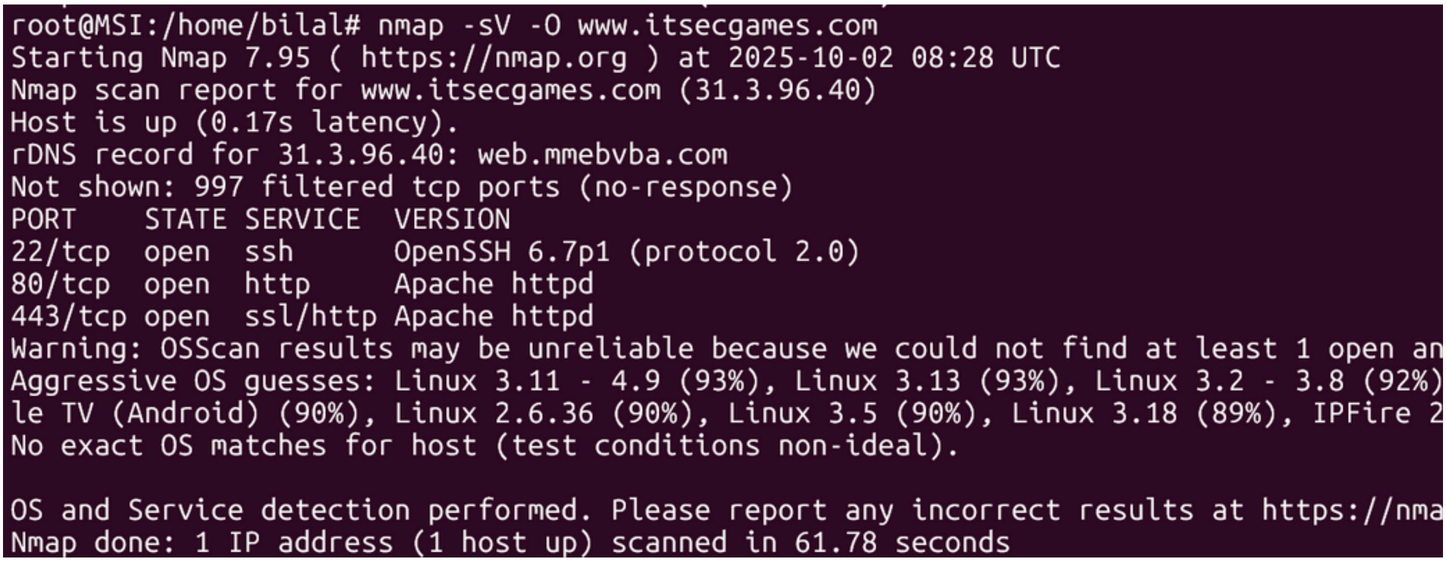
Penetration Test Report

Target: http://www.itsecgames.com/
Scope: External web & network reconnaissance (non-intrusive scanning)
Date: 2025-10-02

By Mohammed k

Finding 01 — Outdated SSH Service (OpenSSH 6.7p1)

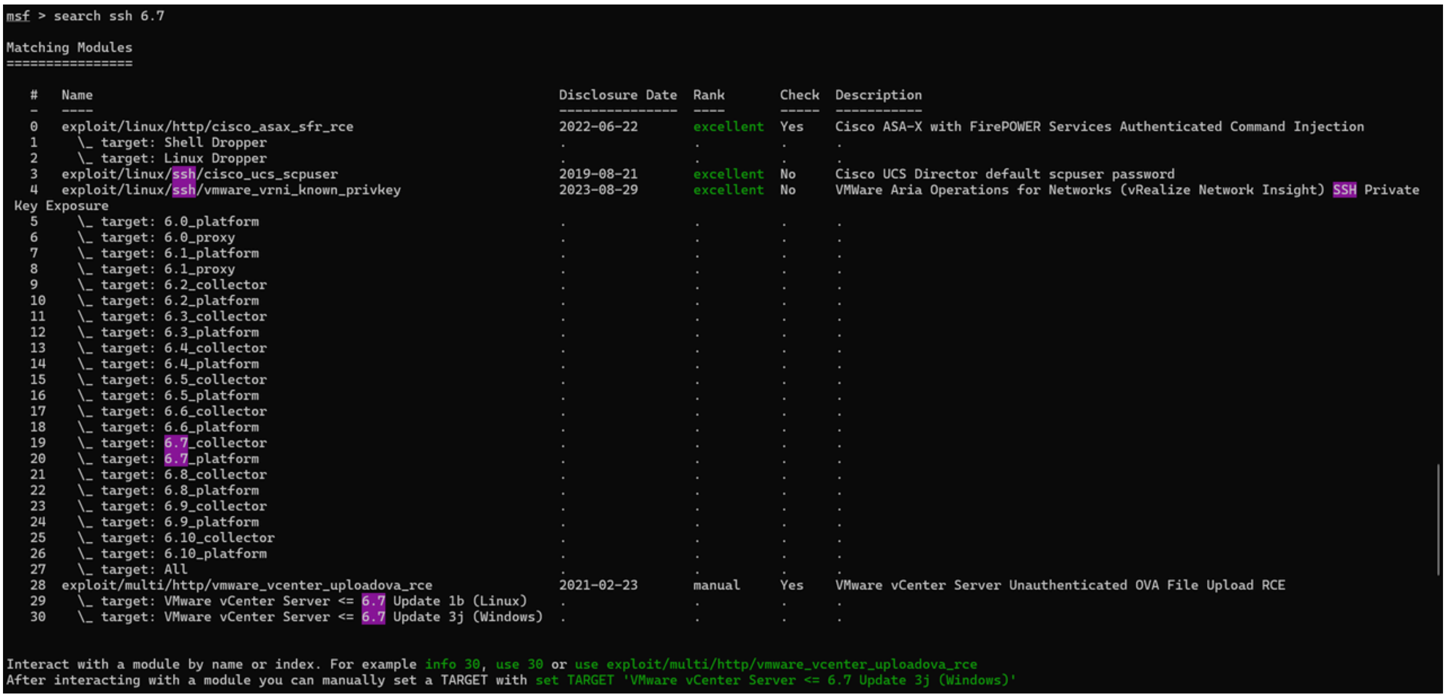
Severity: Medium → High (depends on how exposed the service is)
Affected Service: SSH (TCP/22)
Evidence: Nmap scan showed the server is running OpenSSH 6.7p1.



```
root@MSI:/home/bilal# nmap -sV -O www.itsecgames.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-02 08:28 UTC
Nmap scan report for www.itsecgames.com (31.3.96.40)
Host is up (0.17s latency).
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
443/tcp open  ssl/http Apache httpd
Warning: OSScan results may be unreliable because we could not find at least 1 open an
Aggressive OS guesses: Linux 3.11 - 4.9 (93%), Linux 3.13 (93%), Linux 3.2 - 3.8 (92%)
le TV (Android) (90%), Linux 2.6.36 (90%), Linux 3.5 (90%), Linux 3.18 (89%), IPFire 2
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nma
Nmap done: 1 IP address (1 host up) scanned in 61.78 seconds
```

Why this is a problem:
This version of OpenSSH is old and has several known security issues. Some of them allow attackers to:

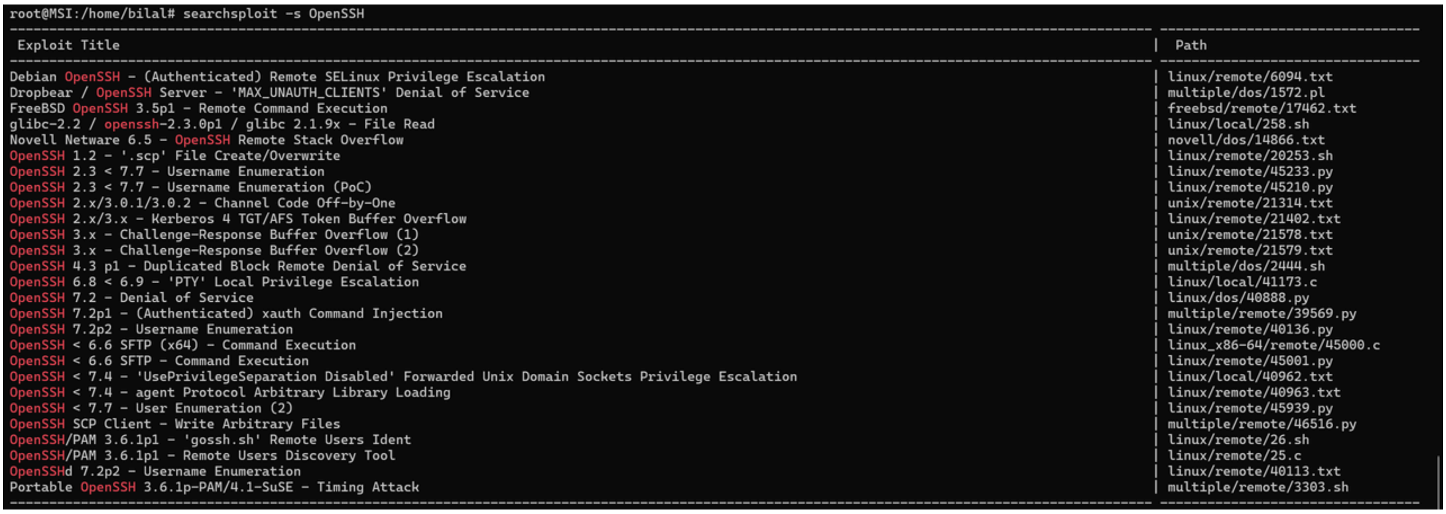


```
msf > search ssh 6.7

Matching Modules
================

   #   Name                                                          Disclosure Date  Rank       Check  Description
   -   ----                                                          ---------------  ----       -----  -----------
   0   exploit/linux/http/cisco_asax_sfr_rce                         2022-06-22       excellent  Yes    Cisco ASA-X with FirePOWER Services Authenticated Command Injection
   1     \_ target: Shell Dropper                                    .                .          .      .
   2     \_ target: Linux Dropper                                    .                .          .      .
   3   exploit/linux/ssh/cisco_ucs_scpuser                           2019-08-21       excellent  No     Cisco UCS Director default scpuser password
   4   exploit/linux/ssh/vmware_vrni_known_privkey                   2023-08-29       excellent  No     VMWare Aria Operations for Networks (vRealize Network Insight) SSH Private
 Key Exposure
   5     \_ target: 6.0_platform                                     .                .          .      .
   6     \_ target: 6.0_proxy                                        .                .          .      .
   7     \_ target: 6.1_platform                                     .                .          .      .
   8     \_ target: 6.1_proxy                                        .                .          .      .
   9     \_ target: 6.2_collector                                    .                .          .      .
  10     \_ target: 6.2_platform                                     .                .          .      .
  11     \_ target: 6.3_collector                                    .                .          .      .
  12     \_ target: 6.3_platform                                     .                .          .      .
  13     \_ target: 6.4_collector                                    .                .          .      .
  14     \_ target: 6.4_platform                                     .                .          .      .
  15     \_ target: 6.5_collector                                    .                .          .      .
  16     \_ target: 6.5_platform                                     .                .          .      .
  17     \_ target: 6.6_collector                                    .                .          .      .
  18     \_ target: 6.6_platform                                     .                .          .      .
  19     \_ target: 6.7_collector                                    .                .          .      .
  20     \_ target: 6.7_platform                                     .                .          .      .
  21     \_ target: 6.8_collector                                    .                .          .      .
  22     \_ target: 6.8_platform                                     .                .          .      .
  23     \_ target: 6.9_collector                                    .                .          .      .
  24     \_ target: 6.9_platform                                     .                .          .      .
  25     \_ target: 6.10_collector                                   .                .          .      .
  26     \_ target: 6.10_platform                                    .                .          .      .
  27     \_ target: All                                              .                .          .      .
  28   exploit/multi/http/vmware_vcenter_uploadova_rce               2021-02-23       manual     Yes    VMware vCenter Server Unauthenticated OVA File Upload RCE
  29     \_ target: VMware vCenter Server <= 6.7 Update 1b (Linux)   .                .          .      .
  30     \_ target: VMware vCenter Server <= 6.7 Update 3j (Windows) .                .          .      .


Interact with a module by name or index. For example info 30, use 30 or use exploit/multi/http/vmware_vcenter_uploadova_rce
After interacting with a module you can manually set a TARGET with set TARGET 'VMware vCenter Server <= 6.7 Update 3j (Windows)'
```



```
root@MSI:/home/bilal# searchsploit -s OpenSSH
------------------------------------------------------------------------------------------------------ -----------------------------------
 Exploit Title                                                                                        |  Path
------------------------------------------------------------------------------------------------------ -----------------------------------
Debian OpenSSH - (Authenticated) Remote SELinux Privilege Escalation                                  | linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIENTS' Denial of Service                                    | multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Execution                                                      | freebsd/remote/17462.txt
glibc-2.2 / openssh-2.3.0p1 / glibc 2.1.9x - File Read                                                | linux/local/258.sh
Novell Netware 6.5 - OpenSSH Remote Stack Overflow                                                    | novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite                                                            | linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration                                                              | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                                                        | linux/remote/45210.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off-by-One                                                     | unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Buffer Overflow                                            | linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (1)                                                  | unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (2)                                                  | unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote Denial of Service                                            | multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege Escalation                                                  | linux/local/41173.c
OpenSSH 7.2 - Denial of Service                                                                       | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection                                               | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration                                                                  | linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Execution                                                          | linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution                                                                | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation  | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                                              | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                                                                  | linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary Files                                                            | multiple/remote/46516.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remote Users Ident                                                   | linux/remote/26.sh
OpenSSH/PAM 3.6.1p1 - Remote Users Discovery Tool                                                     | linux/remote/25.c
OpenSSHd 7.2p2 - Username Enumeration                                                                 | linux/remote/40113.txt
Portable OpenSSH 3.6.1p-PAM/4.1-SuSE - Timing Attack                                                  | multiple/remote/3303.sh
------------------------------------------------------------------------------------------------------ -----------------------------------
```

- Leak sensitive information from the SSH client (CVE-2016-0777).
- Crash the service or cause denial of service (CVE-2016-8858).
- Exploit memory handling bugs that could lead to privilege issues (CVE-2016-10009 and others).
  Even if some fixes are backported by the OS vendor, attackers will still see this as an easy target because the version looks outdated.

Impact:

An attacker could:

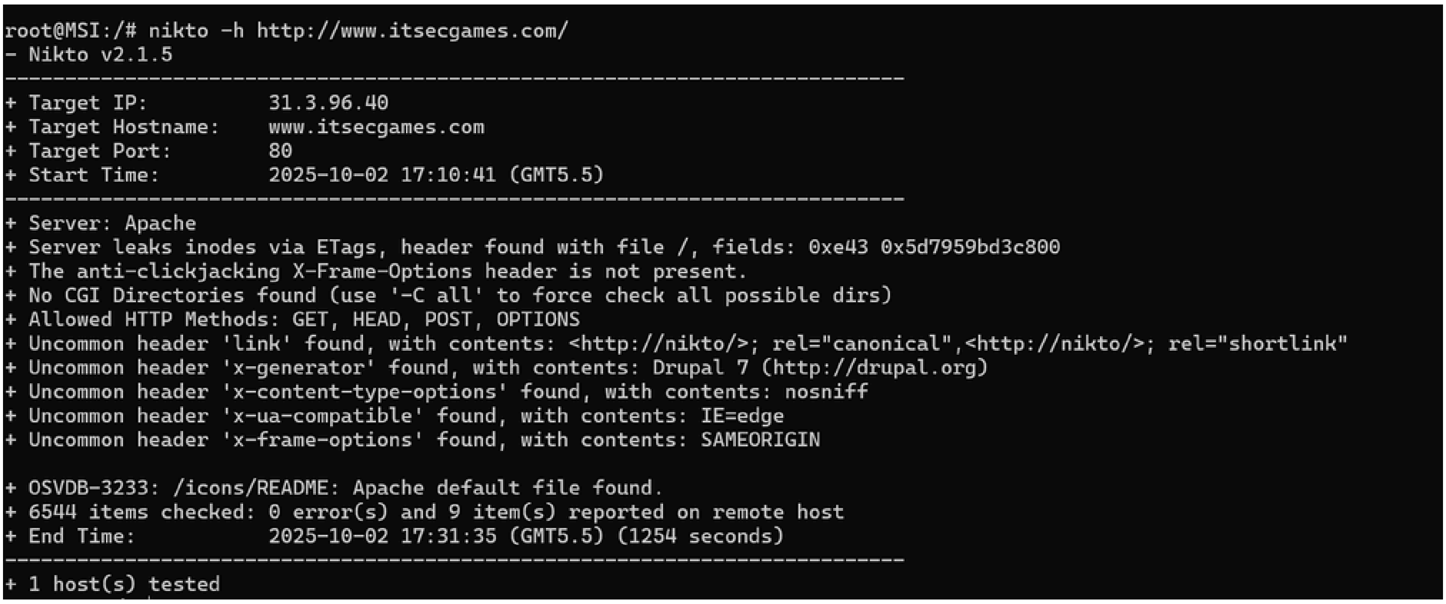
- Try known exploits against this version.
- Cause the SSH service to crash.
- Steal information from users who connect with vulnerable clients.

Recommended Fix:

1. Update SSH to the latest supported version from your OS vendor or directly from OpenSSH.
2. Use stronger keys (e.g., replace old DSA keys with RSA 4096 or ED25519).
3. Harden the SSH config:
   - Disable root login (PermitRootLogin no).
   - Turn off password login (PasswordAuthentication no).
   - Use only strong ciphers, MACs, and key exchange algorithms.
4. Restrict access: only allow SSH from trusted IPs or via a VPN/jump host.
5. Check vendor advisories to confirm which CVEs your package version is patched against.

Finding 02 — Web Server & Application Misconfigurations

Severity: Medium



```
root@MSI:/# nikto -h http://www.itsecgames.com/
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          31.3.96.40
+ Target Hostname:    www.itsecgames.com
+ Target Port:        80
+ Start Time:         2025-10-02 17:10:41 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ Server leaks inodes via ETags, header found with file /, fields: 0xe43 0x5d7959bd3c800
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Uncommon header 'link' found, with contents: <http://nikto/>; rel="canonical",<http://nikto/>; rel="shortlink"
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-ua-compatible' found, with contents: IE=edge
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN

+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2025-10-02 17:31:35 (GMT5.5) (1254 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Evidence:

- ETag header leaks info → exposes file system details useful for fingerprinting.
- Missing X-Frame-Options header → site can be loaded in iframes, allowing clickjacking attacks.
- CMS disclosure (Drupal 7) → revealed by X-Generator header, makes it easier for attackers to look up Drupal-specific exploits.
- Default Apache file accessible (/icons/README) → shows the server is not hardened.
- Server type disclosed (Apache) → version info can help attackers target known Apache flaws.
- OPTIONS method enabled → reveals which HTTP methods are allowed, increasing attack surface.

Why this is a problem:

- Leaked information helps attackers map the system and choose the right exploits.
- Missing security headers makes the site more vulnerable to UI-based attacks like clickjacking.
- Running Drupal 7 (if unpatched) is risky since it has a history of serious CVEs (e.g., Drupalgeddon).
- Default files and unnecessary methods signal weak server hardening.

Impact:

Attackers can use these leaks to:

- Run more targeted attacks (reconnaissance → exploitation).
- Trick users into clicking hidden buttons (clickjacking).
- Launch automated attacks against known Drupal or Apache issues.

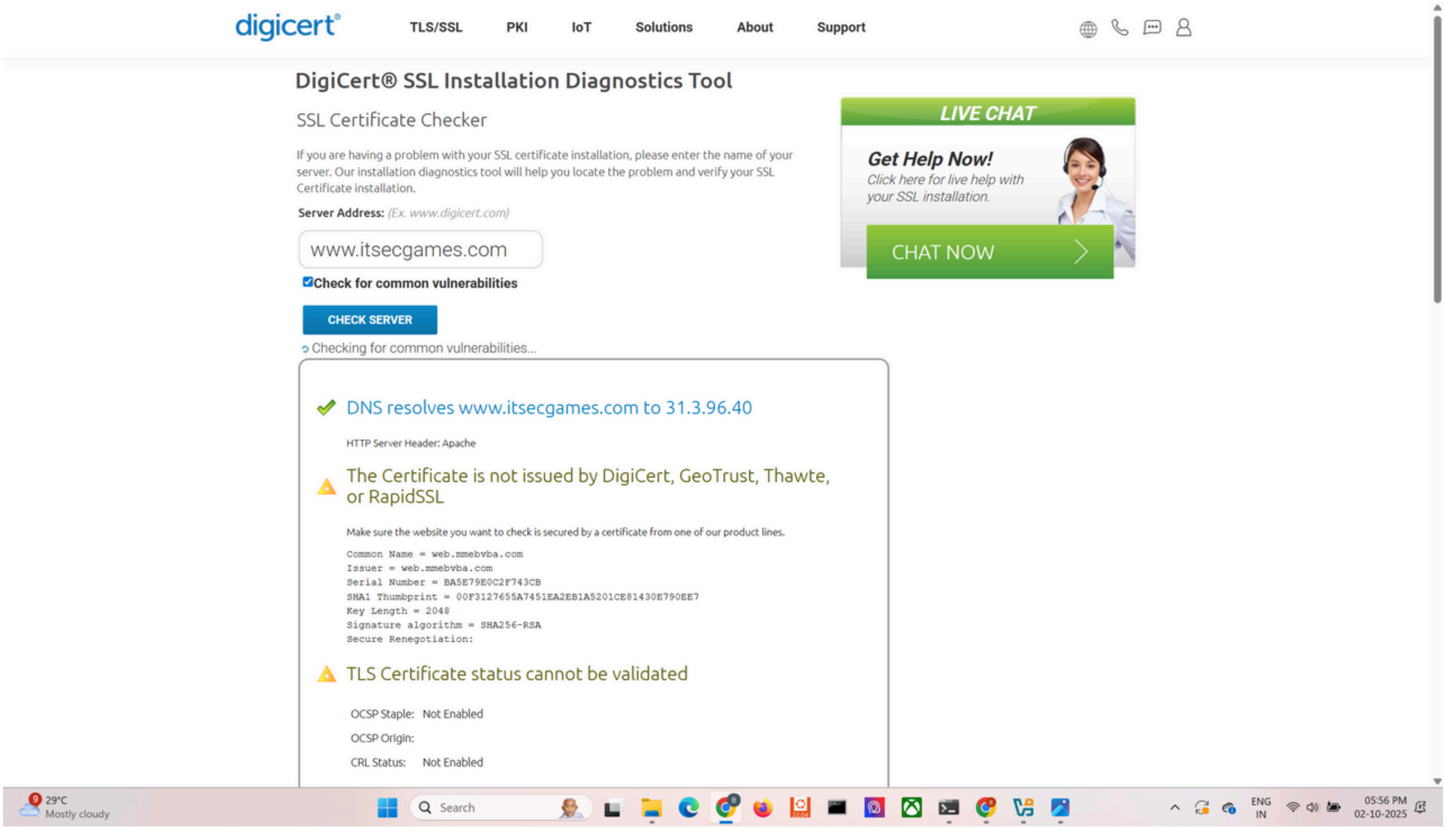
Recommended Fixes:

1. Remove default files (e.g., /icons/README).
2. Hide version info: suppress Server and X-Generator headers via config or reverse proxy.
3. Add security headers:
   - X-Frame-Options: SAMEORIGIN (or DENY)
   - X-Content-Type-Options: nosniff
   - Strict-Transport-Security (if HTTPS is used)
   - Content-Security-Policy for defense in depth
4. Disable unnecessary HTTP methods: only allow GET and POST.
5. Update Drupal 7 to the latest patched release, and keep modules/themes updated.
6. Harden Apache: disable directory listing, limit ServerTokens/ServerSignature, and remove unused content.

Finding 03 — TLS/SSL Certificate Issues

Severity: High (impacts trust, possible MITM risk)
Affected Host: www.itsecgames.com (31.3.96.40)
Service: HTTPS / TLS

Evidence



DigiCert® SSL Installation Diagnostics Tool

SSL Certificate Checker

If you are having a problem with your SSL certificate installation, please enter the name of your server. Our installation diagnostics tool will help you locate the problem and verify your SSL Certificate installation.

Server Address: (Ex. www.digicert.com)

www.itsecgames.com

☑ Check for common vulnerabilities

CHECK SERVER

Checking for common vulnerabilities...

✓ DNS resolves www.itsecgames.com to 31.3.96.40

HTTP Server Header: Apache

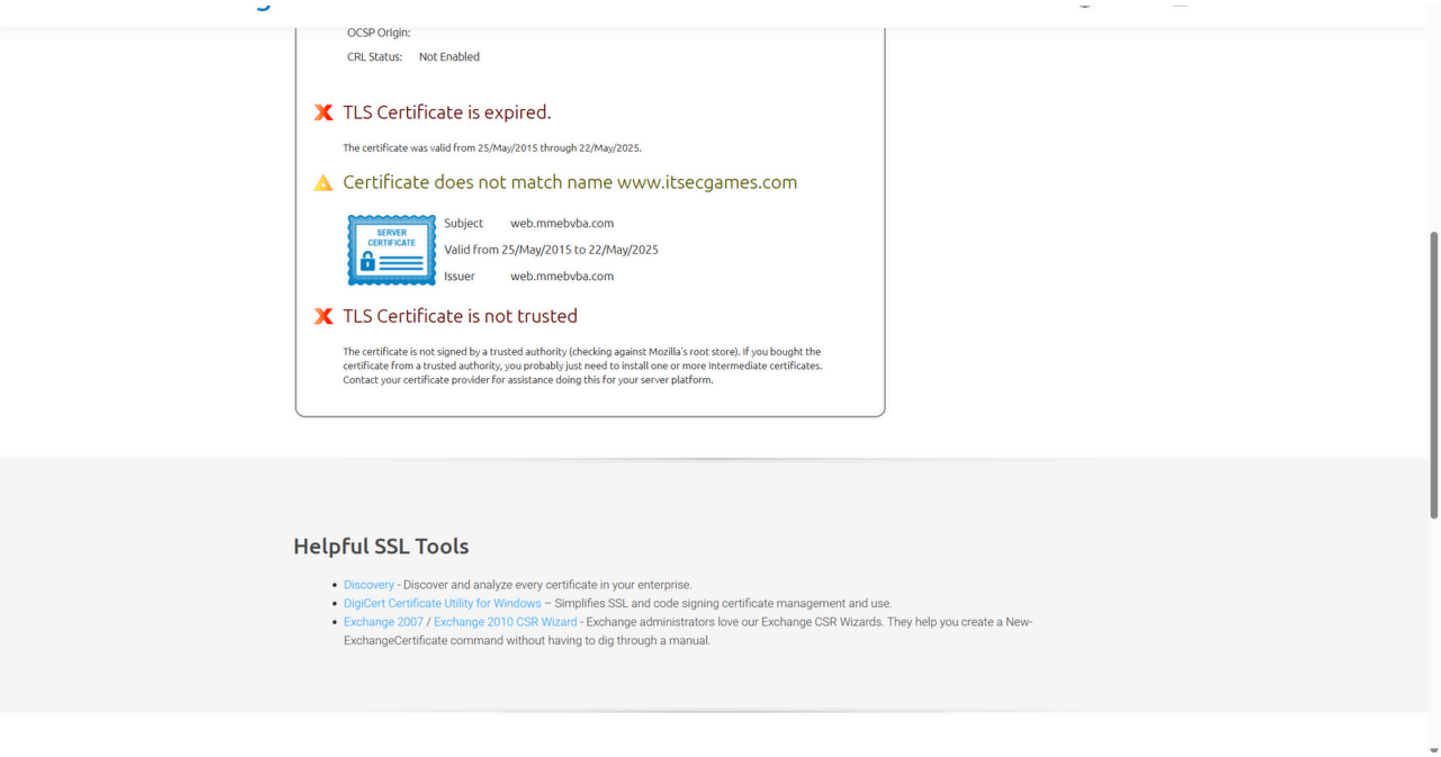
⚠ The Certificate is not issued by DigiCert, GeoTrust, Thawte, or RapidSSL

Make sure the website you want to check is secured by a certificate from one of our product lines.

```
Common Name = web.mmebvba.com
Issuer = web.mmebvba.com
Serial Number = BA5E79E0C2F743CB
SHA1 Thumbprint = 00F3127655A7451EA2EB1A5201CE81430E790EE7
Key Length = 2048
Signature algorithm = SHA256-RSA
Secure Renegotiation:
```

⚠ TLS Certificate status cannot be validated

OCSP Staple: Not Enabled
OCSP Origin:
CRL Status: Not Enabled



OCSP Origin:
CRL Status: Not Enabled

✗ TLS Certificate is expired.

The certificate was valid from 25/May/2015 through 22/May/2025.

⚠ Certificate does not match name www.itsecgames.com

Subject web.mmebvba.com
Valid from 25/May/2015 to 22/May/2025
Issuer web.mmebvba.com

✗ TLS Certificate is not trusted

The certificate is not signed by a trusted authority (checking against Mozilla's root store). If you bought the certificate from a trusted authority, you probably just need to install one or more Intermediate certificates. Contact your certificate provider for assistance doing this for your server platform.

Helpful SSL Tools

- Discovery - Discover and analyze every certificate in your enterprise.
- DigiCert Certificate Utility for Windows – Simplifies SSL and code signing certificate management and use.
- Exchange 2007 / Exchange 2010 CSR Wizard - Exchange administrators love our Exchange CSR Wizards. They help you create a New-ExchangeCertificate command without having to dig through a manual.

The TLS/SSL certificate for the target domain exhibits multiple security and trust issues:

- Expired Certificate → Valid from *25/May/2015* to *22/May/2025*. Certificate is past its expiry date.

- Certificate Mismatch → Subject CN = web.mmebvba.com, does not match requested hostname www.itsecgames.com.
- Self-signed / Not Trusted → Issuer = web.mmebvba.com, certificate is not signed by a trusted Certificate Authority (not DigiCert, GeoTrust, Thawte, or RapidSSL).
- OCSP/CRL Not Enabled → No Online Certificate Status Protocol (OCSP) stapling or Certificate Revocation List checks enabled.
- Secure Renegotiation Not Confirmed → Potential downgrade or renegotiation risks.

Impact

- Trust & Spoofing Risk: Browsers/users will see certificate warnings. Users may ignore these, which can be exploited by an attacker performing a Man-in-the-Middle (MITM) attack.
- Phishing / Impersonation Risk: Domain mismatch allows attackers to impersonate the target website using rogue certificates.
- Compliance Issues: TLS misconfiguration may violate compliance standards (e.g., PCI DSS, ISO 27001).
- Reputation Risk: Visitors will see “Not Secure” warnings, reducing trust in the service.

Remediation

1. Obtain a valid certificate from a trusted Certificate Authority (CA) such as DigiCert, Let’s Encrypt, GeoTrust, Thawte, or RapidSSL.
   - Ensure the Common Name (CN) and Subject Alternative Name (SAN) fields include www.itsecgames.com (and itsecgames.com if needed).
2. Install intermediate certificates (if required by the chosen CA) to ensure browsers can validate the trust chain.
3. Enable OCSP Stapling and CRL checks in Apache to allow clients to verify revocation status efficiently.
4. Reconfigure Apache with strong TLS settings:
   - Disable weak ciphers and protocols (SSLv2, SSLv3, TLS 1.0/1.1).
   - Enforce TLS 1.2+ (preferably TLS 1.3).
   - Configure SSLHonorCipherOrder on and modern cipher suites.