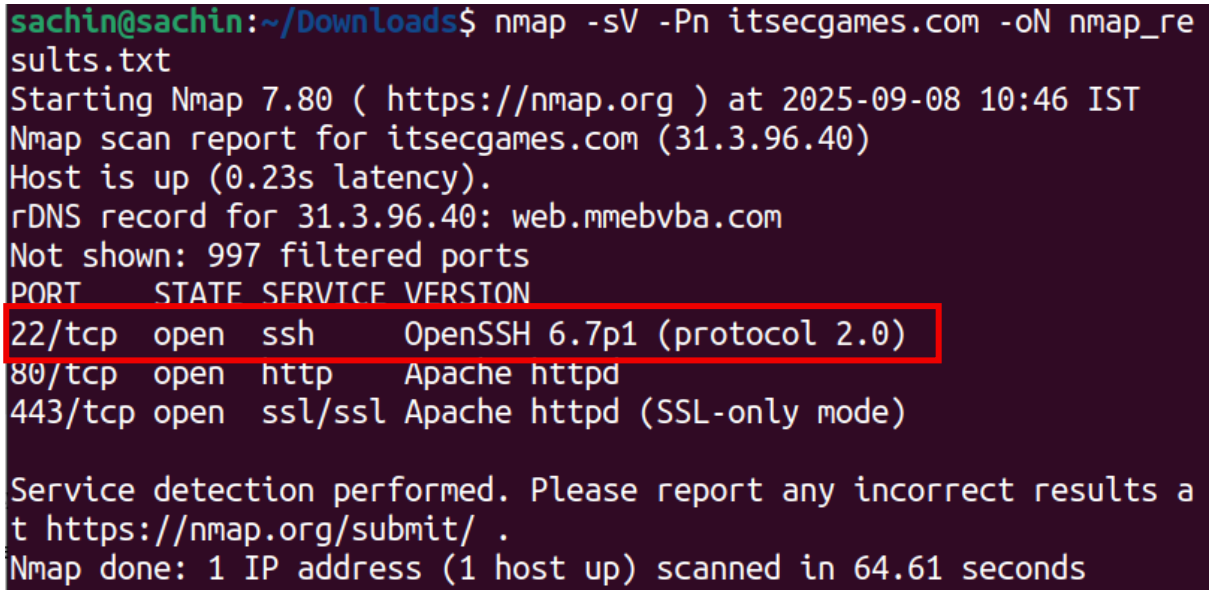
4.2 Outdated OpenSSH 6.7p1

- CVSS v3.1 Score/Vector: 8.1 (High) – AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
- OWASP Top 10: A06:2021 – Vulnerable & Outdated Components

Description: Nmap identified the SSH service as OpenSSH 6.7p1, released in 2014. This version is vulnerable to multiple CVEs, including CVE-2015-5600 (keyboard-interactive brute force).

Impact: An attacker may brute force or exploit OpenSSH to gain unauthorized shell access, leading to full server compromise.

Evidence: Nmap output: 22/tcp open ssh OpenSSH 6.7p1.



Recommendation: Upgrade OpenSSH to the latest stable release (≥ 9.x). Restrict SSH to trusted IPs only and enforce key-based authentication.

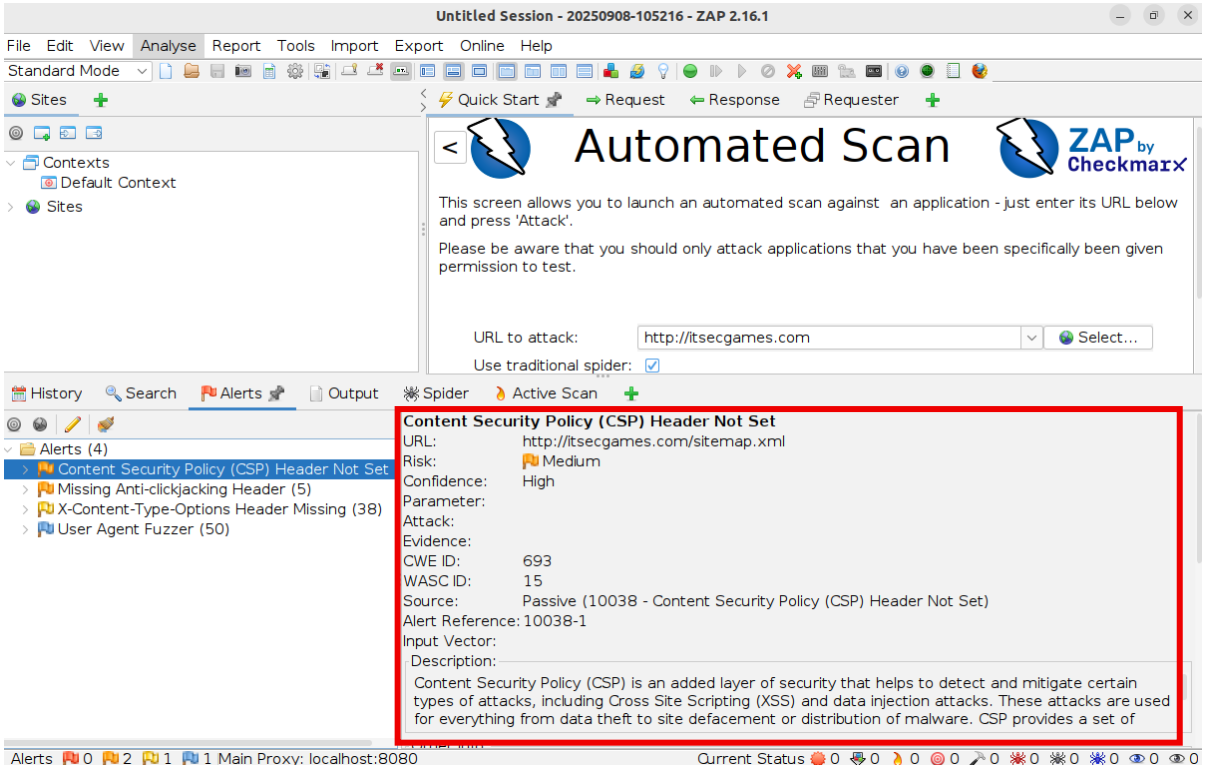
4.3 Missing Content Security Policy (CSP) Header

- CVSS v3.1 Score/Vector: 6.5 (Medium) – AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
- OWASP Top 10: A05:2021 – Security Misconfiguration / A03:2021 – Injection

Description: The application does not implement a Content Security Policy (CSP) header, leaving it vulnerable to XSS and script injection attacks.

Impact: Malicious scripts may be injected into the site, leading to credential theft or session hijacking.

Evidence: OWASP ZAP reported CSP Header Not Set for sitemap.xml.



Recommendation: Implement a strict CSP header (e.g., Content-Security-Policy: default-src 'self';).

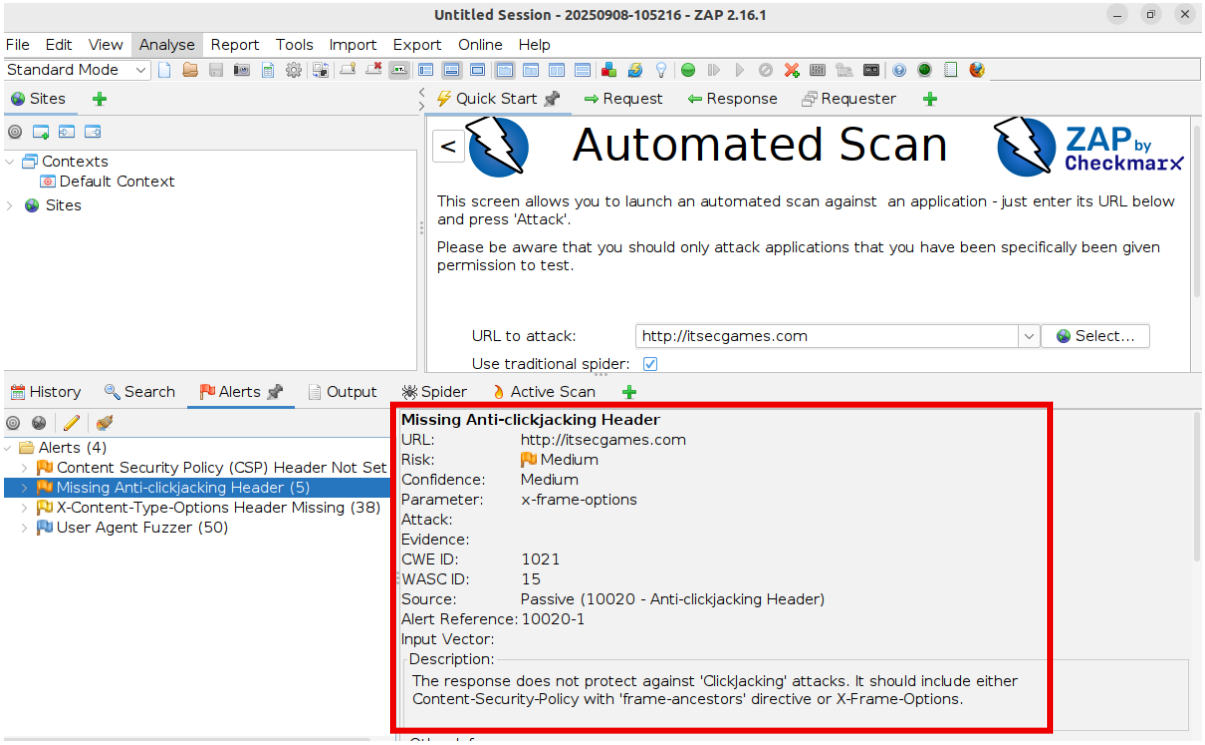
4.4 Missing Anti-Clickjacking Header

- CVSS v3.1 Score/Vector: 6.5 (Medium) – AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
- OWASP Top 10: A05:2021 – Security Misconfiguration

Description: The site does not include the X-Frame-Options or frame-ancestors CSP directive.

Impact: An attacker can embed the application in an iframe and trick users into unintended actions (clickjacking).

Evidence: OWASP ZAP finding: Missing Anti-Clickjacking Header.



Recommendation: Implement X-Frame-Options: DENY or SAMEORIGIN, or use CSP frame-ancestors 'none';.

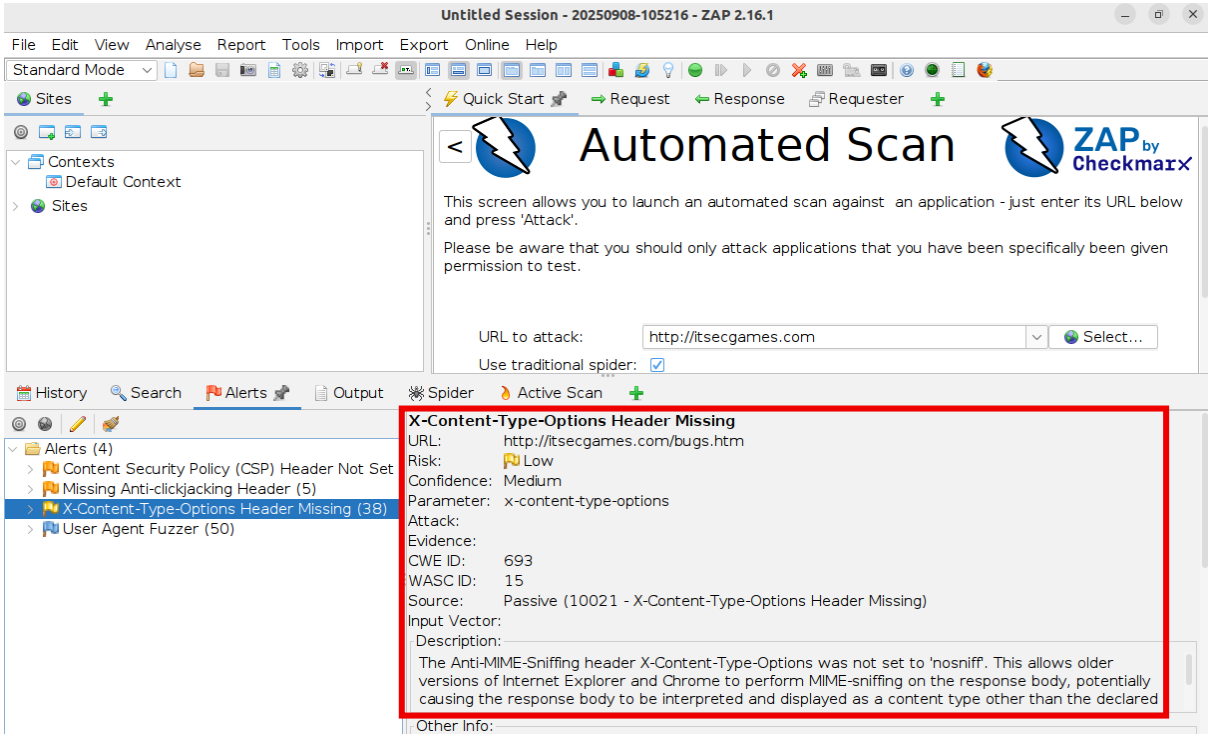
4.5 X-Content-Type-Options Header Missing

- CVSS v3.1 Score/Vector: 4.8 (Low) – AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N
- OWASP Top 10: A05:2021 – Security Misconfiguration

Description: The site does not include the X-Content-Type-Options: nosniff header.

Impact: Browsers may perform MIME sniffing, allowing attackers to bypass intended content-type restrictions.

Evidence: ZAP finding: X-Content-Type-Options Header Missing on bugs.htm.



Recommendation: Add X-Content-Type-Options: nosniff.

4.6 Apache Default File Exposed (/icons/README)

- CVSS v3.1 Score/Vector: 4.3 (Low) – AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
- OWASP Top 10: A05:2021 – Security Misconfiguration

Description: The server exposes /icons/README, a default Apache installation file.

Impact: Information disclosure about the server configuration.

Evidence: Nikto reported /icons/README.

```
sachin@sachin:~/Downloads$ nikto -h http://itsecgames.com -output nikto_report.txt
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          31.3.96.40
+ Target Hostname:    itsecgames.com
+ Target Port:        80
+ Start Time:         2025-09-08 20:42:41 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ Server leaks inodes via ETags, header found with file /, fields: 0xe43 0x5d7959b
d3c800
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ Uncommon header 'link' found, with contents: <http://nikto/>; rel="canonical",<h
ttp://nikto/>; rel="shortlink"
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'x-ua-compatible' found, with contents: IE=edge
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 1 error(s) and 9 item(s) reported on remote host
+ End Time:           2025-09-08 21:24:04 (GMT5.5) (2483 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Recommendation: Remove default Apache files and disable directory listing.

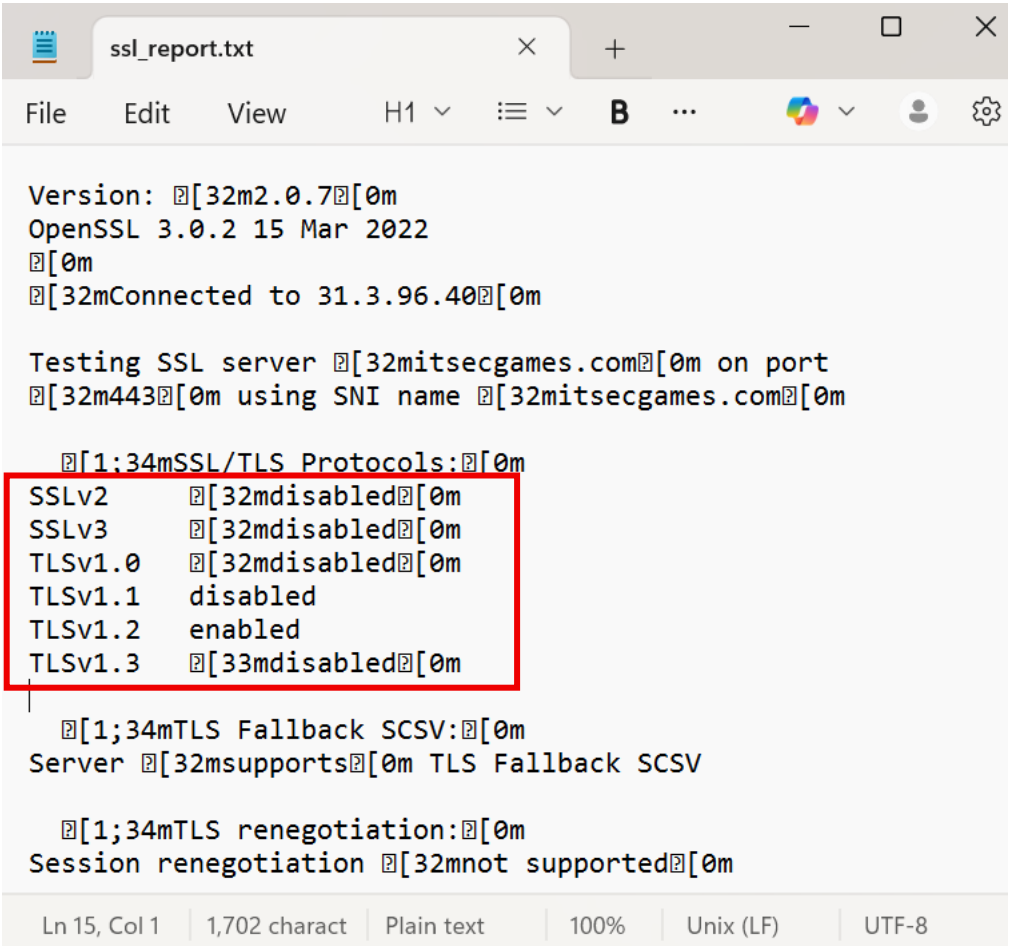
4.7 TLS 1.3 Disabled (TLS 1.2 Only)

- CVSS v3.1 Score/Vector: 3.7 (Informational) – NA
- OWASP Top 10: A05:2021 – Security Misconfiguration

Description: The server supports only TLS 1.2 and does not implement TLS 1.3.

Impact: While TLS 1.2 is secure, lack of TLS 1.3 means weaker forward secrecy and slower handshakes.

Evidence: SSLScan output confirmed only TLS 1.2 support.



Recommendation: Enable TLS 1.3 and enforce HSTS (Strict-Transport-Security).

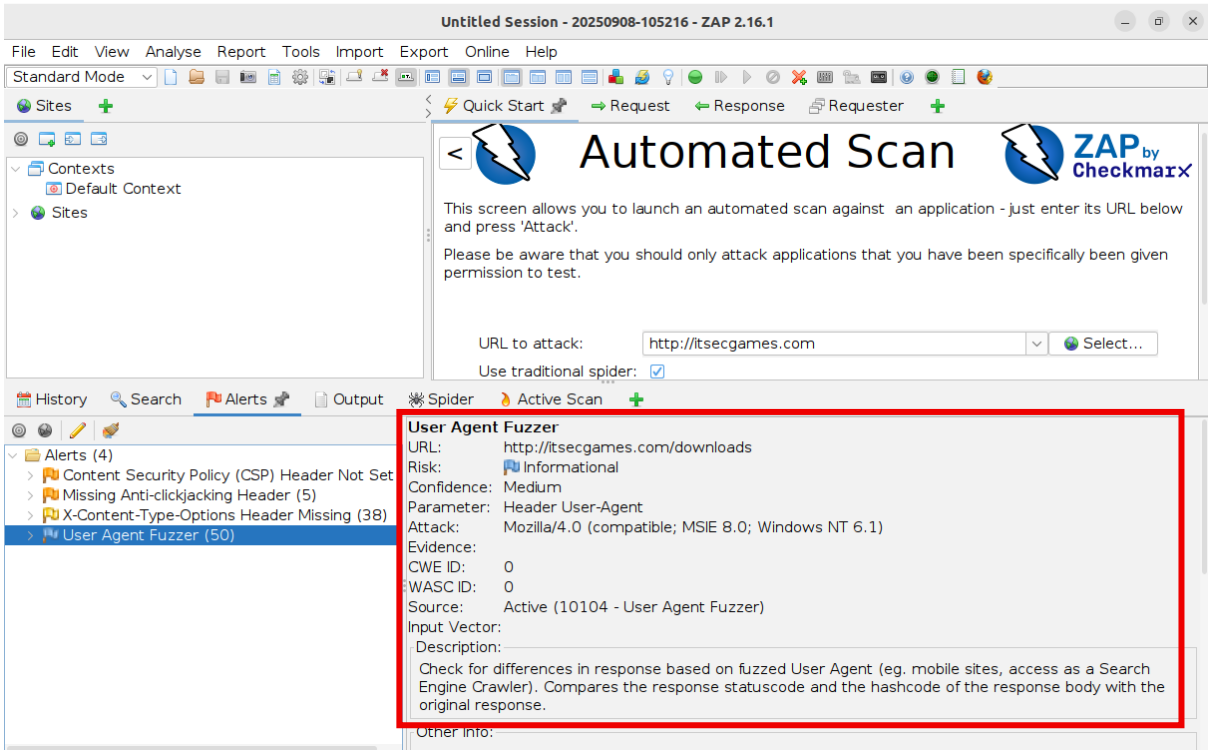
4.8 User-Agent Fuzzer (Inconsistent Responses)

- CVSS v3.1 Score/Vector: (Informational) – NA
- OWASP Top 10: A05:2021 – Security Misconfiguration

Description: The application returned inconsistent responses when tested with different User-Agent strings.

Impact: Could aid attackers in fingerprinting and evasion techniques.

Evidence: OWASP ZAP User Agent Fuzzer plugin finding.



Recommendation: Standardize server responses regardless of User-Agent.

5. SSL/TLS Assessment Summary

- **Protocols:** The server supports **TLS 1.2** as the only secure protocol. While TLS 1.2 is still widely used and considered secure when paired with modern ciphers, the lack of support for **TLS 1.3** is a weakness. TLS 1.3 offers better performance (fewer handshake round trips), enhanced security features, and removes older cryptographic constructs that have potential vulnerabilities. Not enabling TLS 1.3 may indicate outdated server configuration and can reduce compatibility with modern security expectations.
- **Ciphers:** The supported ciphers are **AES-GCM (128-bit and 256-bit)**. These are considered **strong and secure** as they provide authenticated encryption, protecting both the confidentiality and integrity of data. No evidence of weak or deprecated ciphers (such as RC4, 3DES, or NULL ciphers) was observed, which indicates good cipher hygiene on the server.
- **Certificate:** The site uses a **2048-bit RSA certificate**, which is the current industry baseline for public key infrastructure (PKI). The certificate is valid until **November 2025**, meaning it is still within its trusted period and does not pose an immediate expiry risk. The RSA 2048-bit key size is secure for the time being, but industry best practice is shifting towards **Elliptic Curve Cryptography (ECC)** or **RSA 3072/4096-bit** for stronger long-term resilience, especially in the context of emerging quantum threats.
- **Weaknesses:**
  - **TLS 1.3 Disabled:** The absence of TLS 1.3 is a configuration weakness. Modern browsers and security standards increasingly recommend TLS 1.3 for improved security and reduced handshake latency.
  - **No HSTS (HTTP Strict Transport Security):** The server does not enforce HSTS, which means clients may still attempt insecure (HTTP) connections. This leaves users vulnerable to downgrade and **SSL stripping attacks** where attackers can force communication over plaintext HTTP. Implementing HSTS ensures browsers automatically use HTTPS for future connections.
- **Risk Rating:**
  - Medium: Due to lack of TLS 1.3 and missing HSTS, which could enable downgrade attacks or reduce security against modern threat models.

Otherwise, the cryptographic strength of TLS 1.2 and AES-GCM is acceptable.

6. Prioritized Remediation Roadmap

- **Restrict bWAPP to Internal/VPN-only (High Priority)**
  - Restrict access to **internal networks only** or require **VPN-based access**.
  - If external use is necessary, protect it behind **authentication, firewalls, and IP allowlists**.
- **Upgrade Outdated Software – Drupal & OpenSSH (High Priority)**
  - Migrate to the latest **Drupal 10.x** version or an actively supported CMS.
  - Upgrade **OpenSSH** to a current stable release (9.x or later).
  - Apply ongoing patch management policies to avoid similar risks.
- **Add Missing Security Headers (Medium Priority)**
  - Configure web server (Apache) to include:
    - Content-Security-Policy: default-src 'self';
    - X-Frame-Options: SAMEORIGIN
    - X-Content-Type-Options: nosniff
- **Harden Apache Configuration (Medium Priority)**
  - Disable **ServerSignature** and **ServerTokens** to prevent version disclosure.
  - Enable **mod_security** and **mod_evasive** for request filtering and DoS protection.
  - Remove unused Apache modules.
  - Enforce secure cookie flags (HttpOnly, Secure, SameSite).
- **Enable TLS 1.3 and Enforce HSTS (Medium Priority)**
  - Enable **TLS 1.3** alongside TLS 1.2 in Apache's SSL configuration.
  - Add the following header:
    - Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
  - Periodically re-test SSL/TLS with **Qualys SSL Labs** to maintain compliance.

7. Conclusion

The assessment of itsecgames.com revealed multiple critical and high-risk security vulnerabilities that significantly compromise the confidentiality, integrity, and availability of the application and its underlying infrastructure. The presence of outdated software (Drupal 7, OpenSSH 6.7p1), missing security headers, and weak TLS implementation indicates a lack of regular patching, security hardening, and configuration management.

These weaknesses expose the application to a wide range of real-world attack vectors, including remote code execution, injection attacks, credential theft, clickjacking, and man-in-the-middle (MitM) attacks. Exploitation of these flaws could result in data breaches, service disruption, defacement, or complete system compromise.

If this application is supporting production workloads or sensitive business operations, its current security posture is unacceptable. Immediate action must be taken to:

i. Upgrade outdated components and apply vendor security patches.
ii. Implement missing security headers to mitigate client-side attacks.
iii. Strengthen SSL/TLS by enabling TLS 1.3 and enforcing HSTS.
iv. Harden server configurations and remove unnecessary files.
v. Establish a regular vulnerability management and penetration testing cycle.

Failure to address these issues could lead to regulatory non-compliance, reputational damage, and financial loss.

8. Appendices

Appendix A: Abbreviations

Abbreviation	Full Form
CSP	Content Security Policy
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DAST	Dynamic Application Security Testing
DoS	Denial of Service
EOL	End of Life
ETag	Entity Tag
HSTS	HTTP Strict Transport Security
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IDOR	Insecure Direct Object Reference
OWASP	Open Worldwide Application Security Project
PTES	Penetration Testing Execution Standard
RCE	Remote Code Execution
SAN	Subject Alternative Name
SAST	Static Application Security Testing
SQLi	SQL Injection
SSH	Secure Shell
SSL	Secure Sockets Layer
SSV	Server Side Validation
TLS	Transport Layer Security
UI	User Interaction
VPN	Virtual Private Network
XSS	Cross-Site Scripting
ZAP	Zed Attack Proxy

Appendix B: References

Sr. No	References
1	OWASP Top 10 (2021)
2	OWASP Testing Guide v4
3	CVSS v3.1 Specification
4	Nmap Security Scanner
5	Nikto Web Scanner
6	OWASP ZAP (Zed Attack Proxy)
7	SSLScan Tool
8	Apache Security Tips
9	Drupal Security Advisories
10	OpenSSH Security Updates
11	Mozilla Web Security Guidelines (CSP, HSTS, Headers)
12	Qualys SSL Labs – SSL/TLS Best Practices
13	OWASP Cheat Sheet Series (Security Headers)