VULNERABILITY ASSESSMENT REPORT

ITSECGAMES.COM

AARAV SHAH (ROUND 2 ASSESSMENT - SECURITY OFFICER TRAINEE)

DATE: 2025-09-15

# EXECUTIVE SUMMARY

This assessment consolidates several non-destructive automated scans against the public assets of itsecgames.com. The goal was to enumerate the attack surface, identify misconfigurations and service exposures, and provide prioritized remediation actions. The scans detected several high- and medium-risk issues (RDP/UDP exposure, SNMP available, possible Slowloris susceptibility on HTTP, and internal DNS information leakage, Heartbleed vulnerability and expired SSL).

# METHODOLOGY & TOOLS USED

Scans were non-intrusive and focused on discovery and detection. The following tools/results were used to prepare this report:

- RapidScan aggregate run (rs.vul.itsecgames.com.2025-09-15) — includes automated multi-tool outputs  
- SSL Labs server test (certificate & TLS configuration)  
- Nmap (service discovery and NSE checks)  
- Nikto (webserver misconfiguration & header checks)  
- SSLyze (TLS / renegotiation checks)  
- WhatWeb, Wafw00f, dnsmap, Fierce (fingerprinting and subdomain discovery)  
- Censys (service fingerprinting & asset discovery)

No exploitation or destructive testing was performed. The raw RapidScan artifact provided was used as primary evidence and is referenced in the Appendix.

# ATTACK SURFACE SNAPSHOT

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hostname** | **IP (observed)** | **Ports/Services** | **Notes** | **Risk** |
| itsecgames.com / www.itsecgames.com | 31.3.96.40 | 80 (HTTP), 443 (HTTPS), 22 (SSH) | Apache web host; public web app | High |
| vpn.itsecgames.com | 176.95.65.18 | — | VPN appliance (DNS record present) | High |
| firewall.itsecgames.com | 176.95.65.18 | — | Firewall admin console (DNS record present) | High |
| mssql.itsecgames.com / database.itsecgames.com | 81.82.245.81 | — | Database host (DNS record present) | High |
| dc.itsecgames.com / ldap.itsecgames.com | 10.0.1.10 | — | Internal IP found in public DNS (RFC1918 leak) | High |
| \*.mcas.\* (passive records) | — | 80/443 | Microsoft MCAS proxy / passive CT entries | Info |

# FINDINGS

## HIGH SEVERITY

#### RDP detected over UDP (3389 UDP)

Evidence: Nmap/RapidScan reported '3389/udp open|filtered' and flagged RDP over UDP as a high-risk finding.

Impact: Public RDP increases risk of brute-force attacks, exploitation, and availability or lateral-movement opportunities.

#### Heartbleed vulnerability

Evidence: RapidScan/Golismero flagged Heartbleed (CVE-2014-0160) as exploitable. An attacker can leak memory contents including credentials.

Mitigation: Patch OpenSSL to the latest version.

#### Expired / invalid SSL certificate

Evidence: SSL Labs reported the certificate as expired and self-signed. Browsers do not trust this certificate, enabling MITM attacks.

Mitigation: Replace with a valid certificate from a trusted CA.

#### Domain spoofing / hijacking risk

Evidence: RapidScan flagged possible DNS spoofing / hijacking due to lack of DNSSEC.

Mitigation: Deploy DNSSEC on authoritative DNS servers.

#### Internal DNS IP leakage (RFC1918 addresses found in public DNS)

Evidence: dnsmap and fierce outputs show dc.itsecgames.com and ldap.itsecgames.com resolving to 10.0.1.10 (internal RFC1918 address).

Impact: Reveals internal architecture and host names, which helps attacker reconnaissance and reduces security-by-obscurity protections.

#### Slowloris-like DoS susceptibility on HTTP (Apache)

Evidence: Nmap http-slowloris NSE reported 'Probably vulnerable: the DoS attack took +2m13s with 996 concurrent connections' against port 80.

Impact: An attacker could cause resource exhaustion and availability loss via slow-request attacks.

## MEDIUM SEVERITY

#### SNMP service detected (UDP 161)

Evidence: Nmap reported '161/udp open|filtered'. RapidScan flagged SNMP as medium risk.

Impact: SNMPv1/v2 exposure with default community strings can leak network device data and be used for reconnaissance.

#### Missing / weak HTTP security headers and ETag leakage

Evidence: Nikto reported missing X-Frame-Options and X-Content-Type-Options headers. It also noted ETag values that can leak inode information.

Impact: Missing headers increase risk of clickjacking, MIME sniffing, and make exploitation of XSS easier on older browsers; ETag leakage aids fingerprinting.

#### Subdomain enumeration / attack surface expansion

Evidence: dnsmap / fierce / RapidScan enumerated multiple subdomains (vpn, firewall, mssql, database, etc.).

Impact: More subdomains increase the chance of misconfigurations and forgotten services exposed to the Internet.

## LOW / INFORMATIONAL

No IPv6 support: Not a direct vulnerability but limits security and availability benefits. Subdomain enumeration: Multiple subdomains discovered (vpn, firewall, db) expanding attack surface. Server fingerprinting: WhatWeb/Nikto identified Apache with exposed headers.

# REMEDIATION CHECKLIST

### Immediate (hours):

- Block RDP (3389 UDP/TCP) and SNMP (161 UDP) from public access. Use firewall rules or cloud security groups.  
- Remove internal RFC1918 DNS records from public zones and audit DNS files.  
- If the public web app is not required, restrict it behind a VPN or take it offline until hardened.  
- Replace expired SSL certificate with trusted CA-signed cert.

### Short-term (days):

- Enable mod\_reqtimeout / mod\_qos in Apache and tune KeepAlive/Timeout settings.  
- Add security headers (X-Frame-Options, X-Content-Type-Options, Referrer-Policy).  
- Harden SSH: restrict source IPs, enforce key-based auth, disable password logins; enable fail2ban.  
- Patch OpenSSL (Heartbleed).  
- Enable Apache modules to mitigate Slowloris.  
- Add missing security headers.

### Medium-term (weeks):

- Deploy a WAF/CDN for web protection and DoS mitigation (e.g., ModSecurity, Cloudflare, AWS WAF).  
- Patch and harden DB / VPN / firewall appliances reported in DNS.  
- Set up certificate transparency monitoring (crt.sh alerts) and domain monitoring for lookalikes / typosquats.  
- Deploy DNSSEC to prevent spoofing.  
- Add WAF for protection.  
- Enable IPv6 for resilience and IPSec support.

# SELECTED EVIDENCE (FROM RS.VUL.ITSECGAMES.COM - EXCERPT)

Note: Excerpts from rapidscan output. Rapidscan was ran 2-3 along with nuclei, censys and other tools to validate findings.  
  
WAFW00F: No WAF detected (generic detection)  
SSLyze: Secure renegotiation supported; client renegotiation not vulnerable  
Nmap: 3389/udp open|filtered (RDP over UDP detected)  
Nmap: http-slowloris NSE - Probably vulnerable (DoS test took +2m13s)  
Nikto: Missing X-Frame-Options and X-Content-Type-Options headers; ETag may leak inode info  
DNSMap / Fierce: dc.itsecgames.com and ldap.itsecgames.com resolved to 10.0.1.10 (internal IP leak)  
Nmap: 161/udp open|filtered (SNMP)  
WhatWeb: HTML title reported (app fingerprinting)