Security Assessment Report

www.itsecgames.com/

Mohit Sharma

mohit.sh515@gmail.com

22 September, 2025

Executive summary

This assessment evaluated the externally facing security posture of http://www.itsecgames.com/ using passive reconnaissance, active scanning, automated vulnerability tools, directory discovery, and safe manual validation. The site hosts **bWAPP (a deliberately vulnerable web application)** and shows multiple information-disclosure and configuration issues. The most critical findings are:

- **Publicly accessible backup/archive** (indicated by Nikto) — immediate removal recommended.
- **Outdated SSH server banner (OpenSSH_6.7p1) visible** — high risk; update SSH and harden.
- **Missing security headers** (X-Frame-Options, X-Content-Type-Options, CSP absent) medium risk; add headers.

This report documents the steps performed, evidence captured, prioritized findings, and actionable remediation guidance.

Scope and rules

- **Scope:** Only http://www.itsecgames.com/ (no other hosts).
- **Testing policy:** Non-exploitative; passive and active discovery allowed; no unauthorized credential use, no brute-force, no destructive exploitation.
- **Tools used:** whois, dig, host, whatweb, curl, nmap (multiple scans), nikto, gobuster, openssl, ssh (banner probe), OWASP ZAP (scan/export), manual curl checks.

Methodology (summary)

1. **Passive reconnaissance:** WHOIS, DNS lookups, web page inspection and header collection.
2. **Active reconnaissance:** Nmap service/version scans, OS fingerprinting attempts, NSE scripts.
3. **Automated web scanning:** Nikto for common web issues; OWASP ZAP automated scan.
4. **Directory discovery:** gobuster (fast list), robots/sitemap inspection, manual file checks.
5. **Safe manual validation:** confirmable findings with benign probes, SSL certificate check, SSH banner probe.
6. **Prioritization & remediation:** classify findings (High/Medium/Low) and propose fixes.

Findings

Evidence: full raw outputs and screenshots are included as attachments in the submission (tool outputs and screenshots). See Appendix for file references.

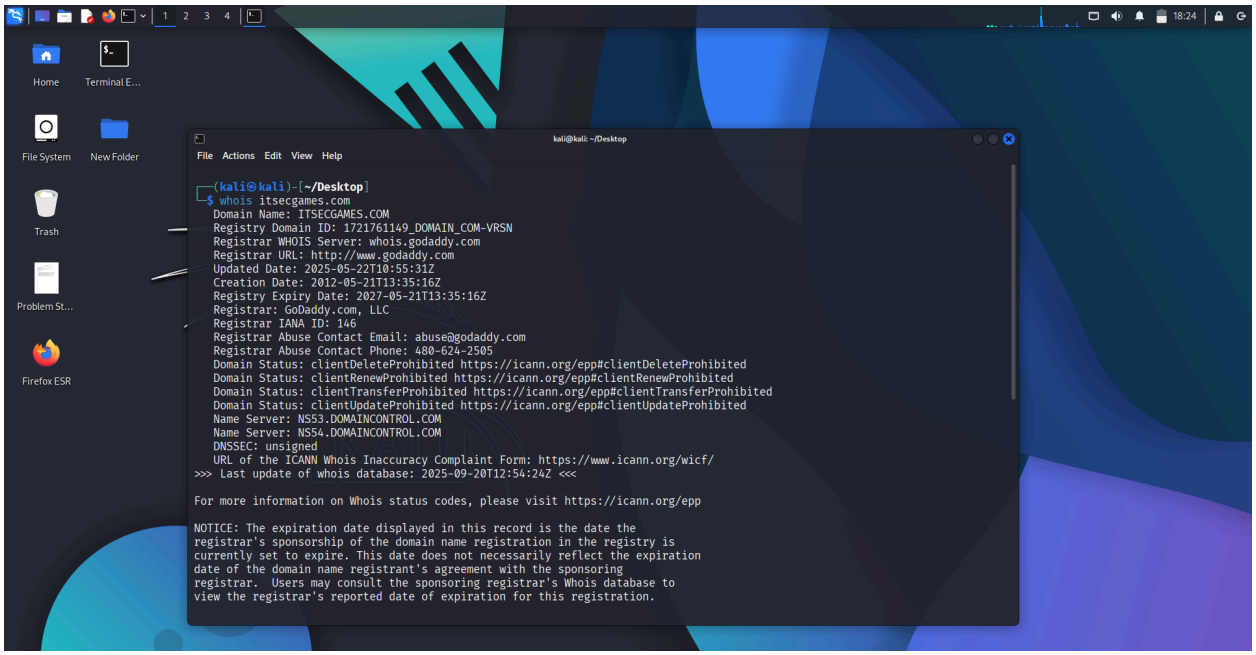
1) Passive reconnaissance

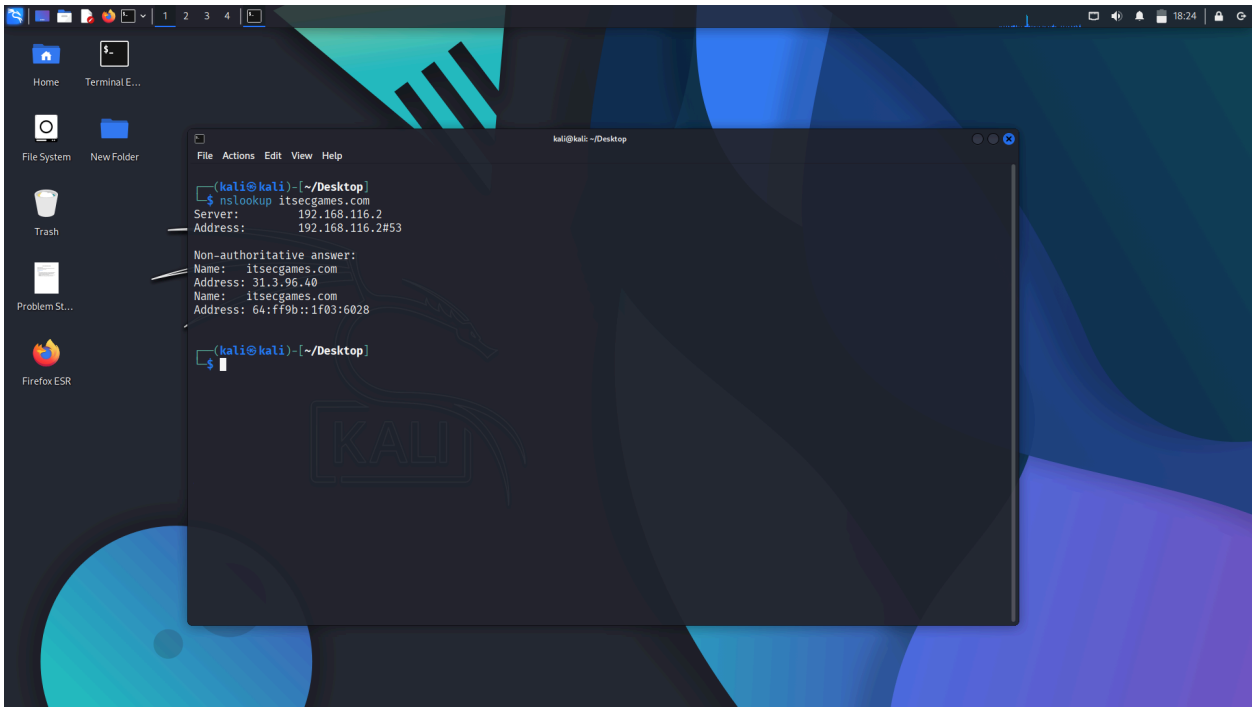
What was done: whois, dig/host/nslookup, whatweb, curl -I, robots/sitemap retrieval.

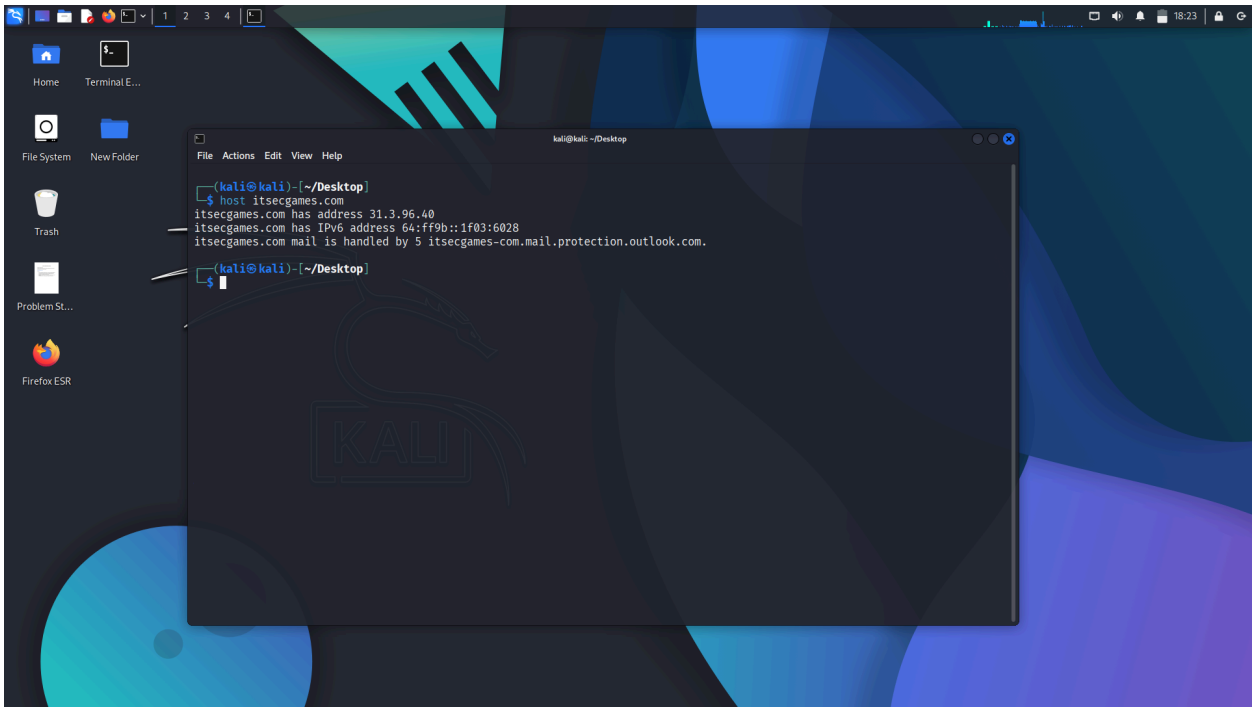
Key observations:

- Registrar: **GoDaddy.com, LLC**; domain created 2012, expires 2027.
- IP: **31.3.96.40** (reverse DNS `web.mmebvba.com`) with an IPv6 mapped address present.
- The title shows **"bWAPP, a buggy web application!"** indicates this host intentionally exposes vulnerabilities for training.
- HTTP headers leak server type: `Server: Apache`. `Last Modified` indicates content last touched 09 Feb 2022.
- `robots.txt` and `sitemap.xml` exist (useful for recon; may list internal paths).

Evidence: Passive recon screenshots and `whois`, `whatweb`, `curl -I` outputs (included).




kali@kali: ~/Desktop
File Actions Edit View Help
┌──(kali㉿kali)-[~/Desktop]
└─$ nslookup itsecgames.com
Server: 192.168.116.2
Address: 192.168.116.2#53
Non-authoritative answer:
Name: itsecgames.com
Address: 31.3.96.40
Name: itsecgames.com
Address: 64:ff9b::1f03:6028
┌──(kali㉿kali)-[~/Desktop]
└─$


kali@kali: ~/Desktop
File Actions Edit View Help
┌──(kali㉿kali)-[~/Desktop]
└─$ host itsecgames.com
itsecgames.com has address 31.3.96.40
itsecgames.com has IPv6 address 64:ff9b::1f03:6028
itsecgames.com mail is handled by 5 itsecgames-com.mail.protection.outlook.com.
┌──(kali㉿kali)-[~/Desktop]
└─$

2) Active reconnaissance (Nmap)

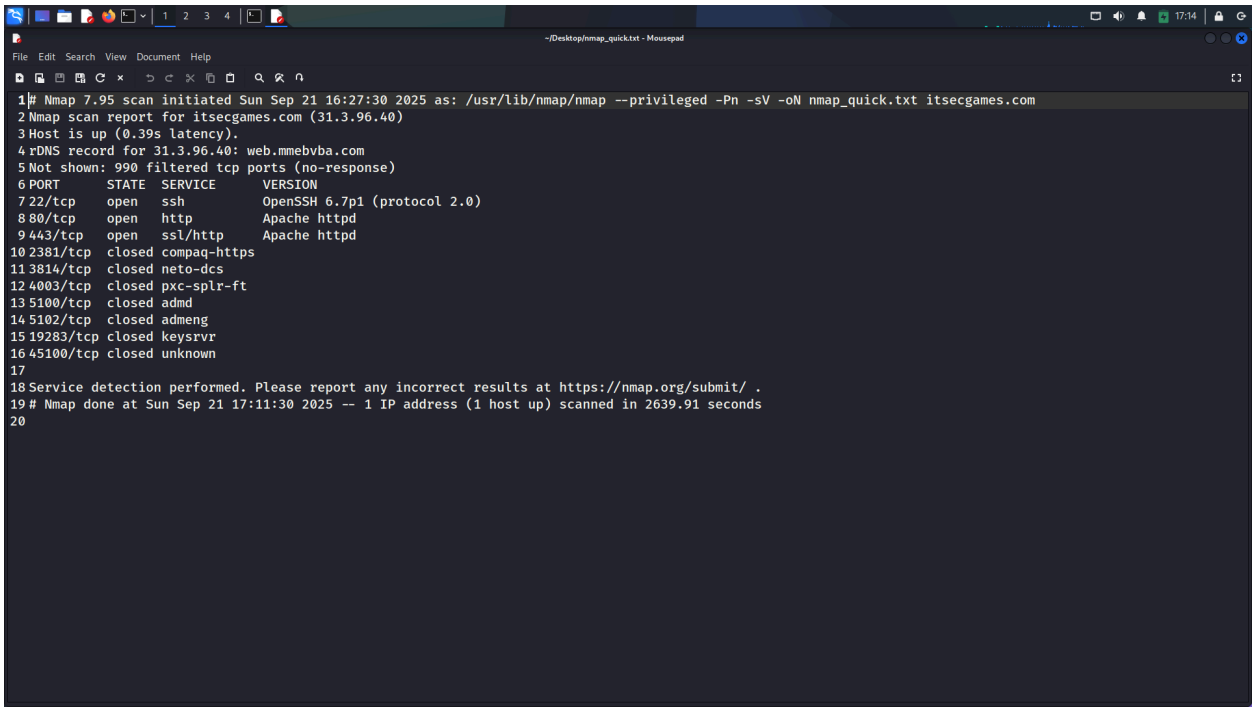
Commands used: `nmap -Pn -sV itsecgames.com`, `nmap -Pn -sV -O itsecgames.com`, `nmap -Pn --script=vuln itsecgames.com`, `nmap -Pn -sV --top-ports 5000 itsecgames.com`.

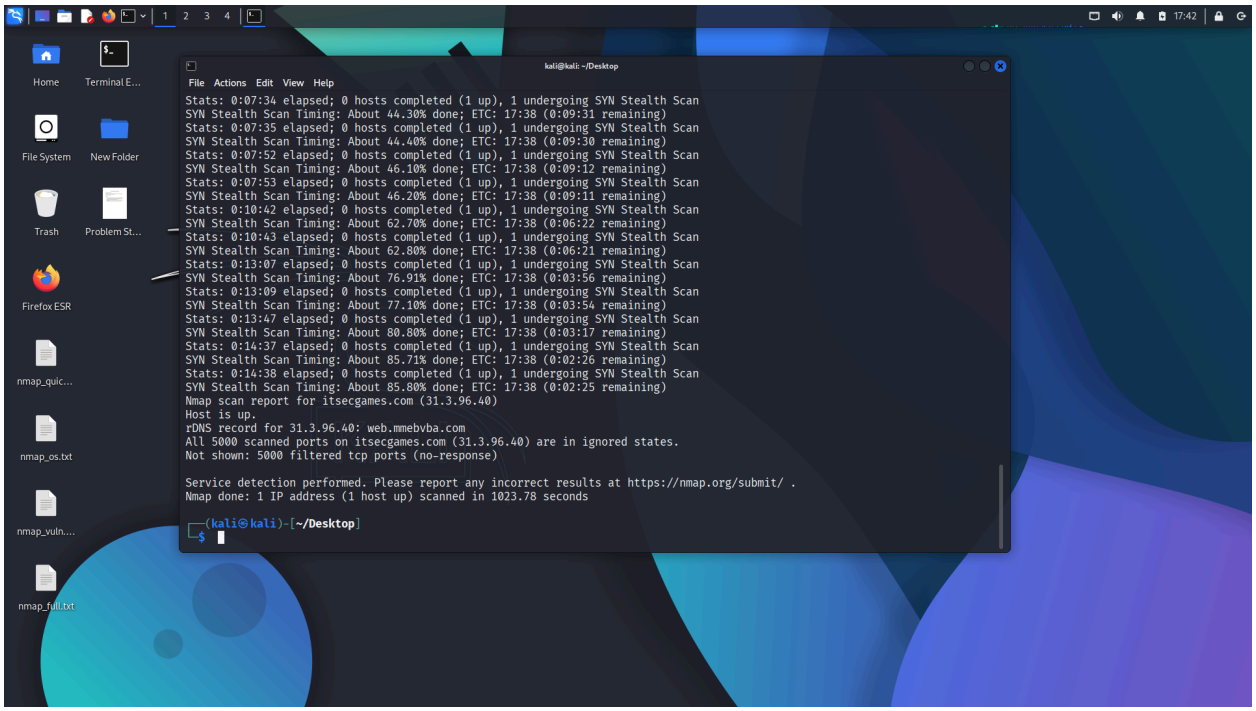
Findings:

- **Open ports:** 22/tcp (SSH — OpenSSH_6.7p1), 80/tcp (HTTP — Apache httpd), 443/tcp (HTTPS — Apache httpd).
- **Most other ports filtered** by firewall many scans returned 'filtered' for top 1000/5000 ports.
- **OS detection is inconclusive** due to lack of varied open/closed ports.
- **NSE vuln scripts returned no actionable results** (likely due to filtering or host hardening).

Impact: Visible outdated SSH banner is a high risk if the server is actually running an outdated OpenSSH version. Web server exposure requires web-level hardening.

Evidence: `nmap_quick.txt`, `nmap_full.txt`, `nmap_os.txt`, `nmap_vuln.txt` (screenshots and raw outputs included).





---

3) Web vulnerability scanning (Nikto + ZAP)

Nikto (partial run): produced the following notable results:

- Missing anti-clickjacking header: **X-Frame-Options**.
- Missing **X-Content-Type-Options** header.
- **ETag header present** with inode-like value → potential information disclosure (CVE-2003-1418).
- Nikto flagged an exposed path `/31.3.96.40.tar.bz2` with **Drupal 7** `X-Generator` headers (archive likely contains site files/backups).

OWASP ZAP (Checkmarx) report: (generated and attached)

- Alerts summary: 3 alerts (two medium, one low).
- Medium: **CSP Header Not Set** (found via robots.txt in passive scan).
- Medium: **Missing Anti-clickjacking Header**.
- Low: **X-Content-Type-Options Header Missing**.

Impact: Missing headers enable client-side attacks such as clickjacking, MIME-type attacks, and increase XSS risk if combined with reflected input. Exposed backup file may contain sensitive data.

Evidence: `nikto_report.txt` (partial) and `ZAP by Checkmarx Scanning Report.pdf` are included.

ZAP by Checkmarx Scanning Report.pdf

---

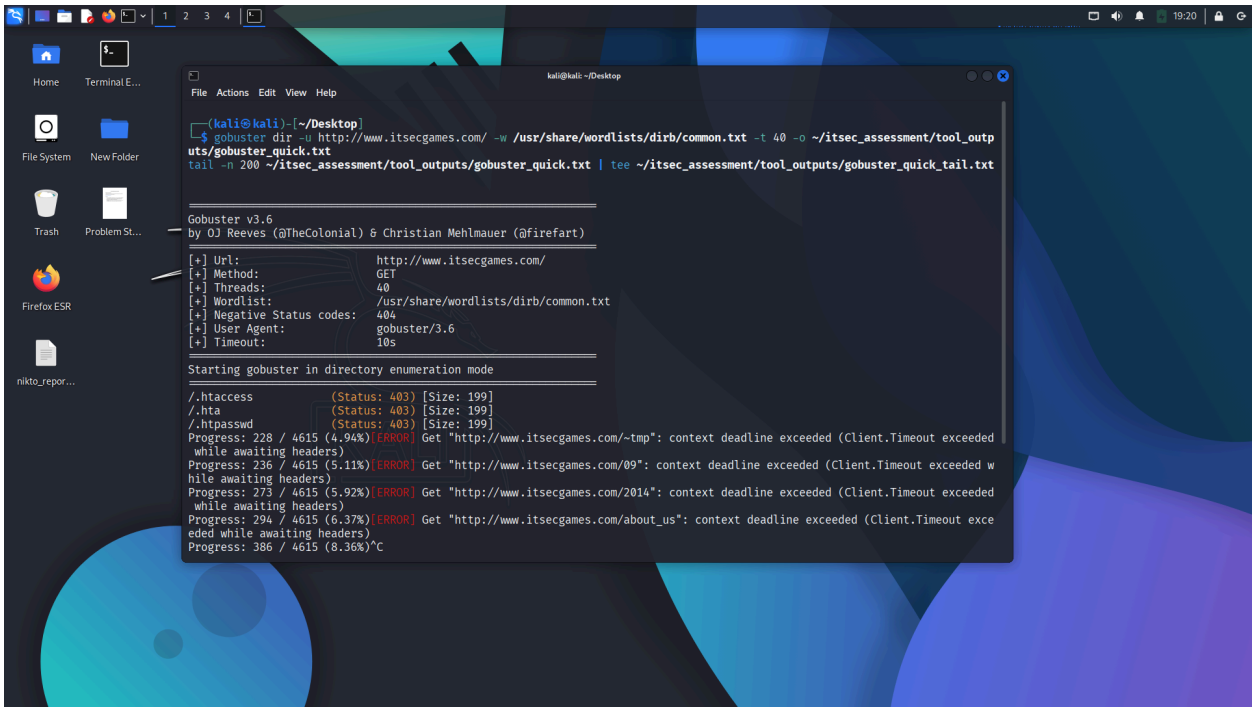
4) Directory discovery & configuration checks

What was done: gobuster quick run, manual checks for common files (`.env`, `config.php`, `phpinfo.php`, admin endpoints), robots/sitemap review, HTTP OPTIONS.

Findings:

- `robots.txt` present (contains disallowed entries; see Appendix).
- Several common checks returned HTTP 404 (phpinfo.php, admin.php, etc.), while `.htpasswd` and `.htaccess` returned 403 (protected) good.
- Gobuster quick found `.hta`, `.htpasswd`, `.htaccess` entries returning 403 (expected).
- HTTP `Allow:` header lists `POST, OPTIONS, GET, HEAD` (no dangerous methods like PUT/DELETE allowed).

Evidence: directory scan output, `admin_checks`, `config_checks`, `gobuster_quick.txt` and screenshots included.



---

5) Safe manual validation

SSH banner probe: a benign banner probe confirmed remote software string **OpenSSH_6.7p1** (server returned remote software version) captured via ssh debug output.

SSL certificate check: certificate issued by Let's Encrypt (issuer R10), valid `notBefore=Aug 6 2025` to `notAfter=Nov 4 2025` a valid certificate in-place.

Archive check: attempted access to `/31.3.96.40.tar.bz2` returned **HTTP 404 Not Found** in the final probe (Nikto earlier saw a reference/header; final HEAD returned 404). Do not download or extract archive; presence was flagged and should be investigated by the owner.

Reflected input checks: benign marker probes showed reflection in certain pages (manual reflection artifacts captured); this indicates input echoing that could be vulnerable to XSS if not properly sanitized.

Evidence: `ssh_banner_probe.txt`, `ssl_info.txt`, manual reflection files and screenshots.

Prioritized findings (table)

ID	Finding	Resource	Severity	Evidence	Recommendation (Immediate/Short/Long)
V-01	Outdated OpenSSH banner (OpenSSH_6.7p1)	SSH – 31.3.96.40:22	High	nmap_quick.txt, ssh_banner_probe.txt, screenshot	Immediate: Upgrade OpenSSH; disable root login; enforce key auth; enable fail2ban.
V-02	Exposed archive / backup referenced (/31.3.96.40.tar.bz2)	/31.3.96.40.tar.bz2 (historical/flagged)	High	nikto_report.txt, manual tarball_head.txt	Immediate: Remove backups from webroot; validate archive contents for credentials; rotate secrets if found.
V-03	Missing security headers (X-Frame-Options, X-Content-Ty	http://www.itsecgames.com/ (homepage)	Medium	nikto_report.txt, ZAP report, screenshots	Short: Add recommended headers; implement CSP and HSTS after

	pe-Options, CSP absent)				HTTPS enforced.
V-04	Reflected input (benign marker observed)	Certain query parameters/pages	Medi um	manual_reflectio n.html, screenshots	Short: Apply input validation and output encoding; use CSP.
V-05	ETag header reveals inode-like values	HTTP headers on /	Low	nikto_report.txt, curl_headers.txt	Routine: Disable ETag (FileETag None) or normalize ETag; hide server tokens.
V-06	bWAPP demo app visible (intentional vulnerable app)	Homepage title / content	Info	whatweb output, screenshots	Info: If this is a training instance, leave in lab; if production, remove demo apps and harden.

Prioritized list of findings & recommendations

1. **Outdated OpenSSH banner (High)**
    - *Risk:* May expose known exploits if version is truly outdated.
    - *Recommendation:* Upgrade OpenSSH; disable root login; enforce key-based authentication; enable account lockout and monitoring.
2. **Exposed archive / backup reference (High)**
    - *Risk:* Sensitive files or credentials may leak if accessible.
    - *Recommendation:* Immediately remove backup archives from webroot; secure backup storage; rotate credentials if exposed.
3. **Missing security headers (Medium)**
    - *Risk:* Enables clickjacking, MIME-sniffing, and XSS risk.
    - *Recommendation:* Add standard headers (X-Frame-Options, X-Content-Type-Options, Content-Security-Policy, Strict-Transport-Security).
4. **Reflected input (Medium)**
    - *Risk:* Potential XSS vector if combined with poor sanitization.
    - *Recommendation:* Implement input validation, output encoding, and a strict Content Security Policy.
5. **ETag header information disclosure (Low)**
    - *Risk:* Reveals inode/file system details that can assist attackers.
    - *Recommendation:* Disable or normalize ETag; limit server tokens.
6. **bWAPP demo application visible (Informational)**
    - *Risk:* Demonstrates intentional vulnerabilities; unsafe if left in production.
    - *Recommendation:* Keep isolated in a training lab; remove from production environments.

Note:

This assessment was performed following assignment constraints: testing was non-destructive and limited to http://www.itsecgames.com/. The presence of bWAPP confirms this is a purposely vulnerable application; findings like reflected input are expected in such a lab. However, configuration issues (headers, archives, visible banners) remain relevant and should be addressed in any real-world deployment.