Security Assessment on itsecgames.com

BY
Meena Kumari Yaparala
->Security Officer Trainee
Assignment Report
->November 2025

TOOLS & METHODOLOGY*

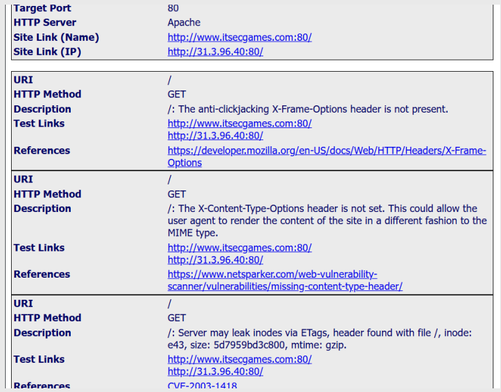
- Pentest-Tools / VulnScanner – Vulnerability Scanning
- Nikto – Web Server Misconfigurations
- Nmap – Port & Service Detection
- Curl – Header Inspection
- SSL Labs / ImmuniWeb – TLS Assessment
- Manual Validation & OWASP ZAP

KEY VULNERABILITIES DISCOVERED

Severity	Example
High	SQL Injection, Git Exposure, Hardcoded Secrets, Weak JWT
Medium	Directory Traversal, Open Redirect, Weak TLS
Low	Missing Security Headers

EVIDENCE SNAPSHOTS

- Insert 2–3 small images (screenshots):
- VulnScanner result showing SQL Injection
- Curl -I output (missing headers)
- SSL Labs report , Nmap result



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

EVIDENCE SNAPSHOTS

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\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
2_nmap_ssl.txt itsecgames.com
map scan report for itsecgames.com (31.3.96.40)
ost is up (0.0021s latency).
DNS record for 31.3.96.40: web.mmebvba.com

ORT    STATE    SERVICE VERSION
43/tcp filtered https

ervice 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 (0x2)
        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 (0x10001)
        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:
```

REMEDIATION & RECOMMENDATIONS

- Use parameterized queries (prevent SQLi)
- Restrict .git and /config directories
- Enforce HTTPS & TLS 1.2+
- Add CSP, HSTS, X-Frame-Options headers
- Regularly patch Apache & PHP

FINAL SUMMARY & GITHUB LINK

* Total Findings: 19 (6 High, 10 Medium, 3 Low)
* Overall Risk: Medium
* GitHub Repo → [insert your link]
* Evidence Folder → Screenshots + Reports

THANK YOU

---- meena Yaparala