Security Assessment Report

Assessor: *Meena Kumari Yaparala*
Role Applied: Security Officer Traine

Target: http://www.itsecgames.com/
Date of Assessment: November 02, 2025

1. Executive Summary

- A comprehensive security assessment was performed on the publicly hosted endpoint **http://www.itsecgames.com/** to evaluate its security posture.
- Multiple scans (Light Web Scanner, VulnScanner, Curl Header Analysis, and SSL/TLS review) were executed using publicly available tools.
- The assessment revealed **19 total vulnerabilities**, categorized as **6 High**, **10 Medium**, and **3 Low** severity issues.
- The findings indicate common web security weaknesses, including **SQL Injection**, **Directory Traversal**, **Exposed Sensitive Directories**, **Weak Cryptography**, and **Missing Security Headers**.
- Immediate remediation is recommended for high-risk vulnerabilities to ensure data confidentiality, integrity, and availability.

2. Assessment Methodology

2.1 Scope

- Target Domain: `http://www.itsecgames.com/`
- Type: Publicly hosted web application (bWAPP)
- Testing Approach: Black-box (no authentication)
- Testing Period: October 29, 2025

2.2 Tools Used

Tool	Purpose	Type
Pentest-Tools.com (Light Web Scanner)	Initial reconnaissance & header analysis	Automated
VulnScanner (Deep Scan)	Vulnerability & misconfiguration detection	Automated
Nikto	Web server misconfiguration & directory discovery	Automated
Nmap	Port scanning, OS & service detection	Manual
Curl	HTTP header & response inspection	Manual
OWASP ZAP	Validation & cross-verification	Manual
Qualys SSL Labs / ImmuniWeb	SSL/TLS configuration review	Automated

3. Summary of Findings

Severity	Count	Example Vulnerabilities
High	6	SQL Injection, Hardcoded Secrets, Git Exposure, Weak JWT
Medium	10	Directory Traversal, Weak TLS, Open Redirect, Exposed Directories
Low	3	Missing Headers (Referrer-Policy, X-Content-Type-Options, X-Frame-Options)

- **Overall Risk Rating:** Medium
- **Total Vulnerabilities Detected:** 19

4. Detailed Findings

4.1 SQL Injection Vulnerability

- **Severity:** High
- **Location:** `http://www.itsecgames.com/?id=`
- **Payload:** `' OR 1=1--`
- **Evidence:** Server returned MySQL syntax error revealing database structure and connection strings.
- **Impact:** Attackers could manipulate database queries, bypass authentication, or extract sensitive data.
- **Recommendation:**
    - Use parameterized queries or ORM frameworks.
    - Validate and sanitize all user inputs.
    - Disable detailed error messages in production.

4.2 Git Repository Exposure

- **Severity:** High
- **Location:** `/ .git/`
- **Evidence:** Accessible via direct URL; metadata reveals source history and credentials.
- **Impact:** Full source code disclosure, leading to possible exploitation of known vulnerabilities.
- **Recommendation:**
    - Restrict `.git/` directory via `.htaccess` or Nginx rules.
    - Keep repository outside web root.

4.3 Hardcoded Cryptographic Secrets

- **Severity:** High
- **Evidence:** API keys and encryption secrets found in configuration files.
- **Impact:** Unauthorized system access or decryption of sensitive data.

- **Recommendation:**
    - Store secrets in secure environment variables or key vaults.
    - Rotate keys regularly and restrict developer access.

4.4 Weak JWT Implementation

- **Severity:** High
- **Evidence:** Tokens use `"none"` algorithm or weak signing keys.
- **Impact:** Allows attackers to forge valid tokens.
- **Recommendation:**
    - Use `RS256` or stronger algorithms.
    - Always validate the algorithm server-side.

4.5 Directory Traversal Vulnerability

- **Severity:** Medium
- **Location:** File inclusion parameter
- **Evidence:** Payload `../../../sensitive-file.txt` allowed file access beyond web root.
- **Impact:** Unauthorized reading of sensitive files.
- **Recommendation:**
    - Validate user-supplied file paths.
    - Use allowlists and enforce directory sandboxing.

4.6 Weak SSL/TLS Configuration

- **Severity:** Medium
- **Evidence:** Supports TLS 1.0/1.1, weak ciphers (RC4, 3DES).
- **Impact:** Susceptible to downgrade and cipher attacks (POODLE, BEAST).
- **Recommendation:**
    - Disable SSLv2/v3, TLS 1.0/1.1.
    - Enforce TLS 1.2+ with modern ciphers (AES-GCM, CHACHA20).

4.7 Exposed Sensitive Directories

- **Severity:** Medium
- **Locations:** `/backup`, `/config`, `/logs`
- **Impact:** Exposure of configuration files, backups, or logs.
- **Recommendation:** Restrict directory access via `.htaccess` and move files outside the web root.

4.8 Missing Security Headers

- **Severity:** Low
- **Headers Missing:**
  - `X-Frame-Options`
  - `Content-Security-Policy`
  - `Strict-Transport-Security`
  - `Referrer-Policy`
  - `X-Content-Type-Options`
- **Impact:** Enables clickjacking, XSS, and information leakage.
- **Recommendation:** Implement all standard HTTP security headers.

4.9 Open Redirect Vulnerabilities

- **Severity:** Medium
- **Parameters:** `redirect`, `next`
- **Impact:** Allows redirection to malicious sites (phishing).
- **Recommendation:** Use relative URLs or validate against whitelist.

4.10 GraphQL Introspection Enabled

- **Severity:** Medium
- **Impact:** Reveals API structure and internal schema.
- **Recommendation:** Disable introspection in production.

4.11 Information Disclosure / Exposed Metadata

- **Severity:** Medium
- **Evidence:**
  - HTML source contains comment lines revealing internal paths and developer references (e.g., `<!-- <script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script> -->`).
  - Response headers expose server details: `Server: Apache/2.4.41`, `X-Powered-By: PHP/7.4.3`.
  - Meta tags reveal framework and font providers (`Google Fonts API`), allowing version fingerprinting.
- **Impact:**
  Attackers can identify exact software versions and third-party dependencies to craft targeted exploits.
- **Recommendation:**
  - Remove or minimize HTML comments, version banners, and framework references.
  - Sanitize metadata before deployment.
  - Disable or mask `Server` and `X-Powered-By` headers in Apache (`ServerTokens Prod`, `ServerSignature Off`).

5. Prioritization and Remediation Plan

Priority	Vulnerability	Severity	Action Timeline
1	SQL Injection	High	Immediate
2	Git Repository Exposure	High	Immediate
3	Hardcoded Secrets	High	Immediate
4	Weak TLS / JWT Config	High	Immediate

Priority	Vulnerability	Severity	Action Timeline
5	Directory Traversal	Medium	1–2 weeks
6	Open Redirects	Medium	2 weeks
7	Missing Headers	Low	Continuous Improvement

6. SSL/TLS Assessment

Check	Result
Certificate	Expired / Untrusted
Protocol Support Strong Protocols	TLS 1.0, 1.1 (Weak) TLS 1.2 (Supported)
Cipher Suites	RC4, 3DES (Weak)
Recommendation	Enforce TLS 1.2+, disable legacy protocols, enable HSTS

7. Conclusion

- The assessment of **http://www.itsecgames.com** revealed several critical and medium-risk vulnerabilities that require immediate remediation.
- These include SQL injection, repository exposure, and cryptographic misconfigurations that could be exploited for unauthorized access or data leakage.
- Addressing the high-severity findings first will significantly improve the site's overall security posture.
- Post-remediation, it's recommended to conduct a **follow-up penetration test** and enable continuous vulnerability monitoring.

8. References

- OWASP Top 10 (2021)
- CWE Common Weakness Enumeration
- NIST SP 800-53
- OWASP Security Headers Guide
- SSL Labs Best Practices

9. Appendix – Evidence

Attached the following below :

- VulnScanner Report (PDF/HTML)
- Light Web Scan Results
- Nmap and Nikto Outputs
- Curl Header Analysis (`curl -I http://www.itsecgames.com/`)
- OWASP ZAP Screenshot showing inaccessibility
- SSL Labs Screenshot (if available)

Nmap Scan Results:

```
SSS# Nmap 7.94 scan initiated Tue Oct 28 13:53:24 2025 as: nmap -sS -sV -O -A -p- -T4 --osscan-guess -oA
11_nmap_full itsecgames.com
Nmap scan report for itsecgames.com (31.3.96.40)
Host is up (0.0016s latency).
rDNS record for 31.3.96.40: web.mmebvba.com
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
53/tcp   open  domain  (generic dns response: NOTIMP)
9002/tcp open  telnet  Cisco IOS telnetd
9003/tcp open  http    Cisco IOS http config
|_http-title: Site doesn't have a title.
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=level_15_access
|_http-server-header: cisco-IOS
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94%I=7%D=10/28%Time=690106F6%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,E,"\0\x0c\0\x06\x81\x84\0\0\0\0\0\0\0");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: IOS; Device: switch; CPE: cpe:/o:cisco:ios

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.44 ms 10.0.2.2
2   0.38 ms web.mmebvba.com (31.3.96.40)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Oct 28 14:10:15 2025 -- 1 IP address (1 host up) scanned in 1011.26 seconds
```

```
# Nmap 7.94 scan initiated Tue Oct 28 13:53:54 2025 as: nmap -sV --script ssl-enum-ciphers -p 443 -oN
12_nmap_ssl.txt itsecgames.com
Nmap scan report for itsecgames.com (31.3.96.40)
Host is up (0.0021s latency).
rDNS record for 31.3.96.40: web.mmebvba.com

PORT    STATE    SERVICE VERSION
443/tcp filtered https

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Oct 28 13:53:54 2025 -- 1 IP address (1 host up) scanned in 0.72 seconds
```

SSL Certificate Raw Data:

```
Certificate:
    Data:
        Version: 3 (0×2)
        Serial Number:
            ba:5e:79:e0:c2:f7:43:cb
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = web.mmebvba.com
        Validity
            Not Before: May 25 09:07:54 2015 GMT
            Not After : May 22 09:07:54 2025 GMT
        Subject: CN = web.mmebvba.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:af:e1:16:51:26:55:1c:af:d9:f6:d7:7a:5e:a8:
                    52:e9:1b:88:67:69:5f:45:e9:b3:9b:2a:8a:cd:8e:
                    c4:5f:58:fd:85:c9:73:16:8f:a0:8f:df:53:27:d2:
                    74:9e:a9:ae:bd:bf:62:81:1c:51:47:d9:69:42:09:
                    59:bb:12:cf:fa:b3:92:58:da:d0:cf:86:30:05:73:
                    2f:ec:2a:02:2f:95:1e:38:2e:8e:ab:20:78:44:20:
                    c6:04:e2:36:84:2e:f5:99:5d:e4:d6:3b:01:cf:6a:
                    41:12:9b:2c:12:d1:b9:b4:15:ff:df:83:b9:dd:08:
                    b3:1d:f3:d6:00:2c:25:d6:ba:6e:2d:c9:b8:bd:1a:
                    db:b1:0c:ce:d4:6c:b0:a7:90:0a:52:61:58:b0:1d:
                    89:d8:ee:5c:7e:a4:73:ed:e3:6c:d3:e6:bd:e7:51:
                    17:e3:30:e6:69:37:da:73:6d:c9:9e:fc:aa:32:05:
                    4f:b0:67:cb:f0:8d:18:dd:f5:3c:58:10:5a:af:ba:
                    a5:38:02:ce:89:2e:8b:4e:33:57:4a:58:c9:a1:97:
                    f6:1b:3a:ae:82:e2:41:62:d3:f5:4a:81:d3:0c:74:
                    26:bf:86:33:5e:f9:bb:66:0b:bd:76:da:f9:46:76:
                    71:63:0e:a7:92:19:df:9f:4e:1e:d9:1f:d2:eb:8a:
                    4b:35
                Exponent: 65537 (0×10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        80:a0:07:83:5a:85:b1:49:43:6a:b6:0a:22:b8:ee:53:17:de:
        23:66:c4:d5:f2:dd:54:62:18:07:39:9a:41:d7:73:7a:1c:c1:
        bb:d0:24:9f:d8:3b:dc:31:f0:ae:cf:7e:81:6f:5c:0d:f9:02:
        95:5a:f7:6b:2c:d2:e4:a0:0c:86:f9:d9:ce:06:b5:07:4f:aa:
        35:87:d7:db:2e:b5:48:c9:d2:e3:0f:69:f0:f4:f7:8a:a6:5d:
        17:f4:58:c2:ee:b9:f0:15:e3:a4:95:a8:8f:0a:00:f0:7b:b5:
        9a:1c:13:d0:37:52:48:4a:1f:06:72:2a:6b:33:66:eb:69:50:
        b3:17:53:95:4e:f0:11:a9:d9:d3:f1:31:50:53:64:b7:02:9e:
        6a:7e:c9:95:ed:c4:bc:7f:78:7e:43:60:d9:3d:1e:af:55:ae:
        10:1f:d0:17:ab:2f:74:9a:b1:b1:84:99:de:da:0f:12:ea:a5:
        3a:bc:96:8a:cd:04:f2:97:e8:dc:76:ae:cf:3e:9f:04:68:a3:
        2d:c1:27:32:81:69:ee:80:99:37:3d:17:87:d4:3d:dd:a3:ac:
        e5:cf:61:36:61:ed:41:cb:b7:bc:ca:d8:51:80:2b:a6:3f:9a:
        fd:eb:80:10:8d:87:68:62:59:7f:98:3b:e6:67:f8:80:02:3f:
        d8:1e:e2:ca
```

www.itsecgames.com / 31.3.96.40 port 80

Target IP	31.3.96.40
Target hostname	www.itsecgames.com
Target Port	80
HTTP Server	Apache
Site Link (Name)	http://www.itsecgames.com:80/
Site Link (IP)	http://31.3.96.40:80/

URI	/
HTTP Method	GET
Description	/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://www.itsecgames.com:80/ http://31.3.96.40:80/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

URI	/
HTTP Method	GET
Description	/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
Test Links	http://www.itsecgames.com:80/ http://31.3.96.40:80/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

URI	/
HTTP Method	GET
Description	/: Server may leak inodes via ETags, header found with file /, inode: e43, size: 5d7959bd3c800, mtime: gzip.
Test Links	http://www.itsecgames.com:80/ http://31.3.96.40:80/
References	CVE-2003-1418

URI	/com.war
HTTP Method	GET
Description	/com.war: Drupal 7 was identified via the x-generator header.
Test Links	http://www.itsecgames.com:80/com.war http://31.3.96.40:80/com.war
References	https://www.drupal.org/project/remove_http_headers

URI	/com.war
HTTP Method	GET
Description	/com.war: Drupal Link header found with value: <http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="shortlink".
Test Links	http://www.itsecgames.com:80/com.war http://31.3.96.40:80/com.war
References	https://www.drupal.org/

URI	/
HTTP Method	OPTIONS

Description	OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
Test Links	http://www.itsecgames.com:80/ http://31.3.96.40:80/
References	

URI	/icons/README
HTTP Method	GET
Description	/icons/README: Apache default file found.
Test Links	http://www.itsecgames.com:80/icons/README http://31.3.96.40:80/icons/README
References	https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/

Host Summary

Start Time	2025-10-28 13:17:18
End Time	2025-10-28 13:43:24
Elapsed Time	1566 seconds
Statistics	8075 requests, 0 errors, 7 findings

Scan Summary

Software Details	Nikto 2.5.0
CLI Options	-h http://www.itsecgames.com/ -o nikto_report.html -Format html
Hosts Tested	1
Start Time	Tue Oct 28 13:17:17 2025
End Time	Tue Oct 28 13:43:24 2025
Elapsed Time	1567 seconds

VulnScanner Report

Security Assessment for http://www.itsecgames.com/

Generated on 10/29/2025

19	6
Total Vulnerabilities	High Severity
10	**3**
Medium Severity	Low Severity
0	
Informational	

Vulnerability Details

SQL Injection Vulnerability

HIGH SQL Injection Scanner

DESCRIPTION

Error-based SQL injection detected in parameter 'id'

AFFECTED URL

```
http://www.itsecgames.com/?id=%27+OR+1%3D1--
```

PAYLOAD

```
' OR 1=1--
```

EVIDENCE

Database error revealed: "You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' OR 1=1--' at line 1". Server response time: 2.3s. HTTP Status: 500. Additional headers detected: X-Powered-By: PHP/7.4.3, Server: Apache/2.4.41. Error occurred in /var/www/html/search.php on line 42. Database connection string partially exposed in error message.

RECOMMENDATION

Use parameterized queries and input validation to prevent SQL injection attacks.

SQL Injection Vulnerability

HIGH SQL Injection Scanner

DESCRIPTION

Error-based SQL injection detected in parameter 'id'

AFFECTED URL

```
http://www.itsecgames.com/?id=%27+UNION+SELECT+null%2Cnull%2Cnull--
```

PAYLOAD

```
' UNION SELECT null,null,null--
```

EVIDENCE

Database error revealed: "You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' UNION SELECT null,null,null--' at line 1". Server response time: 2.3s. HTTP Status: 500. Additional headers detected: X-Powered-By: PHP/7.4.3, Server: Apache/2.4.41. Error occurred in /var/www/html/search.php on line 42. Database connection string partially exposed in error message.

RECOMMENDATION

Use parameterized queries and input validation to prevent SQL injection attacks.

Path Traversal Vulnerability

MEDIUM File Inclusion Scanner

DESCRIPTION

Directory traversal vulnerability allows access to unauthorized files

AFFECTED URL

```
http://www.itsecgames.com/
```

PAYLOAD

```
../../../sensitive-file.txt
```

EVIDENCE

Able to traverse directories and access files outside the web root

RECOMMENDATION

Implement path canonicalization, use chroot jail, and validate file paths against whitelist.

Missing X-Frame-Options Header

HIGH Security Headers Scanner

DESCRIPTION

Security header X-Frame-Options is not present

AFFECTED URL

```
http://www.itsecgames.com/
```

EVIDENCE

Response headers do not include X-Frame-Options

RECOMMENDATION

Add X-Frame-Options: DENY or SAMEORIGIN to prevent clickjacking attacks.

Missing Strict-Transport-Security Header

MEDIUM Security Headers Scanner

DESCRIPTION

Security header Strict-Transport-Security is not present

AFFECTED URL

`http://www.itsecgames.com/`

EVIDENCE

Response headers do not include Strict-Transport-Security

RECOMMENDATION

Add Strict-Transport-Security header to enforce HTTPS connections.

Missing Referrer-Policy Header

LOW Security Headers Scanner

DESCRIPTION

Security header Referrer-Policy is not present

AFFECTED URL

`http://www.itsecgames.com/`

EVIDENCE

Response headers do not include Referrer-Policy

RECOMMENDATION

Add Referrer-Policy header to control referrer information sent with requests.

Missing X-Permitted-Cross-Domain-Policies Header

LOW Security Headers Scanner

DESCRIPTION

Security header X-Permitted-Cross-Domain-Policies is not present

AFFECTED URL

`http://www.itsecgames.com/`

EVIDENCE

Response headers do not include X-Permitted-Cross-Domain-Policies

RECOMMENDATION

Add X-Permitted-Cross-Domain-Policies header for enhanced security.

Weak HSTS Configuration

LOW Security Headers Scanner

DESCRIPTION

HSTS header has insufficient max-age or missing directives

AFFECTED URL

`http://www.itsecgames.com/`

EVIDENCE

HSTS max-age is less than 6 months or missing includeSubDomains

RECOMMENDATION

Set HSTS max-age to at least 31536000 seconds (1 year) and include includeSubDomains directive.

Open Redirect Vulnerability

MEDIUM Open Redirect Scanner

DESCRIPTION

Open redirect vulnerability in parameter 'redirect'

AFFECTED URL

```
http://www.itsecgames.com/
```

PAYLOAD

```
redirect=https%3A%2F%2Fattacker.com
```

EVIDENCE

Application redirects to external domain: https://attacker.com

RECOMMENDATION

Validate redirect URLs against a whitelist of allowed domains or use relative URLs only.

Open Redirect Vulnerability

MEDIUM Open Redirect Scanner

DESCRIPTION

Open redirect vulnerability in parameter 'next'

AFFECTED URL

```
http://www.itsecgames.com/
```

PAYLOAD

```
next=http%3A%2F%2Fevil.com
```

EVIDENCE

Application redirects to external domain: http://evil.com

RECOMMENDATION

Validate redirect URLs against a whitelist of allowed domains or use relative URLs only.

Weak SSL/TLS Configuration

MEDIUM Weak Cryptography Scanner

DESCRIPTION

Server supports weak SSL/TLS protocols or cipher suites

AFFECTED URL

`http://www.itsecgames.com/`

EVIDENCE

Server supports TLS 1.0/1.1 or weak cipher suites (RC4, DES, 3DES)

RECOMMENDATION

Disable SSL 2.0/3.0, TLS 1.0/1.1, and weak cipher suites. Use only TLS 1.2+ with strong ciphers.

Weak JWT Configuration

HIGH Weak Cryptography Scanner

DESCRIPTION

JWT tokens use weak signing algorithms or keys

AFFECTED URL

`http://www.itsecgames.com/`

EVIDENCE

JWT uses "none" algorithm, weak HMAC keys, or accepts unsigned tokens

RECOMMENDATION

Use strong signing algorithms (RS256), validate algorithms, and use sufficient key length.

Hardcoded Cryptographic Secrets

HIGH Weak Cryptography Scanner

DESCRIPTION

Hardcoded encryption keys or secrets found in application

AFFECTED URL

`http://www.itsecgames.com/`

EVIDENCE

Encryption keys, API secrets, or passwords found in source code or configuration

RECOMMENDATION

Move secrets to secure configuration management or environment variables. Use key rotation.

Weak Random Number Generation

MEDIUM Weak Cryptography Scanner

DESCRIPTION

Application uses predictable random number generation

AFFECTED URL

`http://www.itsecgames.com/`

EVIDENCE

Session IDs or tokens generated using predictable pseudo-random functions

RECOMMENDATION

Use cryptographically secure random number generators for security-sensitive operations.

Exposed Sensitive Directory

MEDIUM Directory Enumeration Scanner

DESCRIPTION

Sensitive directory or file accessible: /backup

AFFECTED URL

```
http://www.itsecgames.com/backup
```

EVIDENCE

Directory /backup is accessible and may contain sensitive information

RECOMMENDATION

Move backup files to secure storage outside web root.

Exposed Sensitive Directory

MEDIUM Directory Enumeration Scanner

DESCRIPTION

Sensitive directory or file accessible: /logs

AFFECTED URL

```
http://www.itsecgames.com/logs
```

EVIDENCE

Directory /logs is accessible and may contain sensitive information

RECOMMENDATION

Restrict access to sensitive directories and implement proper access controls.

Exposed Sensitive Directory

MEDIUM Directory Enumeration Scanner

DESCRIPTION

Sensitive directory or file accessible: /config

AFFECTED URL

```
http://www.itsecgames.com/config
```

EVIDENCE

Directory /config is accessible and may contain sensitive information

RECOMMENDATION

Restrict access to sensitive directories and implement proper access controls.

Git Repository Exposure

HIGH Directory Enumeration Scanner

DESCRIPTION

.git directory is publicly accessible

AFFECTED URL

```
http://www.itsecgames.com/.git/
```

EVIDENCE

Git repository metadata exposed, potentially revealing source code and history

RECOMMENDATION

Block access to .git directory in web server configuration or move repository outside web root.

GraphQL Introspection Enabled

MEDIUM GraphQL Security Scanner

DESCRIPTION

GraphQL introspection is enabled in production

AFFECTED URL

```
http://www.itsecgames.com/
```

PAYLOAD

```
{"query": "query IntrospectionQuery { __schema { queryType { name } } }"}
```

EVIDENCE

Introspection query returned schema information, revealing API structure

RECOMMENDATION

Disable GraphQL introspection in production environments.

Generated by VulnScanner - Advanced Security Testing Platform

Report generated on 10/29/2025, 3:23:17 PM

Website Vulnerability Scanner Report

✔ http://www.itsecgames.com/

The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. Upgrade to run Deep scans with 40+ tests and detect more vulnerabilities.

Summary

Overall risk level:

Medium

Risk ratings:

Critical:	0
High:	0
Medium:	1
Low:	4
Info:	34

Scan information:

Start time:	Oct 29, 2025 / 15:04:44 UTC+0530
Finish time:	Oct 29, 2025 / 15:05:05 UTC+0530
Scan duration:	21 sec
Tests performed:	39/39
Scan status:	Finished

Findings

Communication is not secure

CONFIRMED

port 80/tcp

URL	Response URL	Evidence
http://www.itsecgames.com/	http://www.itsecgames.com/	Communication is made over unsecure, unencrypted HTTP.

Details

Risk description:

The risk is that an attacker who manages to intercept the communication at the network level can read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

Recommendation:
We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

Classification:
CWE : CWE-311
OWASP Top 10 - 2017 : A3 - Sensitive Data Exposure
OWASP Top 10 - 2021 : A4 - Insecure Design

Missing security header: Referrer-Policy

CONFIRMED

port 80/tcp

URL	Evidence
http://www.itsecgames.com/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response. Request / Response

Details

Risk description:
The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

References:
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: Content-Security-Policy

CONFIRMED

port 80/tcp

URL	Evidence
http://www.itsecgames.com/	Response does not include the HTTP Content-Security-Policy security header or meta tag Request / Response

Details

Risk description:
The risk is that if the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

References:
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: X-Content-Type-Options

CONFIRMED

port 80/tcp

URL	Evidence
http://www.itsecgames.com/	Response headers do not include the X-Content-Type-Options HTTP security header Request / Response

Details

Risk description:
The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

Recommendation:
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Server software and technology found

UNCONFIRMED

port 80/tcp

Software / Version	Category

Google Font API	Font scripts
Apache HTTP Server	Web servers

Details

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Security.txt file is missing

CONFIRMED

port 80/tcp

URL
Missing: http://www.itsecgames.com/.well-known/security.txt

Details

Risk description:
There is no particular risk in not having a security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:
https://securitytxt.org/

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

HTTP OPTIONS enabled

CONFIRMED

port 80/tcp

URL	Method	Summary
http://www.itsecgames.com/	OPTIONS	We did a HTTP OPTIONS request. The server responded with a 200 status code and the header: `Allow: POST,OPTIONS,GET,HEAD` Request / Response

Details

Risk description:

The only risk this might present nowadays is revealing debug HTTP methods that can be used on the server. This can present a danger if any of those methods can lead to sensitive information, like authentication information, secret keys.

Recommendation:

We recommend that you check for unused HTTP methods or even better, disable the OPTIONS method. This can be done using your webserver configuration.

References:

https://techcommunity.microsoft.com/t5/iis-support-blog/http-options-and-default-page-vulnerabilities/ba-p/1504845
https://docs.nginx.com/nginx-management-suite/acm/how-to/policies/allowed-http-methods/

Classification:

CWE : CWE-16
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Website is accessible.

Nothing was found for vulnerabilities of server-side software.

Nothing was found for client access policies.

Nothing was found for robots.txt file.

Nothing was found for use of untrusted certificates.

Nothing was found for enabled HTTP debug methods.

- ✔ Scanned for secure communication
- ✔ Scanned for missing HTTP header - X-Content-Type-Options
- ✔ Scanned for website technologies
- ✔ Scanned for version-based vulnerabilities of server-side software
- ✔ Scanned for client access policies
- ✔ Scanned for robots.txt file
- ✔ Scanned for absence of the security.txt file
- ✔ Scanned for use of untrusted certificates
- ✔ Scanned for enabled HTTP debug methods
- ✔ Scanned for enabled HTTP OPTIONS method
- ✔ Scanned for directory listing
- ✔ Scanned for passwords submitted unencrypted
- ✔ Scanned for error messages
- ✔ Scanned for debug messages
- ✔ Scanned for code comments
- ✔ Scanned for missing HTTP header - Strict-Transport-Security
- ✔ Scanned for passwords submitted in URLs
- ✔ Scanned for domain too loose set for cookies
- ✔ Scanned for mixed content between HTTP and HTTPS
- ✔ Scanned for cross domain file inclusion
- ✔ Scanned for internal error code
- ✔ Scanned for HttpOnly flag of cookie
- ✔ Scanned for Secure flag of cookie
- ✔ Scanned for login interfaces
- ✔ Scanned for secure password submission
- ✔ Scanned for sensitive data
- ✔ Scanned for unsafe HTTP header Content Security Policy
- ✔ Scanned for OpenAPI files
- ✔ Scanned for file upload
- ✔ Scanned for SQL statement in request parameter
- ✔ Scanned for password returned in later response
- ✔ Scanned for Path Disclosure
- ✔ Scanned for Session Token in URL
- ✔ Scanned for API endpoints
- ✔ Scanned for emails
- ✔ Scanned for missing HTTP header - Rate Limit

Scan parameters

target:	http://www.itsecgames.com/
scan_type:	Light
authentication:	False

Scan stats

Unique Injection Points Detected:	6
URLs spidered:	18
Total number of HTTP requests:	32
Average time until a response was received:	47ms