Monthly Report

On VAPT & Infrastructure-Level Security Enhancement for ***Vibe Gaming***

BY Cyberlog Ltd.

October 2025

Table of contents

Vulnerability Assessment and Penetration Testing (VAPT) Final Report

Client: Vibe Gaming

Target: vibegaming.com.bd (Web Application and Hosting Infrastructure)

Assessment Period: 1 month (October 2025)

Assessment Type: Black Box & Gray Box Testing

Date of Submission: December 5, 2025

Prepared By: Cyberlog

Executive Summary

This report summarizes the findings, risk analysis, and remediation recommendations resulting from the VAPT engagement conducted on **vibegaming.com.bd** and its hosting infrastructure (IP Range: 172.67.149.168, 104.21.29.190).

The assessment identified several weaknesses requiring immediate action. The overall security posture is currently rated **MEDIUM-HIGH RISK**, primarily due to critical vulnerabilities (especially **SQL Injection** in a public-facing API and **Cross-Site Scripting**) that could lead to full database compromise, sensitive customer data theft, or complete site defacement. The infrastructure hardening efforts, while partially implemented, require finalization to achieve a secure baseline.

Risk Level	Count	Example Finding	Remediation Priority
Critical	1	SQL Injection via Public API Endpoin	**P1 (Immediate)**
High	2	Reflected Cross-Site Scripting (XSS) & Weak SSL/TLS Ciphers	**P2 (Urgent)**
Medium	3	Outdated WooCommerce Extension/Plugin	**P3 (Scheduled)**
Low	2	Verbose Error Messaging	P4 (Deferred)

Scope and Methodology

2.1. In-Scope Assets

- **Web Application:** `vibegaming.com.bd`
- **Subdomains & APIs:** All public-facing APIs and endpoints under the main domain.
- **Hosting Infrastructure:** Server IP addresses (172.67.149.168, 104.21.29.190) and associated Nginx and Cloudflare configurations.

2.2. Methodology

The assessment followed the methodology outlined in the VAPT proposal, combining both Black Box (external, unauthenticated perspective) and Gray Box (authenticated perspective with test accounts) testing. The testing was aligned with global standards, including OWASP Top 10 2021, SANS Top 25, and PCI DSS v4.0 requirements (due to e-commerce payment handling). Tools utilized included: Burp Suite Professional, Nessus Professional, Nmap, SQLmap, and custom scripts for manual verification and exploitation attempts.

Detailed Findings and Risk Analysis

The findings are categorized by risk level, determined by a combination of CVSS v3.1 Score and Business Impact Analysis.

3.1. Critical Findings (P1 - Immediate Action Required)

Finding 1: SQL Injection (OWASP A01:2021 - Injection)

CVSS Score	Business Impact	Vulnerable Component
9.8 (Critical)	Complete loss of customer data, full site takeover, PCI DSS violation.	API endpoint for dynamic product filtering (`/api/v1/product/filter`).

Description: An input parameter within the public product filtering API endpoint was found to be unsanitized, allowing for the execution of arbitrary SQL commands. Our testers successfully used an authenticated test user to extract non-sensitive database metadata, confirming the vulnerability is exploitable. If exploited by an external attacker, this could lead to the unauthorized viewing, modification, or deletion of all data, including customer records and administrator hashes.

Recommendation: Implement strict **input validation** and **parameterized queries** (prepared statements) for all database interactions. The application layer must not construct SQL queries using direct user input concatenation.

3.2. High Findings (P2 - Urgent Action Required)

Finding 2: Reflected Cross-Site Scripting (XSS) (OWASP A03:2021 - Injection)

CVSS Score	Business Impact	Vulnerable Component
8.0 (High)	Session hijacking, customer account compromise, malware delivery via infected search results.	The site’s main search function and unauthenticated comment forms.

Description: The application fails to properly sanitize or encode user-supplied input before reflecting it back to the browser in the search results page. A malicious script injected into the search query can be executed in the victim's browser, potentially leading to session cookie theft (allowing account takeover) or redirection to a phishing site.

Recommendation: Implement **output encoding** for all user-controllable data before it is rendered on the HTML page. Ensure that HTTP headers are set to prevent XSS (**Content-Security-Policy**).

Finding 3: Weak SSL/TLS Cipher Suites

CVSS Score	Business Impact	Vulnerable Component
7.5 (High)	Data interception, failure to meet PCI DSS requirements.	Nginx Server Configuration (Port 443).

Description: The Nginx configuration supports outdated and weak SSL/TLS cipher suites (e.g., CBC-mode ciphers). While the Cloudflare layer provides initial protection, the origin server remains vulnerable to downgrade attacks if accessed directly or if a local user is targeted.

Recommendation: Update the Nginx configuration to disable support for **TLS 1.0 and TLS 1.1** and remove all weak cipher suites. Configure the server to prioritize modern, strong ciphers (e.g., **AES-256-GCM**).

3.3. Medium Findings (P3 - Scheduled Action Required)

Finding 4: Outdated WooCommerce Extension

CVSS Score	Business Impact	Vulnerable Component
6.5 (Medium)	Denial of Service, potential unauthorized access to product inventory or pricing.	WooCommerce "Inventory Sync" Extension (Version 2.3.1).

Description: The Inventory Sync extension is running a version with a publicly known vulnerability (CVE-20XX-XXXXX) that permits low-privilege users to lock up administrative pages via a resource exhaustion bug. This poses a threat to administrative stability and site maintenance.

Recommendation: Immediately update the **WooCommerce Inventory Sync Extension to the latest stable version**. If an update is not available, isolate the plugin using a dedicated WAF rule until it can be replaced.

4. Remediation Roadmap and Revalidation

We recommend that Vibe Gaming prioritize the remediation efforts based on the risk levels identified above.

Priority	Finding ID	Remediation Plan	Estimated Effort
P1	SQL Injection (F1)	Implement parameterized queries and robust server-side input validation.	1 Week
P2	XSS (F2)	Apply output encoding for all search and comment functions; deploy Content-Security-Policy header.	3 Days
P2	Weak TLS (F3)	Update Nginx configuration to support only TLS 1.2+ and strong cipher suites.	1 Day
P3	Outdated Plugin (F4)	Patch or replace the vulnerable WooCommerce Inventory Sync Extension.	1 Day

Revalidation

As per the agreement, Cyberlog includes **two free revalidation rounds** within two months of the final report submission. We strongly recommend scheduling the first revalidation scan immediately after all P1 and P2 findings have been addressed to confirm the effectiveness of the patches.

Next Steps:

1. **Client Review: The** Vibe Gaming team reviews the findings and planned remediation actions.
2. **Cyberlog Consulting:** We are available for a detailed technical workshop to discuss the remediation steps with your development team.
3. **Remediation & Patching:** Client implements the fixes.
4. **Revalidation:** Cyberlog conducts the first re-test to confirm all vulnerabilities are closed.

Thank You