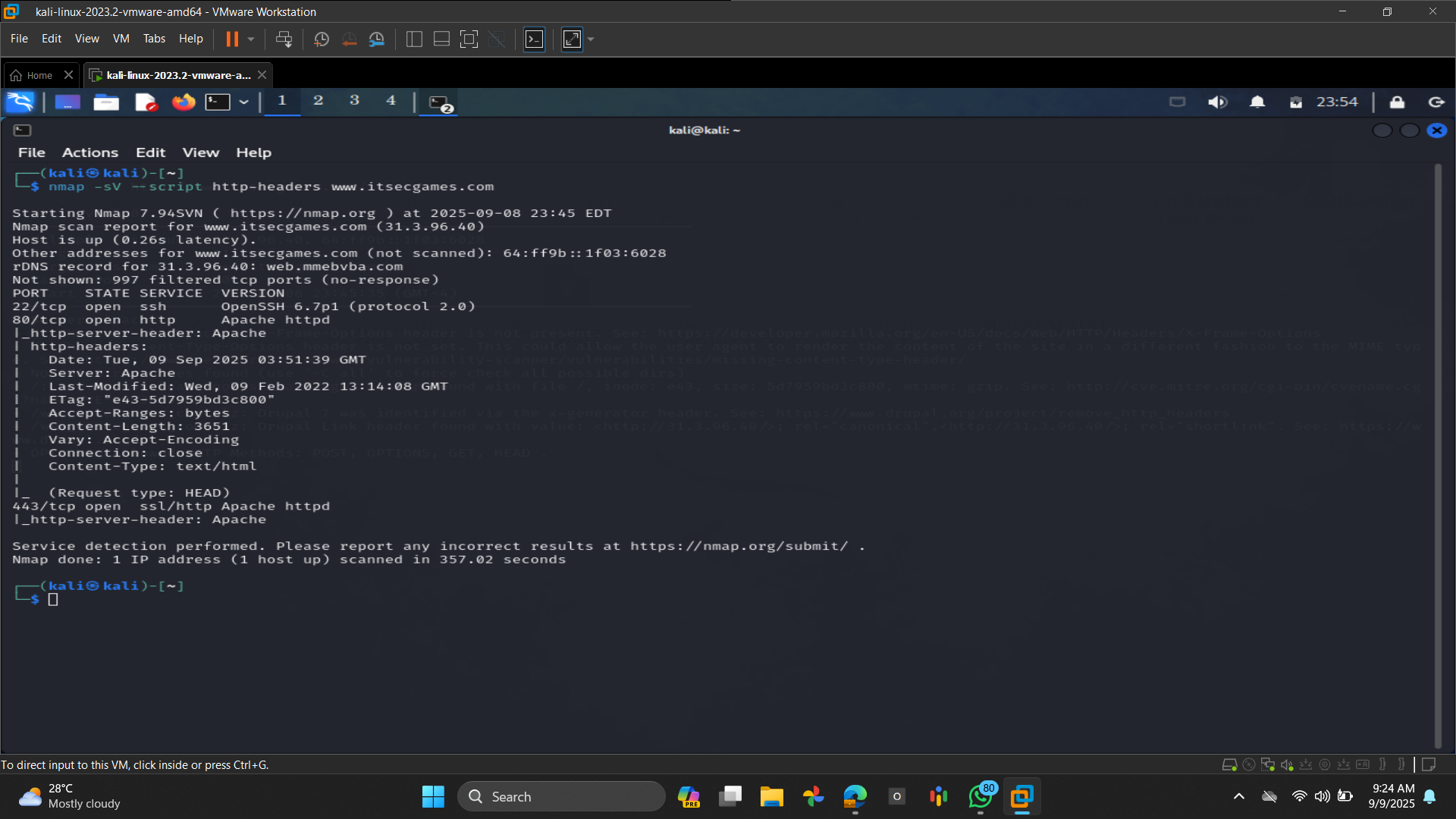
**Assessment - Security Officer Trainee**

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

**Nmap scan output**

****

**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 Outdated OpenSSH (v6.7p1)**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).

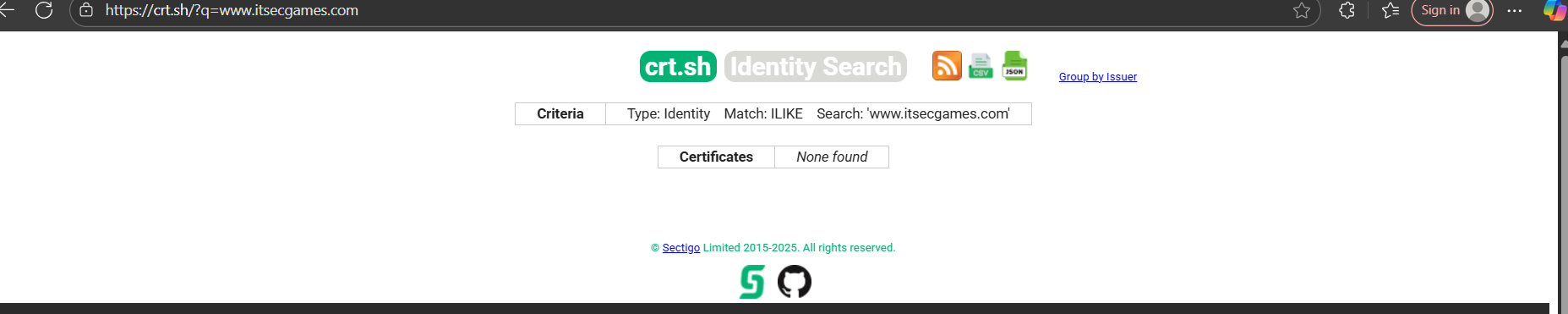
Mitigation:

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/)



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Certificate may be outdated.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"

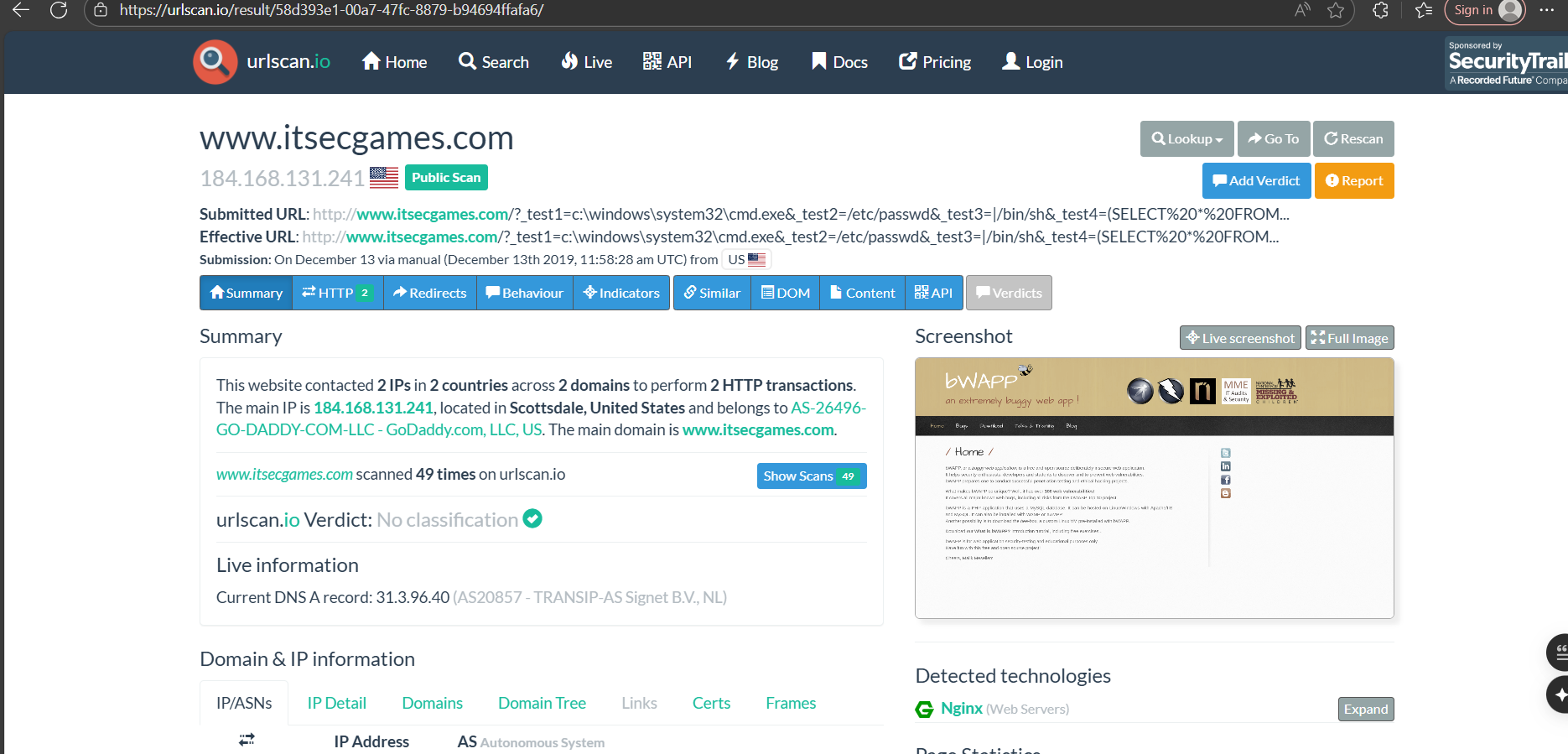
ETag headers can leak inode information, allowing cache-poisoning and user-tracking across servers.

Mitigation:

Disable ETag in Apache:

FileETag None  
  
**5. Local File Inclusion (LFI) exposure**

By Using <https://urlscan.io/>



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).

| **Severity** | **Finding** | **Evidence** | **Recommendation** |
| --- | --- | --- | --- |
| **Critical** | Local File Inclusion (LFI) Exposure | urlscan.io scan shows payloads such as ?test2=/etc/passwd, ?test3=/bin/sh, confirming unsanitized input parameters | Validate and sanitize user input, use allowlists for file paths, disable remote file includes, isolate vulnerable apps (training systems) from production. |
| **High** | Outdated OpenSSH 6.7p1 | 22/tcp open ssh OpenSSH 6.7p1 | Upgrade to **OpenSSH 9.x** or latest stable; disable password authentication, use key-based login. |
| **High** | Missing Security Headers | No **CSP**, **HSTS**, **X-Frame-Options**, **X-Content-Type-Options** in HTTP response | Configure headers in Apache/Nginx (e.g., CSP, HSTS, XFO, XCTO, Referrer-Policy, Permissions-Policy). |
| **Medium** | Weak/Outdated TLS (Likely) | Apache SSL enabled, version/config not validated | Run **sslyze** or **SSL Labs** scan; disable TLS 1.0/1.1, weak ciphers; enable TLS 1.2/1.3 only; renew certificates if expired. |
| **Low** | Information Disclosure (Server Banner) | Response header shows Server: Apache | Hide server version with ServerTokens Prod and ServerSignature Off; use reverse proxy to mask headers. |
| **Low** | ETag Header Enabled | Response includes ETag: "e43-5d7959bd3c800" | Disable ETag in Apache (FileETag None) to prevent file fingerprinting/cache-related disclosure. |