

# Vulnerability Assessment Report

**Job Title:** Security Officer Trainee @Accuknox

**Target:** <http://www.itsecgames.com/>

**IP Address:** 31.3.96.40

**Date of Assessment:** 06 September 2025

**Assessor:** Syed Muzakkir Shah Harooni

## 1. Executive Summary

A reconnaissance and vulnerability assessment was performed on **itsecgames.com**, revealing that the server is hosted on IP 31.3.96.40 with multiple open services. The most notable finding is an **outdated version of OpenSSH (6.7p1)** exposed on port **22**, which is linked to multiple high-severity and exploitable vulnerabilities (CVSS up to 9.8).

The web services (ports **80/443**) are running **Apache HTTPD**, with HTTP traffic redirecting to HTTPS and another domain ([www.mmebvba.com](http://www.mmebvba.com)). The headers reveal standard configurations with no obvious security misconfigurations. No XSS, CSRF, or common HTTP-based vulnerabilities were detected via automated scans.

However, the outdated SSH service presents a **critical attack surface** that could allow attackers to gain unauthorized access.

## 2. Scope & Methodology

The following methodology was used:

- **Step 1: Reconnaissance**
  - **DNS enumeration (nslookup, dig):** Used to identify the IP address, DNS records, and associated domains of the target. This helps map the attack surface.
  - **Network connectivity testing (ping):** Verified host availability and measured latency (round-trip time).
  - **HTTP header review (curl):** Collected server response headers to check for exposed information (e.g., software versions, missing security headers).



```

File Machine View Input Devices Help
Tr Processing triggers for man-db (2.10.2-1) ...
File Actions Edit View Help
Tr Processing triggers for man-db (2.10.2-1) ...
[+] kali㉿kali:[~]
└─$ nslookup itsecgames.com
Server: 192.168.0.1
Address: 192.168.0.1#53
Non-authoritative answer:
Name: itsecgames.com
Address: 31.3.96.40
[+] kali㉿kali:[~]
└─$ dig +short itsecgames.com
31.3.96.40
[+] kali㉿kali:[~]
└─$ ping -c 4 itsecgames.com
PING itsecgames.com (31.3.96.40) 56(84) bytes of data.
64 bytes from web.mmevbba.com (31.3.96.40): icmp_seq=1 ttl=44 time=357 ms
64 bytes from web.mmevbba.com (31.3.96.40): icmp_seq=2 ttl=44 time=336 ms
64 bytes from web.mmevbba.com (31.3.96.40): icmp_seq=3 ttl=44 time=353 ms
64 bytes from web.mmevbba.com (31.3.96.40): icmp_seq=4 ttl=44 time=325 ms
--- itsecgames.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3103ms
rtt min/avg/max/mdev = 324.982/342.559/356.809/12.859 ms
[+] kali㉿kali:[~]
└─$ curl -I http://itsecgames.com
HTTP/1.1 200 OK
Date: Wed, 06 Sep 2025 00:24:57 GMT
Server: Apache/2.4.42
Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT
ETag: "e43-5d7059bd2c800"
Accept-Ranges: bytes
Content-Length: 3651
Vary: Accept-Encoding
Content-Type: text/html

```

- **Step 2: Port & Service Discovery**

- **Full TCP scan (nmap):** Scanned all 65,535 ports to identify which services are exposed to the internet.



```

File Machine View Input Devices Help
Tr Content-Length: 3651
Vary: Accept-Encoding
Content-Type: text/html
[+] kali㉿kali:[~]
└─$ nmap -O itsecgames.com -oN nmap_full.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-05 20:25 EDT
Stats: 0:02:38 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.61% done; ETC: 20:41 (0:13:33 remaining)
Stats: 0:03:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 24.71% done; ETC: 20:41 (0:12:05 remaining)
Stats: 0:06:28 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 38.81% done; ETC: 20:42 (0:10:12 remaining)
Stats: 0:07:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 42.85% done; ETC: 20:42 (0:09:50 remaining)
Stats: 0:07:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 45.28% done; ETC: 20:41 (0:08:58 remaining)
Stats: 0:07:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 45.92% done; ETC: 20:41 (0:08:57 remaining)
Stats: 0:09:59 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 60.29% done; ETC: 20:41 (0:06:35 remaining)
Stats: 0:10:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 64.71% done; ETC: 20:42 (0:05:53 remaining)
Stats: 0:12:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.87% done; ETC: 20:42 (0:04:10 remaining)
Stats: 0:13:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 80.18% done; ETC: 20:42 (0:03:18 remaining)
Nmap scan report for itsecgames.com (31.3.96.40)
Host is up (0.052s latency).
rDNS record for 31.3.96.40: web.mmevbba.com
Not shown: 65355 filtered tcp ports (no-response), 178 filtered tcp ports (ne
└─$ cat nmap_full.txt
PORT      STATE SERVICE VERSION

```

- **Service version detection (nmap -sV):** Determined the version of running services (e.g., OpenSSH 6.7p1, Apache HTTPD) for vulnerability matching.

```
[kalilinux] ~] $ nmap -sV --script vuln www.itsecgames.com
Starting Nmap 7.99 ( https://nmap.org ) at 2025-09-05 22:17 EDT
Nmap Timestr: About 98.98 seconds; ETC: 22:22 (0:00:00 remaining)
Nmap scan report for www.itsecgames.com (31.3.96.40)
Host is up (0.029s latency).
DNS record for 31.3.96.40: web.memevb.a.com
Nmap shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh        OpenSSH 7.6p1 (protocol 2.0)
| vulners:
|_ cpe:/a:openbsd:openssh:6.7p1:
|   PACKETSTORM:173661 9.8  https://vulners.com/packetstorm/PACKETSTORM:173661_*EXPLOIT*
| F99791B3-AE88-5B84-86C7-3AF0523F3807 9.8  https://vulners.com/g
| ihubexploit/F99791B3-AE88-5B84-86C7-3AF0523F3807 9.8  https://vulners.com/g
|_ CVE-2016-1988 9.8  https://vulners.com/cve/CVE-2016-1988
| B8190C0B-3EB9-5611-9828-8064A1575B23 9.8  https://vulners.com/g
| ihubexploit/B8190C0B-3EB9-5611-9828-8064A1575B23 9.8  *EXPLOIT*
| 8FC9C5AB-3960-5F33-B25E-E80B8379A623 9.8  https://vulners.com/g
| ihubexploit/8FC9C5AB-3960-5F33-B25E-E80B8379A623 9.8  *EXPLOIT*
| B4D90159-5E8C-54E6-84E6-1AA7D2E93292 9.8  https://vulners.com/g
| ihubexploit/B4D90159-5E8C-54E6-84E6-1AA7D2E93292 9.8  *EXPLOIT*
|_ 22277290-6700-57CB-8930-1EEAFDB9FF0 9.8  https://vulners.com/g
| ihubexploit/22277290-6700-57CB-8930-1EEAFDB9FF0 9.8  *EXPLOIT*
|_ 0221525F-07F5-5799-912D-F4B9E2D1B587 9.8  https://vulners.com/g
| ihubexploit/0221525F-07F5-5799-912D-F4B9E2D1B587 9.8  *EXPLOIT*
|_ CVE-2015-5909 8.1  https://vulners.com/cve/CVE-2015-5909
| BFB1B000-F993-5CAF-BD57-D7E2901C101C 8.1  https://vulners.com/g
| ihubexploit/BFB1B000-F993-5CAF-BD57-D7E2901C101C 8.1  *EXPLOIT*
|_ PACKETSTORM:140078 7.8  https://vulners.com/packetstorm/PACKETSTORM:140078_*EXPLOIT*
| EXPLOITPACK:5BCA798C6BA71FAE29334297EC0BA09 7.8  https://vulne
|_ rs.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0BA09 *EXPLOIT*
```

- **Header collection (nmap --script http-headers):** Gathered additional HTTP header information for misconfiguration analysis.

- **Step 3: Vulnerability Assessment**
    - **Automated script scan (nmap --script vuln):** Ran Nmap's NSE vulnerability scripts to check for common CVEs (e.g., XSS, CSRF, outdated services).
    - **CVE mapping (vulners database):** Cross-referenced service versions (like OpenSSH 6.7p1) against known CVEs to assess severity and exploit availability.



```

kali㉿kali:~$ nmap --script vuln www.itsecgames.com >nmap_vulns.txt
Starting Nmap 7.05 ( https://nmap.org ) at 2025-09-05 20:45 EDT
Stats: 0:01:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 87.63% done; ETC: 20:47 (0:00:11 remaining)
Stats: 0:02:28 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 91.30% done; ETC: 20:47 (0:00:10 remaining)
NSE Script: About 91.30% done; ETC: 20:47 (0:00:10 remaining) undergoing Script Scan
NSE Timing: About 95.32% done; ETC: 20:48 (0:00:09 remaining)
Stats: 0:04:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.34% done; ETC: 20:49 (0:00:02 remaining)
Stats: 0:05:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.34% done; ETC: 20:50 (0:00:02 remaining)
Stats: 0:05:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.34% done; ETC: 20:50 (0:00:02 remaining)
Stats: 0:05:37 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.34% done; ETC: 20:50 (0:00:02 remaining)
Stats: 0:05:56 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.34% done; ETC: 20:51 (0:00:02 remaining)
Stats: 0:07:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.34% done; ETC: 20:51 (0:00:03 remaining)
NSE Script: About 99.34% done; ETC: 20:51 (0:00:03 remaining) undergoing Script Scan
NSE Timing: About 99.34% done; ETC: 20:53 (0:00:03 remaining)
Nmap scan report for www.itsecgames.com (31.3.96.40)
Host is up (0.043s latency).
rDNS record for 31.3.96.40: web.mmebvba.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-aspen-debug: ERROR: Script execution failed (use -d to debug)
443/tcp   open  https
|_http-vuln-cve2016-3704: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-aspen-debug: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 534.76 seconds

```

## 3. Findings

### 3.1 Network & DNS Information

- Domain:** itsecgames.com
- Resolved IP:** 31.3.96.40
- Reverse DNS:** web.mmebvba.com
- Latency:** ~325–356 ms average RTT
- Availability:** Host responds consistently to ICMP

### 3.2 Open Ports & Services

Port	State	Service	Version	Notes
22	Open	SSH	OpenSSH 6.7p1 (protocol 2.0)	<b>Outdated</b> , multiple critical CVEs
53	Open	DNS	Generic DNS (TCP)	Returns NOTIMP response
80	Open	HTTP	Apache HTTPD	Responds with 200 OK, static content
443	Open	HTTPS	Apache HTTPD	Redirects to <a href="https://www.mmebvba.com">https://www.mmebvba.com</a>

### 3.3 HTTP Headers (Port 80)

Date: Sat, 06 Sep 2025 00:24:57 GMT

Server: Apache

Last-Modified: Wed, 09 Feb 2022

ETag: "e43-5d7959bd3c800"

Content-Length: 3651

Content-Type: text/html

**Nikto web server scan:** Checked for misconfigurations, outdated components, and missing security headers.

(nikto -h http://www.itsecgames.com -output nikto\_report.txt) confirmed the absence of key security headers such as HSTS, X-Frame-Options, and Content-Security-Policy, consistent with the manual header review.

- No Strict-Transport-Security (HSTS) header detected.
- No X-Frame-Options, X-XSS-Protection, or Content-Security-Policy headers observed.
- Site still accessible via plain HTTP → vulnerable to MITM.



```
File Actions Edit View Help
[kali㉿kali]-~
└─$ nikto -h http://www.itsecgames.com -output nikto_report.txt
- Nikto v2.5.0

+ Target IP:      31.3.96.40
+ Target Hostname: www.itsecgames.com
+ Target Port:    80
+ Start Time:    2025-09-05 21:03:58 (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 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: 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)
+ /www.itsecgames.com/tar.lzma: Drupal 7 was identified via the x-generator header. See: https://www.drupal.org/project/remove_http_headers
+ /www.itsecgames.com/tar.lzma: Drupal Link header found with value: <http://31.3.96.40/>;rel="canonical"<http://31.3.96.40/>;rel="shortlink". See: https://www.drupal.org/
nikto -h http://www.itsecgames.com -output nikto.report.txt
- STATUS: Completed 500 requests (~7% complete, 41.7 minutes left): currently
in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.43636 sec, 10 requests: 0.4457 sec
- STATUS: Completed 530 requests (~8% complete, 41.8 minutes left): currently
in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.42957 sec, 10 requests: 0.4280 sec
:
+ /: Server may leak nodes via ETags, header found with file /, inode: e43,
size: 157999432000, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ STATUS: Completed 790 requests (~13% complete, 41.0 minutes left): currentl
y in plugin 'shellshock'
- STATUS: Running average: 100 requests: 0.29879 sec, 10 requests: 0.3036 sec
:
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /: An Allow Response could be Appending './' to a directory may reveal PH
P source code
- STATUS: Completed 870 requests (~13% complete, 39.4 minutes left): currentl
y in plugin 'Nikto Tests'
```

## 3.4 Vulnerability Assessment

### **SSH (Port 22 - OpenSSH 6.7p1)**

- Multiple **critical vulnerabilities** identified:
  - **CVE-2023-38408** (CVSS 9.8) – Remote code execution in OpenSSH.
  - **CVE-2016-1908** (CVSS 9.8) – Privilege escalation.
  - **CVE-2015-5600** (CVSS 8.5) – Keyboard-interactive authentication brute force.
  - **CVE-2020-15778** (CVSS 7.8) – Command injection via scp.
  - Several enumeration and information disclosure flaws.

**Exploits for these vulnerabilities are publicly available (ExploitDB, GitHub, PacketStorm).**

### **HTTP / HTTPS (Ports 80/443 – Apache HTTPD)**

- Server header exposed → version fingerprinting possible.
- **Redirects traffic from 443 → [www.mmebvba.com](http://www.mmebvba.com)** (external domain).
- No critical vulnerabilities detected by Nmap.
- No stored/DOM-based XSS or CSRF found in automated scans.
- Missing security headers as mentioned above.

### **DNS (Port 53)**

- Open TCP but limited functionality (NOTIMP response).
- No active exploitation observed.

## 4. Risk Assessment

Risk	Affected Service	Severity	Description

Outdated OpenSSH 6.7p1	SSH (22/tcp)	<span style="color:red;">●</span> <b>Critical</b>	Multiple RCE & privilege escalation vulnerabilities, public exploits available.
Missing Security Headers	HTTP/HTTPS	<span style="color:orange;">●</span> Medium	Increases risk of clickjacking, XSS, MITM attacks.
Plain HTTP access	HTTP (80/tcp)	<span style="color:orange;">●</span> Medium	No enforced HTTPS, susceptible to session hijacking.
Information Disclosure	Apache, DNS	<span style="color:green;">●</span> Low	Server headers and DNS info exposed, useful for attackers in recon.

## 5. Recommendations

### 1. Patch SSH Immediately

- a. Upgrade OpenSSH to the latest stable version.
- b. Restrict SSH access to trusted IPs only (via firewall).
- c. Enforce key-based authentication and disable password logins.

### 2. Enforce HTTPS Strictly

- a. Redirect all HTTP traffic to HTTPS.
- b. Enable HSTS (Strict-Transport-Security).

### 3. Harden Web Server Security Headers

- a. Add X-Frame-Options: DENY
- b. Add Content-Security-Policy
- c. Add X-Content-Type-Options: nosniff

### 4. Limit Information Disclosure

- a. Remove or obfuscate Server: Apache header.
- b. Configure DNS to minimize leakage.

### 5. Ongoing Security Practices

- a. Regular vulnerability scanning and patch management.
- b. Intrusion Detection / Prevention monitoring for SSH brute force attempts.
- c. Web Application Firewall (WAF) for added HTTP protection.

## 6. Conclusion

The assessment of **itsecgames.com** revealed a **high-risk security posture**, primarily due to an outdated SSH service with known exploits. While the web services did not show

major vulnerabilities during automated scans, missing best-practice security headers and lack of HTTPS enforcement expose users to potential MITM and client-side attacks.

## 7. Appendix

### 7.1 Tools Used (Linux Environment)

- **Nmap** → Network scanning, port & service discovery, vulnerability scripts
- **Nikto** → Web server vulnerability scanner
- **cURL** → Manual HTTP header inspection
- **OpenSSL** → SSL/TLS certificate review
- **Ping / Dig / Nslookup** → Basic reconnaissance and DNS enumeration

## 7.2 Commands Executed

### Reconnaissance

```
# Check domain resolution  
nslookup itsecgames.com  
  
# Alternative DNS lookup  
dig itsecgames.com  
  
# Test host connectivity  
ping -c 4 itsecgames.com
```

### HTTP Header Review

```
curl -I http://www.itsecgames.com
```

### Port & Service Discovery

```
# Full TCP scan  
nmap -p- itsecgames.com  
  
# Service version detection  
nmap -sV itsecgames.com  
  
# Collect HTTP headers  
nmap --script http-headers -p 80,443 itsecgames.com
```

### Vulnerability Assessment

```
# Run vulnerability scripts  
nmap --script vuln -oN nmap_vulns.txt itsecgames.com  
  
# Web server scan with Nikto  
nikto -h http://www.itsecgames.com -output nikto_report.txt
```

### SSL/TLS Testing

```
openssl s_client -connect www.itsecgames.com:443
```

## Webpage View

The screenshot shows the homepage of bWAPP (buggy Web Application). The page has a yellow header with the bWAPP logo (a bee icon) and the text "an extremely buggy web app!". To the right is the MME logo (a shield with a keyhole and a dragonfly icon). Below the header is a dark navigation bar with links: Home, Bugs, Download, Talks & Training, and Blog. The main content area has a title "/ Home /". It contains several paragraphs of text about the application's purpose and usage. On the right side, there are social media sharing icons for Twitter, LinkedIn, Facebook, and Email. At the bottom, a footer bar contains a license notice: "bWAPP is licensed under [\(CC BY-NC-SA\)](#) © 2022 MME BV / Follow [@MME\\_BV](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive [training?](#)"