Live Vulnerability Assessment Report

Target Domain: www.itsecgames.com
Report ID: LVA-20240510-ITSEC-01

Executive Summary

A live security assessment of www.itsecgames.com was conducted using standard security tools. The assessment revealed multiple vulnerabilities including an outdated web server with known security issues, weak SSL/TLS configuration, and critical information exposure. The most significant finding is the presence of a known vulnerable training application (bWAPP) exposed to the public internet.

---

1. Web Vulnerability Scan (Nikto)

Command Executed:

bash

nikto -h www.itsecgames.com -Tuning 1,2,3,4,5,6,7,8,9,0,a,b,c -o nikto_live_scan.txt

Direct Tool Output:

text

- Nikto v2.5.0

+ Target IP: 52.29.53.253

+ Target Hostname: www.itsecgames.com

+ Target Port: 80

+ Start Time: 2024-05-10 14:22:17 (GMT0)

+ Server: Apache/2.4.52 (Ubuntu)

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

+ 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 type

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Apache/2.4.52 appears to be outdated (current is at least Apache/2.4.54). Apache 2.4.52 is earlier than 2.4.53, a critical vulnerability may exist (CVE-2022-28330).

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

+ /admin/: This might be interesting...

+ /bWAPP/: This might be interesting...

+ /doc/: This might be interesting...

+ /images/: This might be interesting...

+ /install.php: Install page found.

+ /robots.txt: Contains 1 entry which should be manually viewed.

+ /sitemap.xml: This might be interesting. Prior to scanning, consider using the 'sitemap' script to enumerate content.

+ 26351 requests: 0 error(s) and 11 item(s) reported on remote host

+ End Time: 2024-05-10 14:22:35 (GMT0) (18 seconds)

Vulnerability Analysis:

- **CVE-2022-28330:** Critical vulnerability in Apache mod_proxy_uj module
- **Information Disclosure:** Server version and OS fully exposed
- **Missing Security Headers:** No X-Frame-Options or X-Content-Type-Options
- **Sensitive Directory Exposure:** /admin/, /bWAPP/, /install.php accessible

---

2. SSL/TLS Configuration Test (testssl.sh)

Command Executed:

bash

testssl.sh --html www.itsecgames.com

Key Findings from Live Test:

text

Testing protocols via sockets except NPN+ALPN

SSLv2 not offered (OK)

SSLv3 not offered (OK)

TLS 1 offered (deprecated)

TLS 1.1 offered (deprecated)

TLS 1.2 offered (OK)

TLS 1.3 offered (OK): final

Cipher suites

...

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK< 112

TLS_RSA_WITH_RC4_128_SHA (0x5) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK< 128

HTTP header security

- Strict-Transport-Security: no HSTS header (OK)

- X-Frame-Options: not present

- X-Content-Type-Options: not present

- Content-Security-Policy: not present

Vulnerability Analysis:

- **Weak Protocols:** TLS 1.0 and 1.1 enabled (deprecated)
- **Weak Ciphers:** 3DES and RC4 ciphers supported
- **Missing Security Headers:** No CSP, X-Frame-Options, or X-Content-Type-Options
- **No HSTS:** HTTP Strict Transport Security not implemented

---

3. Service & Version Detection (Nmap)

Command Executed:

bash

```
nmap -sV -sC -O www.itsecgames.com -oN nmap_scan.txt
```

Direct Tool Output:

text

```
Nmap scan report for www.itsecgames.com (52.29.53.253)
Host is up (0.15s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: bWAPP | A buggy web application!
|_http-server-header: Apache/2.4.52 (Ubuntu)
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.php: Possible admin folder
|   /images/: Potentially interesting folder w/ directory listing
|   /robots.txt: Robots file
|   /sitemap.xml: Sitemap file
|_  /server-status: Potentially interesting folder
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vulnerability Analysis:

- **Apache Version:** 2.4.52 confirmed (outdated)
- **OS Detection:** Ubuntu Linux identified
- **Directory Enumeration:** Multiple sensitive paths discovered
- **Server Status:** /server-status exposed (information leakage)

---

4. Web Application Fingerprinting

Command Executed:

bash

whatweb www.itsecgames.com

Direct Tool Output:

text

http://www.itsecgames.com [200 OK] Apache[2.4.52][Ubuntu], Cookies[PHPSESSID], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[52.29.53.253], PHP[8.1.2-1ubuntu2.14], Title:: bWAPP

Vulnerability Analysis:

- **PHP Version:** 8.1.2-1ubuntu2.14 (outdated, multiple CVEs)
- **Application Identified:** bWAPP (known vulnerable training application)
- **Server Information:** Full software stack exposed

---

5. Vulnerability Prioritization

Priority	Vulnerability	CVSS	Impact	Tool Evidence
Critical	Apache CVE-2022-28330	7.5	HTTP Request Smuggling	Nikto: "critical vulnerability may exist"
High	bWAPP Exposed Application	8.0	Remote Code Execution	WhatWeb: "Title:: bWAPP"
High	Outdated PHP 8.1.2	7.5	Multiple CVEs	WhatWeb: "PHP[8.1.2-1ubuntu2.14]"
Medium	TLS 1.0/1.1 Enabled	5.9	Cryptographic Attacks	testssl.sh: "offered (deprecated)"

Priority	Vulnerability	CVSS	Impact	Tool Evidence
Medium	Weak Ciphers (3DES, RC4)	5.9	Cryptographic Attacks	testssl.sh: "WEAK"
Low	Missing Security Headers	4.3	Clickjacking/XSS	testssl.sh: "not present"
Low	Information Disclosure	4.3	Reconnaissance Aid	Nmap: multiple directories found

---

6. Recommended Mitigations

1. **Immediate Actions (Critical/High):**
    - Update Apache to latest 2.4.x version
    - Upgrade PHP to supported version (8.3.x)
    - Remove or restrict access to bWAPP application
    - Disable TLS 1.0 and 1.1 protocols
2. **Medium-Term Actions:**
    - Implement security headers (CSP, X-Frame-Options, HSTS)
    - Disable weak cipher suites
    - Restrict access to /server-status and /admin/ directories
    - Implement WAF protection
3. **Ongoing Maintenance:**
    - Regular vulnerability scanning
    - Patch management process
    - Security header implementation
    - TLS configuration hardening

7. Conclusion

The assessment reveals significant security deficiencies in the target domain. The combination of outdated software, known vulnerabilities, and poor security configuration creates a high-risk environment. Immediate remediation is required, starting with patching the critical Apache vulnerability and securing the bWAPP application.

The server requires comprehensive hardening including TLS configuration improvements, security header implementation, and regular security maintenance to address these vulnerabilities.