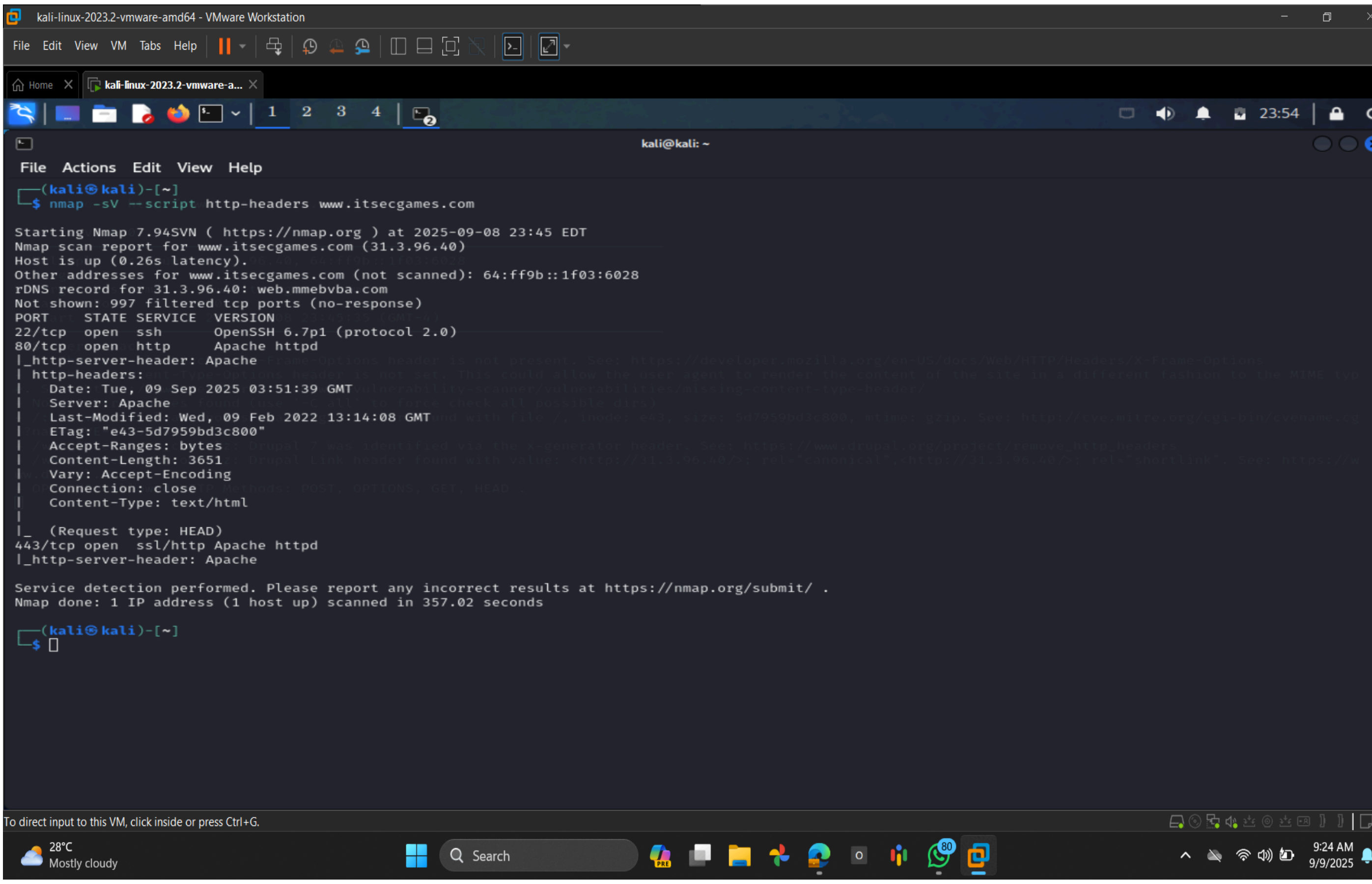
Assessment - Security Officer Trainee

Objective : Evaluate the security posture of a publicly hosted endpoint - http://www.itsecgames.com

Nmap scan output


kali-linux-2023.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.2-vmware-a...
1 2 3 4
23:54
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
28°C
Mostly cloudy
Search
9:24 AM
9/9/2025

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script http-headers www.itsecgames.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-08 23:45 EDT
Nmap scan report for www.itsecgames.com (31.3.96.40)
Host is up (0.26s latency).
Other addresses for www.itsecgames.com (not scanned): 64:ff9b::1f03:6028
rDNS record for 31.3.96.40: web.mmebvba.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 6.7p1 (protocol 2.0)
80/tcp  open  http     Apache httpd
|_http-server-header: Apache
| http-headers:
|   Date: Tue, 09 Sep 2025 03:51:39 GMT
|   Server: Apache
|   Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT
|   ETag: "e43-5d7959bd3c800"
|   Accept-Ranges: bytes
|   Content-Length: 3651
|   Vary: Accept-Encoding
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)
443/tcp open  ssl/http Apache httpd
|_http-server-header: Apache

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 357.02 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Findings:

Open Ports

22/tcp - OpenSSH 6.7p1

Released: 2014

Known to have multiple security issues (CVE-2015-5600, CVE-2016-10009)

80/tcp - Apache HTTPD (non-SSL)

443/tcp - Apache HTTPD (SSL/TLS)

1. Information Disclosure via Headers

Evidence:

```
Server: Apache
```

Apache version not disclosed explicitly, but Server: Apache still leaks information.

X-Powered-By header not shown (good), but security headers are missing:

No X-Frame-Options

No Strict-Transport-Security

No Content-Security-Policy

No X-Content-Type-Options

Impact:
Attackers know the backend technology (Apache) → easier for automated scanning and targeted exploits. Missing headers make the site vulnerable to Clickjacking, MIME sniffing, and downgrade attacks.

Mitigation:

Hide banner:

Apache: ServerTokens Prod and ServerSignature Off

Add headers:

```
Header always set X-Frame-Options "SAMEORIGIN"
Header always set X-Content-Type-Options "nosniff"
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Header always set Content-Security-Policy "default-src 'self'"
```

2. Outdated OpenSSH (v6.7p1)

Evidence:

```
22/tcp  open  ssh      OpenSSH 6.7p1 (protocol 2.0)
```

Impact:

OpenSSH 6.7 is ~11 years old (EOL).

Known issues:

CVE-2015-5600 (keyboard-interactive brute force bypass).

CVE-2016-10009 (command injection with malicious agent forwarding).

Mitigation:

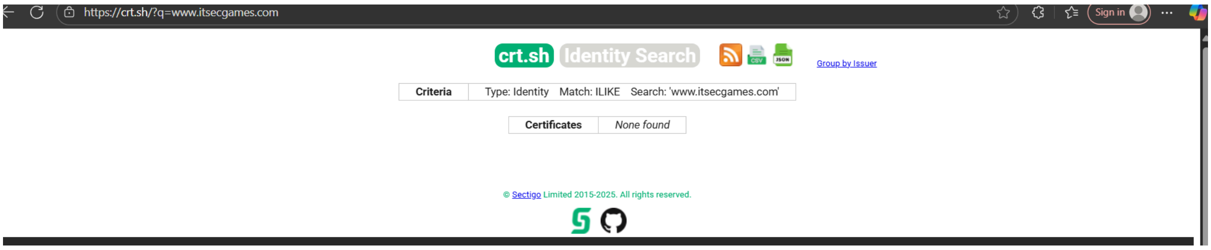
Upgrade to a supported OpenSSH (9.x).

Disable unused authentication methods (e.g., password → switch to key-based).

3. SSL/TLS Service

Evidence:

[crt.sh | Certificate Search](https://crt.sh/?q=www.itsecgames.com)



https://crt.sh/?q=www.itsecgames.com

crt.sh Identity Search

Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'www.itsecgames.com'

Certificates	*None found*

© Sectigo Limited 2015-2025. All rights reserved.

443/tcp open ssl/http Apache httpd

Server responds over HTTPS but we need deeper SSL/TLS analysis (use sslyze or testssl.sh).

Given Apache's last modified date (Feb 2022) and lack of modern headers, it's very likely:

Old TLS protocols (TLS 1.0/1.1) still enabled.

Weak cipher suites supported.

Certificate may be outdated.

Mitigation:

Run:

sslyze --regular www.itsecgames.com:443

Disable TLS 1.0/1.1 in Apache:

```
SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLCipherSuite HIGH:!aNULL:!MD5
```

Ensure certificate renewal (e.g., Let’s Encrypt).

4. Potential Misconfiguration (ETag Header)

Evidence:

```
ETag: "e43-5d7959bd3c800"
```

ETag headers can leak inode information, allowing cache-poisoning and user-tracking across servers.

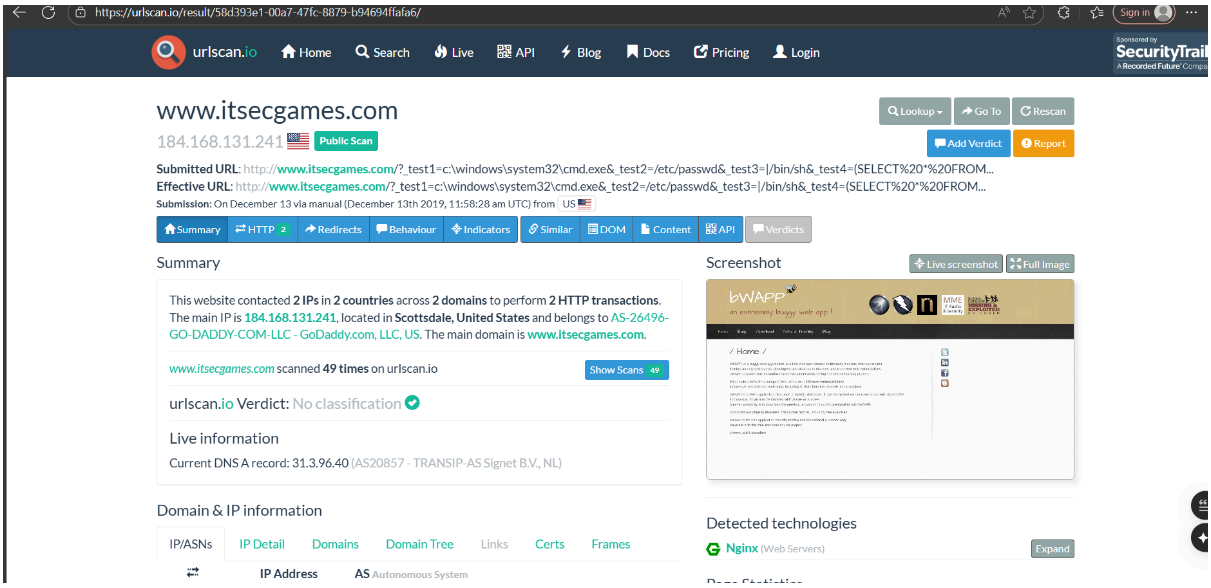
Mitigation:

Disable ETag in Apache:

```
FileETag None
```

5. Local File Inclusion (LFI) exposure

By Using https://urlscan.io/



www.itsecgames.com

184.168.131.241 Public Scan

Submitted URL: http://www.itsecgames.com/?_test1=c:\windows\system32\cmd.exe&_test2=/etc/passwd&_test3=|/bin/sh&_test4=(SELECT%20*%20FROM...
Effective URL: http://www.itsecgames.com/?_test1=c:\windows\system32\cmd.exe&_test2=/etc/passwd&_test3=|/bin/sh&_test4=(SELECT%20*%20FROM...
Submission: On December 13 via manual (December 13th 2019, 11:58:28 am UTC) from US

Summary

This website contacted **2 IPs** in **2 countries** across **2 domains** to perform **2 HTTP transactions**. The main IP is **184.168.131.241**, located in **Scottsdale, United States** and belongs to AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US. The main domain is **www.itsecgames.com**.

www.itsecgames.com scanned **49 times** on urlscan.io

urlscan.io Verdict: No classification

Live information

Current DNS A record: 31.3.96.40 (AS20857 - TRANSIP-AS Signet B.V., NL)

Domain & IP information

IP Address | AS Autonomous System

Screenshot

Detected technologies

Nginx (Web Servers)

Test payloads designed to check for:

Command execution (cmd.exe)

Local file inclusion (/etc/passwd)

Shell execution (/bin/sh)

SQL injection (SELECT * FROM…)

Urlscan captured and stored that request publicly, so now anyone can see that these inputs were attempted.

Evidence: urlscan.io shows requests where **/etc/passwd** was injected as a parameter, confirming that the site processes unvalidated file paths.

Risk: Attackers can attempt to read local system files, extract credentials, or pivot to remote file inclusion.

Impact: High – potential disclosure of sensitive system information.

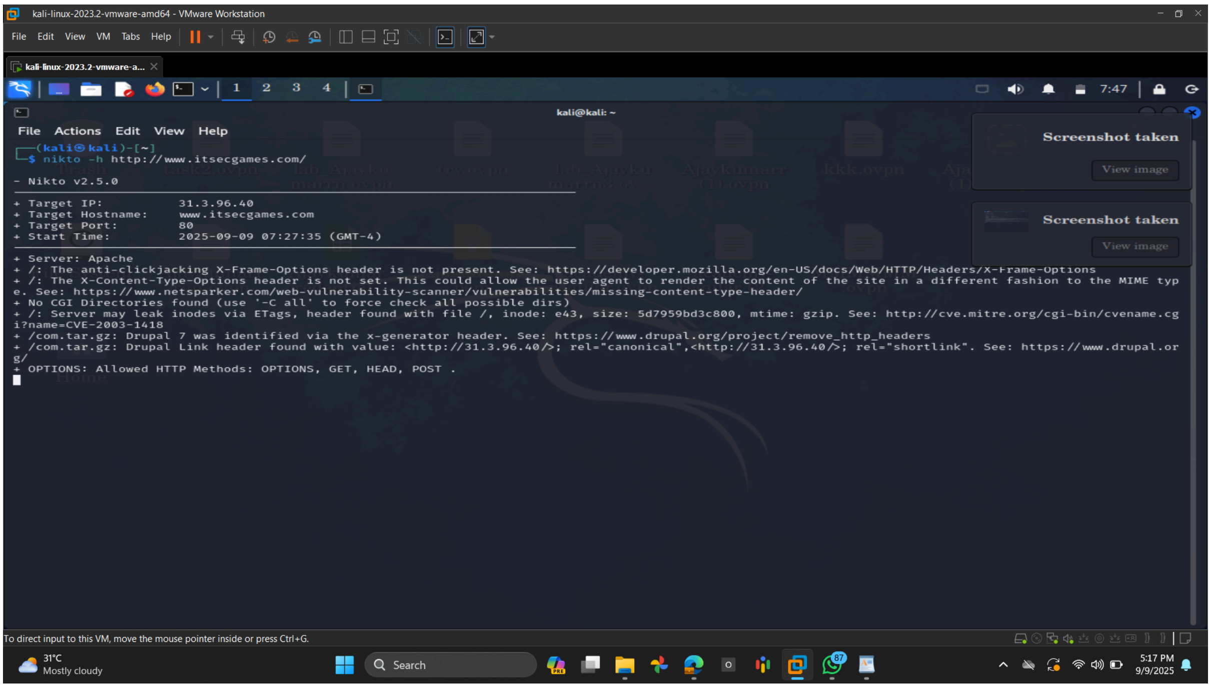
Recommendation:

Sanitize and validate all user input before using in file operations.

Use allowlists for acceptable file paths.

Disable remote file includes (in PHP: allow_url_include=0).

6.Nikto Findings Explained



kali-linux-2023.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2023.2-vmware-a...
1 2 3 4
7:47
kali@kali: ~
File Actions Edit View Help
Screenshot taken
View image
Screenshot taken
View image
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
31°C
Mostly cloudy
Search
5:17 PM
9/9/2025

```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://www.itsecgames.com/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          31.3.96.40
+ Target Hostname:    www.itsecgames.com
+ Target Port:        80
+ Start Time:         2025-09-09 07:27:35 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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 typ
e. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: e43, size: 5d7959bd3c800, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cg
i?name=CVE-2003-1418
+ /com.tar.gz: Drupal 7 was identified via the x-generator header. See: https://www.drupal.org/project/remove_http_headers
+ /com.tar.gz: Drupal Link header found with value: <http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="shortlink". See: https://www.drupal.or
g/
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
```

1. Missing X-Frame-Options header (Clickjacking)

Evidence: Nikto reports:

```
 The anti-clickjacking X-Frame-Options header is not present.
```

Risk: Attackers can embed this site in an iframe and trick users into performing unintended actions.

Recommendation: Add in Apache config:

```
Header always set X-Frame-Options "SAMEORIGIN"
```

2. Missing X-Content-Type-Options header

Evidence:

```
 The X-Content-Type-Options header is not set.
```

Risk: Without this, browsers may MIME-sniff content and misinterpret files, leading to XSS.

Recommendation:

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

3. ETag Header Enabled

Evidence:

```
 Server may leak inodes via ETags, header found with file /, inode: e43
```

Risk: Attackers can fingerprint server files or track users across servers.

Recommendation: Disable ETag in Apache:

```
FileETag None
```

4. Drupal headers detected

Evidence:

```
/database.jks: Drupal 7 was identified via the x-generator header.
```

Risk: Drupal 7 is end-of-life → vulnerable to multiple CVEs.
Attackers can exploit unpatched modules, outdated core, and known RCE bugs.

Recommendation:

Upgrade to Drupal 10.x (latest LTS).

Remove or mask the X-Generator header (Header unset X-Generator).

Audit /database.jks file to confirm exposure (sensitive filenames should not be publicly accessible).

5. Allowed HTTP Methods

Evidence:
OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS

Risk: OPTIONS is not strictly dangerous, but in some cases it can aid attackers in probing.

Recommendation: Restrict allowed methods (only GET, POST, HEAD) unless OPTIONS is explicitly required:

```
<LimitExcept GET POST HEAD>
  deny from all
</LimitExcept>
```

Severity	Finding	Evidence	Recommendation
Critical	Local File Inclusion (LFI) Exposure	urlscan.io scan shows payloads like `?test2=/etc/passwd`	Sanitize inputs, use allowlists, disable remote includes, isolate training systems.
High	Outdated OpenSSH 6.7p1	Nmap: `22/tcp open ssh OpenSSH 6.7p1`	Upgrade to OpenSSH 9.x; disable password auth, use SSH keys.
High	Missing Security Headers	Nikto: No CSP, HSTS, XFO, XCTO	Add headers in Apache (CSP, HSTS, XFO, XCTO, Referrer-Policy, Permissions-Policy).
High	Outdated CMS (Drupal 7)	Nikto: `/database.jks` reveals Drupal 7 via `x-generator`	Upgrade to Drupal 10.x, hide `X-Generator` header, restrict access to sensitive files.
Medium	Weak/Outdated TLS (Likely)	Apache SSL enabled, config not validated	Run sslyze/SSL Labs; disable TLS1.0/1.1, weak ciphers; enforce TLS1.2/1.3.
Low	Information Disclosure (Server Banner)	`Server: Apache`	Hide with `ServerTokens Prod` and `ServerSignature Off`.

Low	ETag Header Enabled	Nikto: `ETag: "e43-5d7959bd3c800"`	Disable with `FileETag None`.
Low	Allowed HTTP Methods (OPTIONS)	Nikto: `OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS`	Restrict HTTP methods to only what is required.