Prioritized Vulnerability Findings & Mitigation Report

Target: www.itsecgames.com

Priority	Finding	Impact	CVSS	Evidence	Recommended Mitigation
Critical	**Outdated PHP Version (8.1.2)**	PHP 8.1.2 is End-of-Life (EOL) and contains unpatched vulnerabilities, including critical CVEs leading to **Remote Code Execution**.	9.8+	X-Powered-By: PHP/8.1.2-1ubuntu2.14	**1. Immediately upgrade PHP** to a supported version (8.3.x). **2. Disable the** X-Powered-By **header** by setting expose_php = Off in php.ini.
Critical	**Known Vulnerable Application (bWAPP)**	The presence of this intentionally vulnerable app on the public internet provides a low-barrier entry point for full server compromise.	8.0+	Page title, <!-- bWAPP, version 2.2 --> comment	**1. If not required:** Remove it from the production server immediately. **2. If required:** Isolate it on a separate network segment behind a firewall with strict IP whitelisting and Multi-Factor Authentication (MFA).

Priority	Finding	Impact	CVSS	Evidence	Recommended Mitigation
High	**Outdated Apache Server (CVE-2022-28330)**	Apache 2.4.52 is vulnerable to HTTP Request Smuggling (CVE-2022-28330), allowing cache poisoning, session hijacking, and security control bypass.	7.5	Server: Apache/2.4.52 (Ubuntu), Nikto scan	**Apply latest OS security patches** to upgrade Apache to the most recent version in the 2.4.x branch (e.g., 2.4.58+).
High	**Support for Deprecated TLS Protocols**	TLS 1.0 and 1.1 are enabled. They contain known vulnerabilities (e.g., BEAST) and fail compliance standards (PCI DSS).	5.9	testssl.sh protocol check	**Disable TLS 1.0 and TLS 1.1** in the web server's SSL configuration. Allow only TLS 1.2 and 1.3.
Medium	**Information Disclosure via Headers**	The server banner reveals exact Apache version and OS. The PHP banner reveals the exact EOL version, allowing	4.3	Server and X-Powered-By headers	**1. Configure Apache:** Set ServerTokens Prod and ServerSignature Off. **2. Configure PHP:** Set expose_php = Off.

Priority	Finding	Impact	CVSS	Evidence	Recommended Mitigation
		precise exploit targeting.			
Medium	**Weak SSL/TLS Cipher Suites**	The server supports weak ciphers (3DES, RC4), which provide inadequate encryption and are vulnerable to cryptographic attacks.	5.9	testssl.sh cipher list	**Harden the cipher suite list.** Disable weak ciphers (RC4, 3DES, NULL, EXPORT). Prefer modern, strong ciphers (e.g., AES-GCM).
Medium	**Missing HTTP Security Headers**	The absence of key security headers increases exposure to client-side attacks like clickjacking, MIME-sniffing, and XSS.	4.3	testssl.sh, Nikto scan	**Implement security headers** in the Apache config: • Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains" • Header always set X-Frame-Options "SAMEORIGIN" • Header always set X-Content-Type-Options "nosniff"

Priority	Finding	Impact	CVSS	Evidence	Recommended Mitigation
					• Header always set Content-Security-Policy "default-src 'self';"
Low	**Sensitive Directory Exposure**	Paths like /admin/, /server-status/, and /install.php are publicly accessible, providing additional attack surface.	3.5	Nikto, Nmap http-enum script	**Restrict access** to sensitive paths using Apache's Require ip directive or firewall rules. Block public access to /server-status.
Low	**SSL Certificate Expiration**	The certificate from Let's Encrypt expires on **July 11, 2024**. This will cause a service disruption if not renewed.	2.0	testssl.sh certificate check	**Ensure automatic certificate renewal** (e.g., Certbot) is configured and functioning correctly. Monitor expiration.

Recommended Remediation Timeline

Immediate (Within 24-48 Hours):

1. **Address Critical Findings:** Upgrade PHP and Apache. This is the highest priority to mitigate known, exploitable vulnerabilities.
2. **Isolate or Remove bWAPP:** This application poses an immediate and severe risk.

Short-Term (Within 1 Week):

3. **Harden TLS Configuration:** Disable TLS 1.0/1.1 and weak ciphers.
4. **Suppress Information Headers:** Configure Apache and PHP to stop leaking version information.
5. **Implement Security Headers:** Add HSTS, X-Frame-Options, and CSP headers.

Ongoing Maintenance:

6. **Monitor Certificate Expiration:** Ensure automatic renewal processes are reliable.
7. **Establish a Patch Management Process:** Schedule regular updates for the OS and all software packages to prevent future outdated software vulnerabilities.
8. **Perform Regular Vulnerability Scans:** Conduct weekly or monthly scans using tools like Nikto to detect new misconfigurations.

Conclusion

By addressing these findings in the order of priority outlined, the security posture of www.itsecgames.com will be dramatically improved. The critical actions involve patching the severely outdated software and managing the risk posed by the vulnerable web application. The subsequent hardening steps will then align the server with modern security best practices.