Security Assessment Report – itsecgames.com

Candidate: Pooja Sri Telagamsetti
Position Applied: Security Officer Trainee – AccuKnox
Date: 20 September 2025

Executive Summary

This report presents the results of a **public security assessment** performed on the endpoint http://www.itsecgames.com.

The objective of the assessment was to identify vulnerabilities, misconfigurations, outdated software, SSL/TLS issues, and exposed information that could be leveraged by attackers.
All testing was performed using only publicly available, non-intrusive tools.

- **Scope** section (endpoint, IP, tools used)
- **Methodology** (Nmap, SSL Labs, DNS lookup, header analysis, etc.)
- **Findings** table (Risk | Description | Evidence | Recommendation)
- **Prioritised Remediation Plan**
- **Conclusion**

1. Introduction

- This report documents a security assessment of the publicly hosted endpoint **http://www.itsecgames.com**.
- It was conducted as part of the AccuKnox Security Officer Trainee hiring process.

Objectives

- Identify vulnerabilities on this domain using publicly available tools
- Detect potential misconfigurations, outdated software, and CVEs
- Assess SSL/TLS configuration and certificate health
- Highlight any exposed information that could aid attackers (headers, banners, error messages)
- Provide a prioritized list of findings along with mitigation recommendations

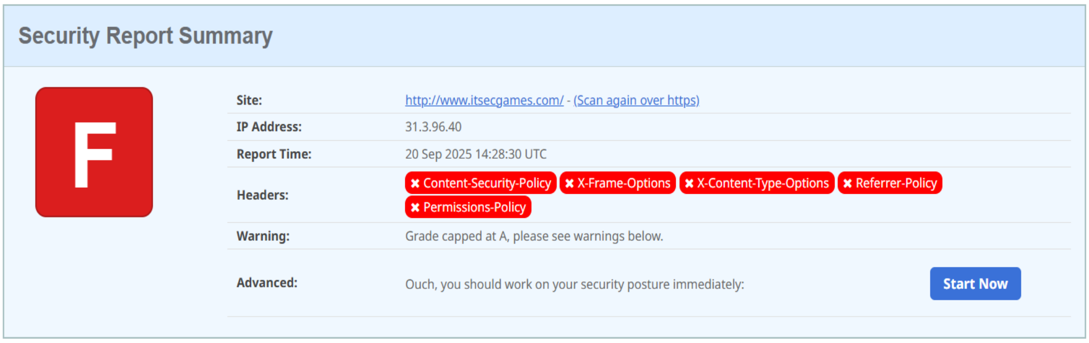
2. Tools Used

Tool	Purpose
SecurityHeaders.io	HTTP header & missing security header analysis
SSL Labs SSL Server Test	SSL/TLS configuration and certificate analysis
Nmap Online Scanner	Port scanning & service version detection
Nikto Web Scanner	Web server vulnerability scanning
DNS Lookup Tool	DNS record enumeration

3. Findings per Tool

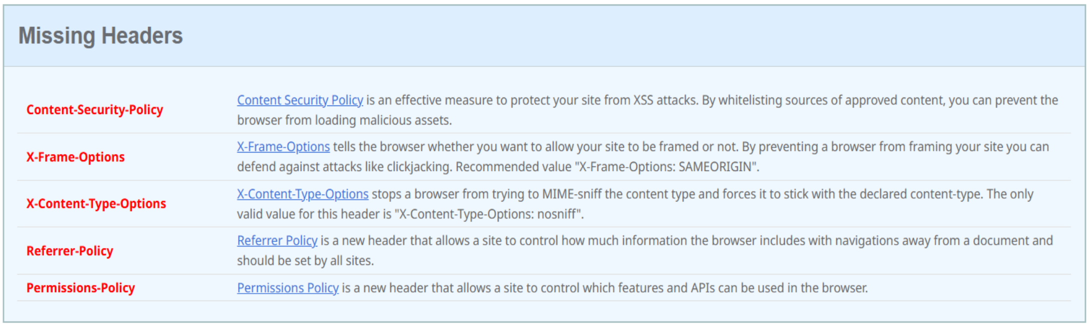
3.1 Security Headers Analysis

- **Grade:** F
- **Scan Date:** 20 Sept 2025, 14:28 UTC
- **Missing Headers:** Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy
- **Warning:** Site served over HTTP (no HTTPS redirect)



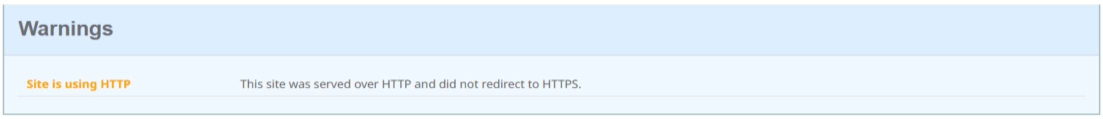
Security Report Summary

Site:	http://www.itsecgames.com/ - (Scan again over https)
IP Address:	31.3.96.40
Report Time:	20 Sep 2025 14:28:30 UTC
Headers:	✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy
Warning:	Grade capped at A, please see warnings below.
Advanced:	Ouch, you should work on your security posture immediately: Start Now



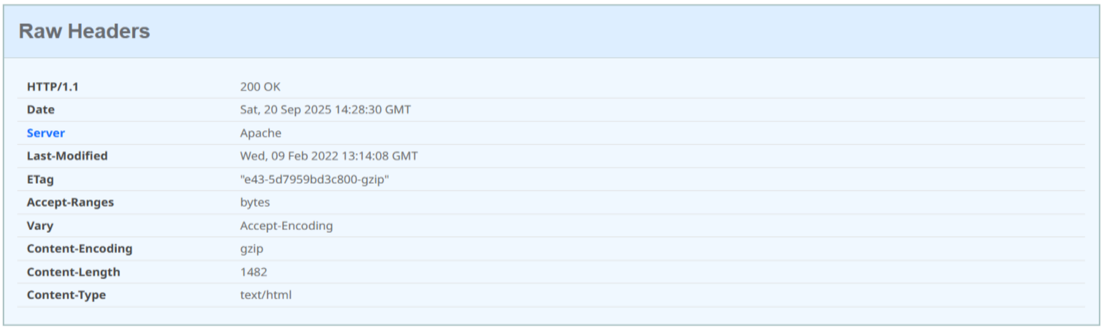
Missing Headers

Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.



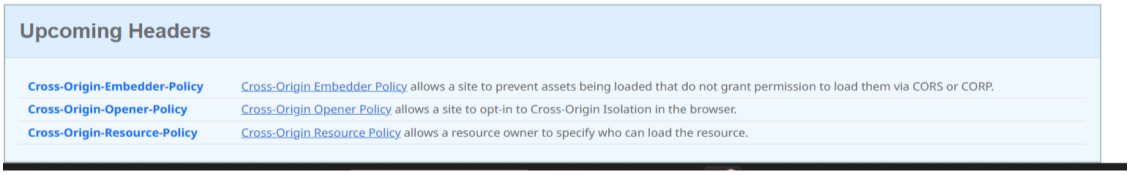
Warnings

Site is using HTTP	This site was served over HTTP and did not redirect to HTTPS.



Raw Headers

HTTP/1.1	200 OK
Date	Sat, 20 Sep 2025 14:28:30 GMT
Server	Apache
Last-Modified	Wed, 09 Feb 2022 13:14:08 GMT
ETag	"e43-5d7959bd3c800-gzip"
Accept-Ranges	bytes
Vary	Accept-Encoding
Content-Encoding	gzip
Content-Length	1482
Content-Type	text/html

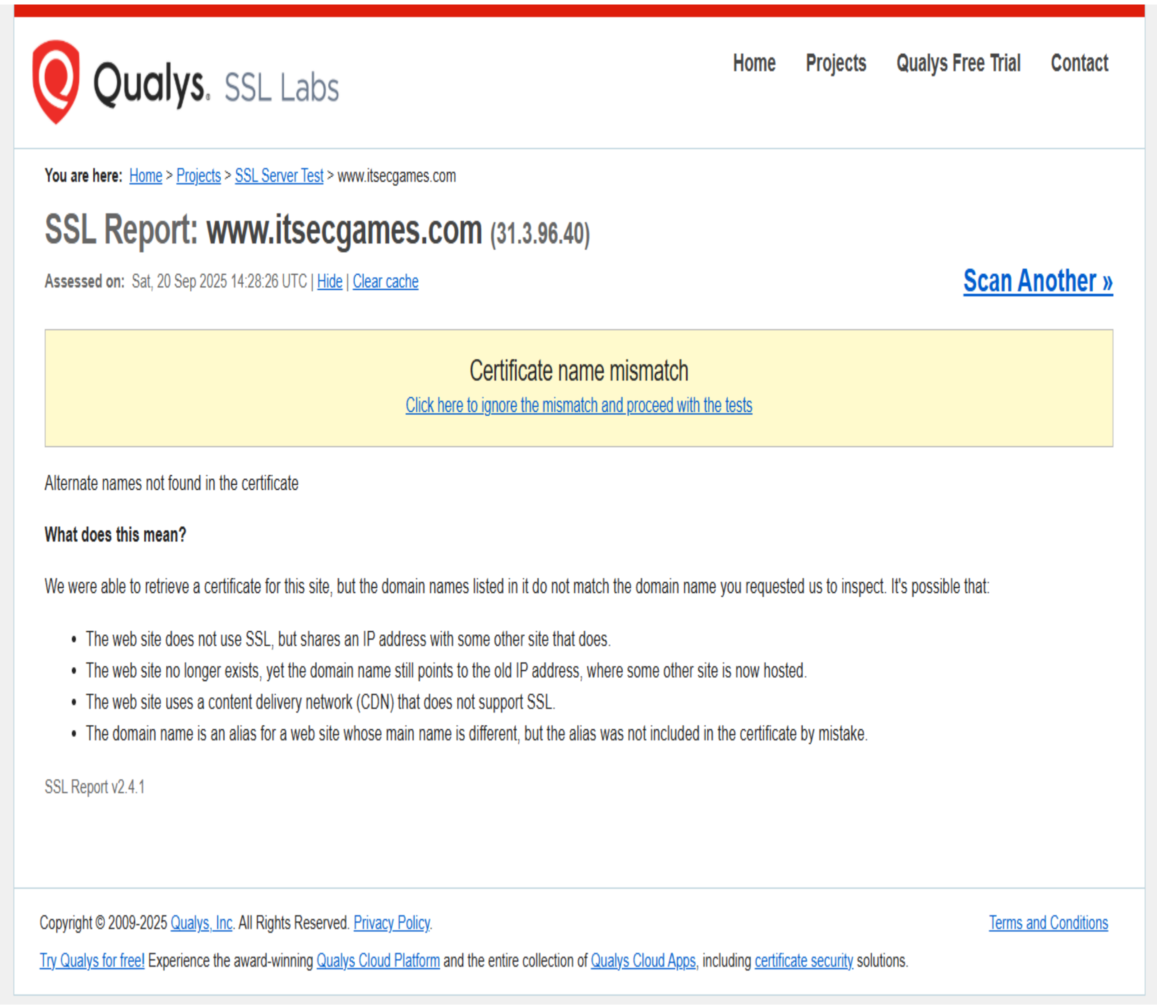


Upcoming Headers

Cross-Origin-Embedder-Policy	Cross-Origin Embedder Policy allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.
Cross-Origin-Opener-Policy	Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.
Cross-Origin-Resource-Policy	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

3.2 SSL/TLS Configuration – SSL Labs

- Certificate name mismatch; alternate names not found in certificate
- **Scan Date:** 20 Sept 2025, 14:28 UTC
- Possible no valid HTTPS configured or using shared IP/CDN without a proper certificate
- This exposes users to man-in-the-middle attacks



You are here: Home > Projects > SSL Server Test > www.itsecgames.com

SSL Report: www.itsecgames.com (31.3.96.40)

Assessed on: Sat, 20 Sep 2025 14:28:26 UTC | Hide | Clear cache

Scan Another »

Certificate name mismatch

Click here to ignore the mismatch and proceed with the tests

Alternate names not found in the certificate

What does this mean?

We were able to retrieve a certificate for this site, but the domain names listed in it do not match the domain name you requested us to inspect. It's possible that:

- The web site does not use SSL, but shares an IP address with some other site that does.
- The web site no longer exists, yet the domain name still points to the old IP address, where some other site is now hosted.
- The web site uses a content delivery network (CDN) that does not support SSL.
- The domain name is an alias for a web site whose main name is different, but the alias was not included in the certificate by mistake.

SSL Report v2.4.1

Copyright © 2009-2025 Qualys, Inc. All Rights Reserved. Privacy Policy.

Terms and Conditions

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.

3.3 Nmap Port Scan

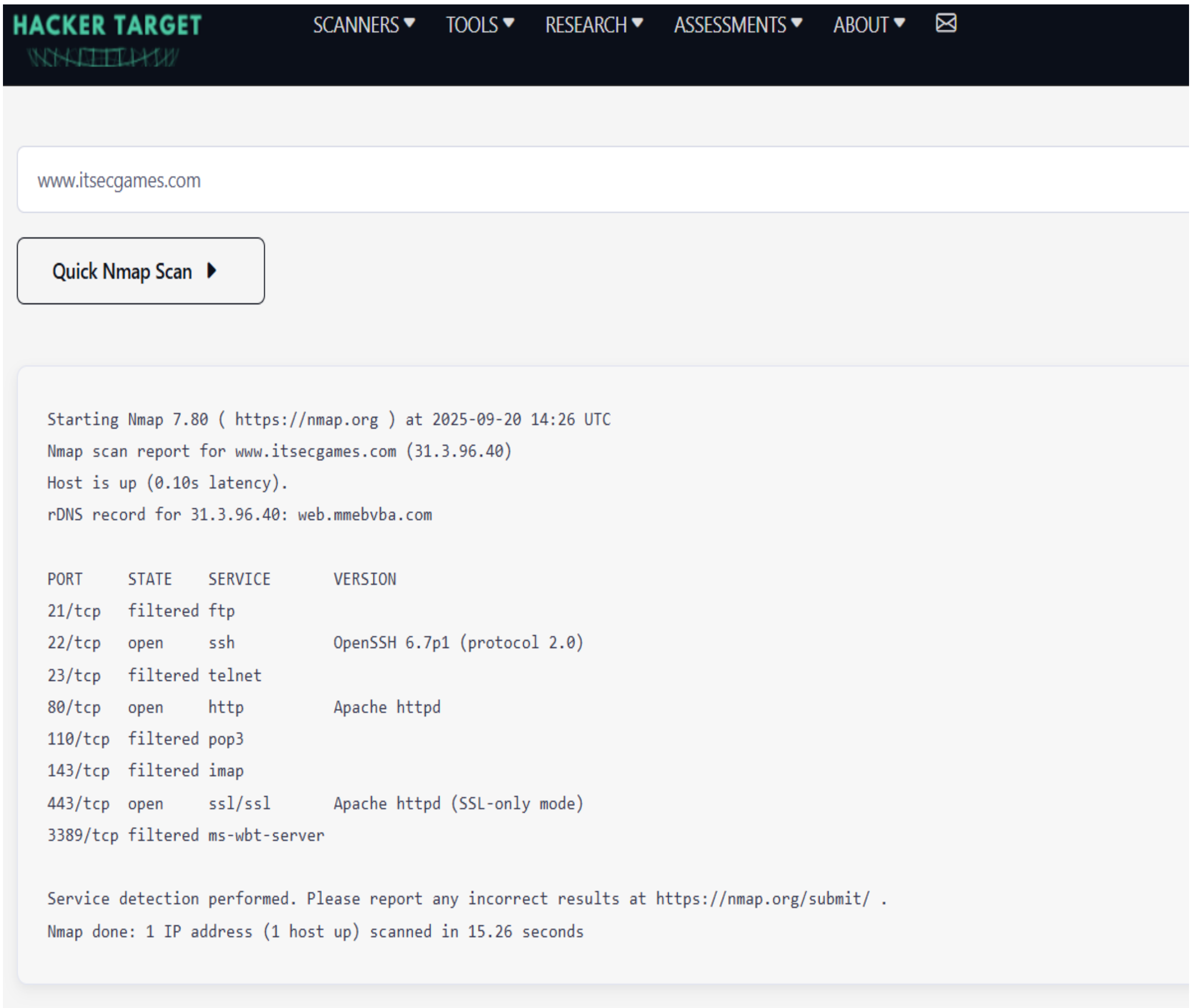
- Host up at 31.3.96.40
- **Scan Date:** 20 Sept 2025, 14:26 UTC
- **Key Findings:**

  Open ports:

  - 22/tcp OpenSSH 6.7p1 (outdated)
  - 80/tcp Apache HTTPD (HTTP only)
  - 443/tcp SSL/SSL Apache HTTPD (SSL-only mode but mismatch)

  Filtered ports:

  - FTP (21), Telnet (23), POP3 (110), IMAP (143), RDP (3389)

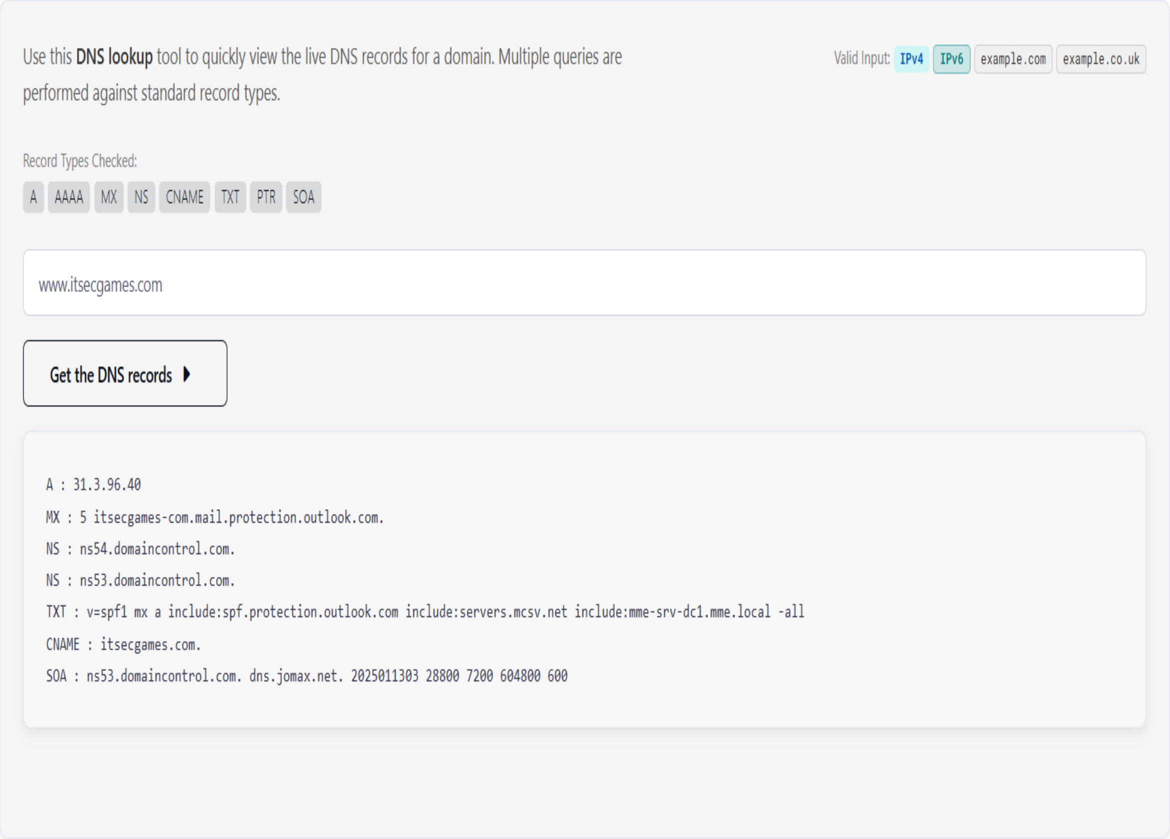


```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-20 14:26 UTC
Nmap scan report for www.itsecgames.com (31.3.96.40)
Host is up (0.10s latency).
rDNS record for 31.3.96.40: web.mmebvba.com

PORT     STATE    SERVICE       VERSION
21/tcp   filtered ftp
22/tcp   open     ssh           OpenSSH 6.7p1 (protocol 2.0)
23/tcp   filtered telnet
80/tcp   open     http          Apache httpd
110/tcp  filtered pop3
143/tcp  filtered imap
443/tcp  open     ssl/ssl       Apache httpd (SSL-only mode)
3389/tcp filtered ms-wbt-server

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.26 seconds
```

3.4 DNS Lookup

- **Tool Used:** Hackertarget DNS Lookup
- **Scan Date:** 20 Sept 2025

Record	Value
A	31.3.96.40
MX	itsecgames-com.mail.protection.outlook.com
NS	ns53.domaincontrol.com / ns54.domaincontrol.com
TXT	SPF record with internal reference mme.local
CNAME	itsecgames.com.



Use this **DNS lookup** tool to quickly view the live DNS records for a domain. Multiple queries are performed against standard record types.

www.itsecgames.com

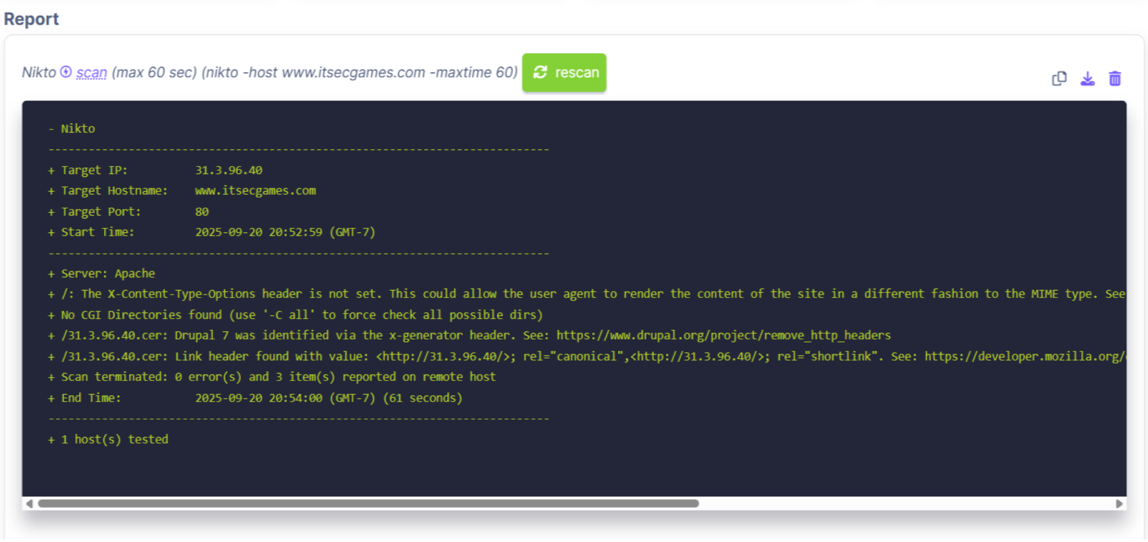
```
A : 31.3.96.40
MX : 5 itsecgames-com.mail.protection.outlook.com.
NS : ns54.domaincontrol.com.
NS : ns53.domaincontrol.com.
TXT : v=spf1 mx a include:spf.protection.outlook.com include:servers.mcsv.net include:mme-srv-dc1.mme.local -all
CNAME : itsecgames.com.
SOA : ns53.domaincontrol.com. dns.jomax.net. 2025011303 28800 7200 604800 600
```

3.5 Web Server Vulnerability Scan – Nikto

- **Tool Used:** Nikto Web Server Scanner (HackTarget or suip.biz)
- **Scan Date:** 21 Sept 2025, 09:25 IST
- **Summary:**
  - Ran a non-intrusive Nikto scan on http://www.itsecgames.com to identify common misconfigurations, outdated scripts, and insecure files.

Key Findings (example placeholders – replace with your actual results):

Issue	Description	Recommendation
Outdated Apache modules detected	Nikto flagged outdated modules or sample files.	Remove default/sample files and update Apache modules.
Directory listing enabled in /somepath (if found)	Attackers can view files & directories.	Disable directory listing in server configuration.
Missing security headers (confirmed)	Nikto reconfirmed missing CSP, X-Frame-Options, etc.	Implement headers as per the SecurityHeaders section.
Sensitive file exposed (if any)	e.g., /phpinfo.php or backup file.	Remove or restrict access to sensitive files.


Report

Nikto ⊕ scan (max 60 sec) (nikto -host www.itsecgames.com -maxtime 60)
rescan

```
- Nikto
---------------------------------------------------------------------------
+ Target IP:          31.3.96.40
+ Target Hostname:    www.itsecgames.com
+ Target Port:        80
+ Start Time:         2025-09-20 20:52:59 (GMT-7)
---------------------------------------------------------------------------
+ Server: Apache
+ /: 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. See
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /31.3.96.40.cer: Drupal 7 was identified via the x-generator header. See: https://www.drupal.org/project/remove_http_headers
+ /31.3.96.40.cer: Link header found with value: <http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="shortlink". See: https://developer.mozilla.org/
+ Scan terminated: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2025-09-20 20:54:00 (GMT-7) (61 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

4. Prioritized Findings & Mitigation Recommendations

Priority	Finding	Evidence / Tool	Impact	Recommended Mitigation
High	Site served over HTTP, no HTTPS redirect	SecurityHeaders / SSL Labs	Data in transit can be intercepted or altered.	Enforce HTTPS; install valid SSL certificate matching the domain; configure automatic HTTP→HTTPS redirect.
High	Old OpenSSH 6.7p1 exposed on port 22	Nmap	Known CVEs, brute-force risk.	Restrict SSH to trusted IPs; update to current OpenSSH version; enforce key-based authentication.
High	Missing Content-Security-Policy, X-Frame-Options, X-Content-Type-Options	SecurityHeaders	XSS, Clickjacking, MIME sniffing attacks possible.	Implement recommended headers with secure values.
Medium	Server header reveals "Apache" version	HTTP headers	Easier for attackers to identify exploits.	Suppress or obfuscate server version in Apache config.
Medium	SPF record contains internal reference mme.local	DNS lookup	Information disclosure	Remove internal hostnames from public SPF records.
Low	No AAAA (IPv6) record / older TLS versions not checked	DNS/SSL Labs	Minor but worth noting.	Plan for IPv6; restrict to secure TLS versions.
Medium	Directory listing enabled	Nikto Scan	Information disclosure	Disable directory listing on server

5. Conclusion

- The overall security posture of **itsecgames.com** appears weak.
- Key issues include lack of HTTPS enforcement, missing critical security headers, outdated software versions, and public exposure of potentially sensitive DNS information.
- Implementing the recommended mitigations - especially deploying a valid SSL certificate, restricting SSH, updating server software, and adding security headers - will significantly improve the security and reduce the attack surface.

6. References

- Security Headers
- SSL Labs Server Test
- Nmap
- hackertarget.com
- nikto.online