## 

## 

Proposal for

Vulnerability Assessment and Penetration Testing (VAPT) and

Infrastructure-Level Security Enhancement for

**vibegaming.com.bd**

## 

| Project Title | : | Proposal for Vulnerability Assessment and Penetration Testing (VAPT)  and Infrastructure-Level Security Enhancement |
| --- | --- | --- |
| Project For | : | Vibe Gaming |
| Managed By | : | Cyberlog |
| Executed By | : | Cyberlog |
| Starting Date | : | Immediate |

**Table of contents**

[**Introduction 2**](#_1925qjf4vo3o)

[**Purpose of Our Work 2**](#_inx3nxhib9r9)

[Purpose of the VAPT Engagement 2](#_ajhqrp9z1l67)

[Purpose of Infrastructure-Level Security Enhancements 2](#_on58jcsqxq4a)

[**Level of Criticality 3**](#_7lup5um9pt7o)

[Why VAPT Is Critical for vibegaming.com.bd 3](#_2637o8h4iyfe)

[Why Infrastructure Security is Crucial for vibegaming.com.bd 3](#_w8y51o7stp0w)

[**Objectives: 3**](#_w7fps647qpzu)

[**In-Scope of the Work: 4**](#_whl1hovjp0da)

[For VAPT 4](#_pkebqkf0g50o)

[For Infrastructure Security 4](#_qjzv04oyo7l)

[**Our Approaches for VAPT 4**](#_jdyflxt6yc3)

[▪ Vulnerability Assessment (VA): 4](#_kibe1ewoywed)

[▪ Penetration Testing (PT): 5](#_r04zb0ngzxw9)

[Black Box Testing: 5](#_efznuweypvs9)

[Gray Box Testing: 5](#_pt7zdmceegsr)

[**Our Approaches for Infrastructure Security 6**](#_w7vw384hmwc)

[**Methodology 6**](#_582swav6unq9)

[Stages of VAPT 6](#_v5tl1dnw5qol)

[Stages of Infrastructure Security 7](#_15cagkdfn1mw)

[**Project Management Plan 7**](#_4ip3ej4ih5z3)

[**Deliverables 8**](#_ktss8arm1cz8)

[For VAPT 8](#_b4esfcozutfe)

[For Infrastructure Security 8](#_67rf6rc14vci)

[**Other Important Issues 8**](#_m7lcvu8gi46b)

[**List of Tools to be Used for VAPT 9**](#_996glsg76iv9)

[Licensed Tools 9](#_g3c8ujorfq0d)

[Reconnaissance and Information Gathering 9](#_46m5feocddt)

[Vulnerability and Scanning 9](#_iv4kn11j5g0z)

[Web Application Security Testing 9](#_1323clxwcjoe)

[API and Web Application Security 10](#_pr84b4mekv4n)

[Network and Infrastructure Testing 10](#_yt3q5fdu5tv2)

[Exploration and Privilege Acceleration 10](#_evadnfx15rhz)

[Own Script 10](#_ow4464oh0kud)

[**List of Tools to be Used for Infrastructure Security 10**](#_4eagzf6ffha)

[**Financial Proposal 11**](#_dkwo74kgqnmc)

[**Payment Terms & Conditions 12**](#_glxprr56i9eo)

[**Conclusion 12**](#_q5eqyq7umoht)

# Introduction

In today’s evolving cyber threat landscape, securing digital infrastructure is paramount for safeguarding sensitive information, ensuring service availability, and maintaining stakeholder trust. While Vulnerability Assessment and Penetration Testing (VAPT) identifies existing weaknesses, infrastructure-level security enhancements are essential to proactively fortify systems against both known and emerging threats.

This proposal outlines the measures to be implemented at the infrastructure and network level to enhance the overall cybersecurity posture.

# Purpose of Our Work

## Purpose of the VAPT Engagement

This Vulnerability Assessment and Penetration Testing (VAPT) engagement is initiated to evaluate the security posture of vibegaming.com.bd, identify technical vulnerabilities, and simulate real-world attack scenarios in a controlled environment. The ultimate goal is to:

* Identify vulnerabilities in the application, server configurations, plugins, and APIs.
* Simulate potential exploitation scenarios without causing harm or disruption.
* Assess the risk impact of vulnerabilities to the business, its data, and its users.
* Deliver clear, prioritized, and actionable recommendations for remediation.
* Support compliance with cybersecurity standards such as OWASP Top 10, PCI-DSS (for eCommerce), and ISO 27001.

## Purpose of Infrastructure-Level Security Enhancements

The purpose is to strengthen the organization’s core IT environment by deploying layered defenses across firewalls, servers, operating systems, and applications. These measures aim to:

* Reduce the risk of unauthorized access and data breaches.
* Ensure resilience against Distributed Denial of Service (DDoS) attacks and malicious traffic.
* Enforce standardized security configurations across servers and networks.
* Improve regulatory and compliance readiness.

# Level of Criticality

## Why VAPT Is Critical for Vibe Gaming

## As an eCommerce website, vibegaming.com.bd is a high-value target for threat actors aiming to:

* Steal sensitive customer data (user accounts, emails, payment details, etc.).
* Inject malicious scripts (e.g., card skimmers, redirectors).
* Deface the site or take control of the administrative interface.
* Disrupt online transactions or manipulate product listings.

Given the use of open-source components like WordPress, WooCommerce, and various JavaScript libraries and CDN-based assets, the attack surface can grow rapidly if not managed securely. Additionally, integrations such as Elementor, RankMath SEO, Google Site Kit, and Cloudflare offer both functionality and potential vulnerabilities if misconfigured or outdated. VAPT exercises help ensure that the platform remains resilient against evolving threats by proactively identifying and remediating security weaknesses before they can be exploited.

## Why Infrastructure Security is Crucial for vibegaming.com.bd

Our client relies on uninterrupted IT services to operate efficiently. Without robust infrastructure-level controls:

* Systems remain vulnerable to targeted cyberattacks.
* Cloud-based resources could be disrupted, impacting availability.
* Application-level security may fail if underlying OS or firewall configurations are weak.
* Compliance failures could lead to reputational and financial loss.

By implementing infrastructure security enhancements, we ensure a secure, resilient, and future-ready IT environment.

# Objectives:

The main objectives of this VAPT engagement are:

◻ Identify Security Weaknesses: Detect vulnerabilities across the web application in the domain listed.

◻ Assess Exploitation Feasibility: Conduct controlled penetration testing to validate whether vulnerabilities can be exploited, simulating real-world attack scenarios.

◻ Evaluate Infrastructure & Applications: Review URL and backend servers for misconfigurations, weak authentication, injection flaws, insecure APIs, and compliance gaps.

◻ Provide Risk Prioritization: Assign severity levels (Critical/High/Medium/Low) to vulnerabilities with CVSS scoring and business impact mapping.

◻ Ensure Compliance Alignment: Validate security against best practices and international frameworks such as OWASP Top 10, SANS Top 25, ISO/IEC 27001, NIST SP 800-115, and PCI DSS v4.0.

◻ Actionable Remediation Roadmap: Deliver practical recommendations, remediation guidelines, and verification of fixes to strengthen security posture.

# In-Scope of the Work:

## For VAPT

| **Category** | **Description** |
| --- | --- |
| Web Application | vibegaming.com.bd |
| Subdomains | All subdomains |
| API Endpoints | All APIs under the main domain |
| Hosting Infra | IP Range: 172.67.149.168, 104.21.29.190 |

## 

## For Infrastructure Security

* Cloudflare Firewall Policy Update
  + Configure firewall rules for rate limiting, IP blocking, and DDoS protection.
  + Recommend upgrading to the Cloudflare Pro plan for enhanced features.
* Nginx Security Policy Hardening
  + Apply ModSecurity or equivalent WAF (Web Application Firewall) rules.
  + Harden HTTP headers, TLS/SSL configurations, and request filtering.
* Operating System Security Policy Update
  + Implement firewall policies (iptables, UFW).
  + Secure SSH configurations and disable unused services.
  + Enforce audit logging and system monitoring.
* Application-Level Security (Post-VAPT)
  + Integrate findings from the VAPT into application security updates.
  + Ensure secure coding practices and deployment controls.
* Theme development, plugin development, and WooCommerce development are the main areas of WordPress development.

# Our Approaches for VAPT

Here's a breakdown of the two main components of VAPT:

## ▪ Vulnerability Assessment (VA):

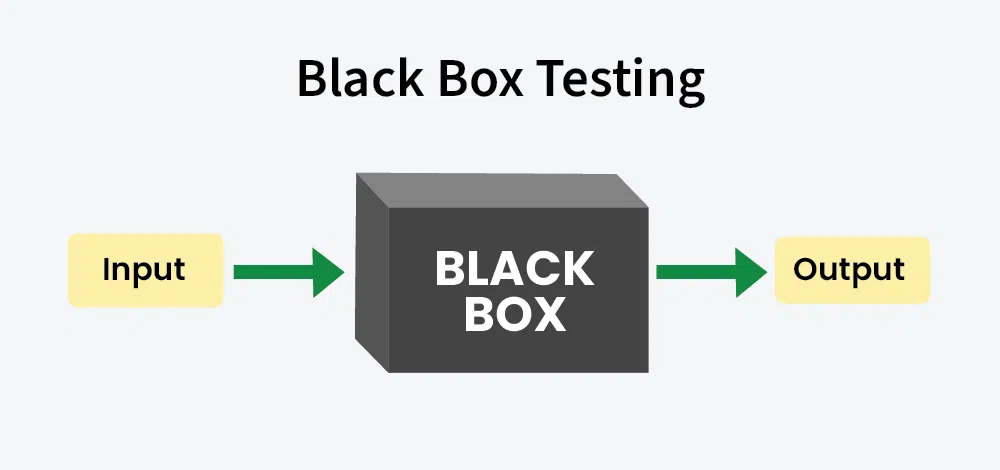
This involves systematically scanning and analyzing systems, applications, and networks to identify potential security weaknesses or vulnerabilities. Vulnerability assessment tools are used to automate the process of identifying known vulnerabilities in software and systems. These assessments provide a baseline understanding of an organization's security posture and help prioritize which vulnerabilities should be addressed first.

## ▪ Penetration Testing (PT):

Also known as ethical hacking, penetration testing involves simulating real-world attacks on a system or network to identify potential entry points and exploit vulnerabilities. Penetration testers, also known as ethical hackers, attempt to actively exploit vulnerabilities to understand the potential impact and the extent of a successful attack. This process helps organizations understand the practical risks associated with the identified vulnerabilities and the potential consequences of a security breach.

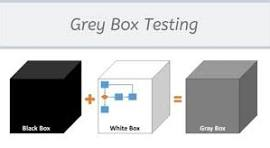
## Black Box Testing:

In Black Box testing, the tester does not know the internal workings of the system being tested. It focuses on testing the functionality and behavior of the application from an end-user perspective. Testers typically use specifications, requirements, and design documents to design test cases. The goal is to identify whether the application behaves correctly and meets its requirements.



## Gray Box Testing:

Gray-Box Testing is a combination of both Black Box and White Box testing. Testers have partial knowledge of the internal workings of the system, such as access to the code or architecture documentation. This approach aims to simulate the knowledge an attacker might have while still benefiting from insights into the internal code.



# Our Approaches for Infrastructure Security

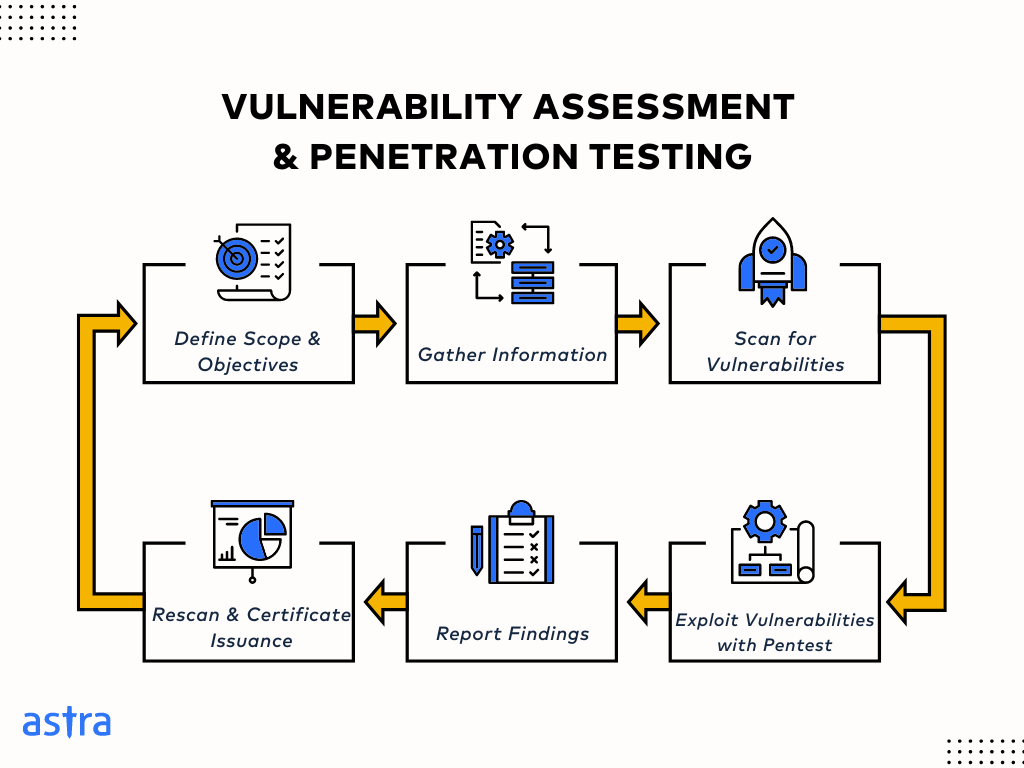
We adopt a layered defense-in-depth strategy that combines proactive configurations, continuous monitoring, and adaptive controls. Our approach ensures:

* Systematic hardening at each layer (cloud, network, OS, application).
* Compatibility with the existing IT environment.
* Compliance alignment with industry best practices (OWASP, NIST, ISO 27001).

# Methodology

## Stages of VAPT

Vulnerability Assessment and Penetration Testing (VAPT) is usually carried out in a series of well-defined stages. It begins with **planning and scoping**, where the objectives, assets, and boundaries of the assessment are agreed upon, and legal permissions are obtained. Next comes **information gathering (reconnaissance)**, during which testers collect data about the target—such as IP addresses, DNS records, technology stack, open ports, and any publicly available information—to understand the environment. Based on what they find, they move to **threat modeling and vulnerability identification**, mapping potential attack surfaces and using a mix of automated tools and manual techniques to detect weaknesses like misconfigurations, missing patches, or insecure code. The process then advances to **exploitation**, where testers attempt to actively leverage those vulnerabilities—through methods such as SQL injection, cross-site scripting, or privilege escalation—to evaluate real-world risk. After exploitation, **post-exploitation** activities help determine how far an attacker could go if the weakness were abused, such as gaining higher privileges or moving laterally across systems. Once testing is complete, a clear **report** is produced, containing an executive summary, detailed technical findings, risk ratings, and recommended remediation measures. Finally, after the issues are fixed, a **remediation and re-testing** phase ensures that all patches and configuration changes have been applied correctly, closing the loop on the VAPT cycle.



## Stages of Infrastructure Security

Stages of Implementation

* Assessment Stage – Review current infrastructure policies and gaps.
* Design Stage – Define updated firewall, OS, and security configurations.
* Implementation Stage – Apply security configurations in a controlled manner.
* Testing Stage – Validate rules, perform controlled attack simulations.
* Handover & Training—Document policies and train the client’s technical staff.

# Project Management Plan

The project management plan for the Technical Proposal for Vulnerability Assessment and Penetration Testing (VAPT) & Infrastructure Security aims to ensure a seamless, efficient, and effective assessment process. This plan outlines a strategic approach to managing the VAPT consultancy from initiation to completion, emphasizing clear timelines, defined roles and responsibilities, and effective communication channels.

Proposed Time Schedule for the Engagement

| **Activities** | **Working Days** |
| --- | --- |
| Kick-off Meeting, Scope Identification & Validation, Team Formation, and The VAPT Plan Document. | 01 |
| Engagement in the Data Collection & Information Gathering, performing both automated and manual vulnerability assessment and penetration testing, and system examinations as outlined in the scope. | 15 |
| Report Development, Sharing Draft Report, Feedback from the Stakeholders Team, and Issuing the Final Report |
| Performing the revalidation after fixing the observations by the concerned stakeholders and issuing the revalidation report (2 Times within 2 months from the first report submission). | Need Basis |
| Total | 16 Workdays \* |

\* *Approximately 2 Weeks (16 days)*

# Deliverables

## For VAPT

▪ Detailed VAPT Report (per asset):

o Executive Summary (management view)

o Technical Findings (per asset with screenshots & proof of concept) o Risk Categorization (CVSS scoring)

o Business Impact Analysis

o Recommended Remediation Actions

▪ Consolidated Security Posture Report: Heatmaps, trend analysis, and overall security ranking.

▪ Remediation Verification Report: Post-fix validation (1 free retest round included).

▪ Presentation & Workshop: Findings presented to stakeholders, Q&A session, and mitigation roadmap.

## For Infrastructure Security

* Configured and hardened firewall (Cloudflare + OS-level).
* Hardened Nginx server with WAF policies.
* Updated OS-level security configurations and documentation.
* Post-implementation validation report.
* Knowledge transfer session with the IT team.

# Other Important Issues

◻ Confidentiality & NDA: All testing will follow strict NDA and confidentiality guidelines.

◻ Testing Windows: To be aligned with the client’s operational requirements to avoid service disruptions.

◻ Access Requirements: Test accounts, API tokens, VPN access (if internal testing), and staging environments (if available).

◻ Safety Mechanism: Non-destructive testing techniques will be used; exploitation attempts will be controlled.

◻ Compliance Focus: Mapping findings against ISO 27001, NIST, OWASP, and PCI DSS to help meet regulatory & audit needs.

◻ Knowledge Transfer: Internal IT/security teams will be trained on identified gaps and future preventive measures.

# List of Tools to be Used for VAPT

## Licensed Tools

✓ Nessus Professional – For infrastructure & web vulnerability scanning

✓ Burp Suite (Professional)—For web application vulnerability scanning

✓ Acunetix (Professional)—For web application vulnerability scanning

## Reconnaissance and Information Gathering

✓ Nmap – Network discovery and port scanning

✓ Masscan – High-speed port scanning

✓ Shodan / Censys – Public exposure & Internet-facing asset discovery ✓ theHarvester – Email, domain, and subdomain harvesting

✓ Amass – Subdomain enumeration

✓ Maltego – OSINT & relationship mapping

✓ Recon-ng – Web-based reconnaissance framework

✓ Sublist3r / Subfinder – Subdomain enumeration

## Vulnerability and Scanning

✓ Nessus – Infrastructure & web vulnerability scanning

✓ OpenVAS (Greenbone) – Open-source vulnerability scanner

✓ QualysGuard – Enterprise vulnerability management

✓ Nexpose (Rapid7 InsightVM) – Network vulnerability scanning

✓ Burp Suite (Pro/Community) – Web application vulnerability scanning

✓ Acunetix – Web application & API vulnerability scanner

✓ Nikto – Web server scanning

✓ Wapiti – Web app vulnerability scanning

## Web Application Security Testing

✓ OWASP ZAP (Zed Attack Proxy) – Automated & manual web testing

✓ Burp Suite Professional – Proxy interception, fuzzing, and exploit testing

✓ SQLmap – Automated SQL injection exploitation

✓ Commix – Command injection testing

✓ XSStrike – Advanced XSS testing tool

✓ Wfuzz / Dirbuster / Gobuster – Directory and file brute forcing

✓ WhatWeb / Wappalyzer – Web technology fingerprinting

✓ CMSMap / WPScan / Droopescan – CMS (WordPress, Joomla, Drupal) security testing

## API and Web Application Security

✓ Postman – API functional testing

✓ Burp Suite Pro (with API plugins) – API fuzzing and manipulation

✓ OWASP ZAP API Scanner – Automated API security testing

✓ SoapUI / ReadyAPI – SOAP/REST service testing

✓ JWT Tool / jwt-cracker – JSON Web Token testing

✓ GraphQLmap – GraphQL security testing

## Network and Infrastructure Testing

✓ Metasploit Framework – Exploitation framework

✓ ExploitDB / Searchsploit – Exploit database

✓ Hydra / Medusa / Ncrack – Password brute-force tools

✓ Responder – LLMNR, NBT-NS, and MDNS poisoning

✓ BloodHound – Active Directory attack path analysis

✓ Ettercap / Bettercap – Man-in-the-Middle attacks

✓ Wireshark / Tcpdump – Network traffic analysis

## Exploration and Privilege Acceleration

✓ Metasploit – Exploitation framework

✓ Empire / Covenant – Post-exploitation

✓ Mimikatz – Credential extraction

✓ BeEF (Browser Exploitation Framework)—Browser security testing

✓ PowerSploit – PowerShell exploitation

## Own Script

✓ Own developed script – For manual penetration testing

# List of Tools to be Used for Infrastructure Security

* Cloudflare Firewall (Pro Plan).
* Nginx + ModSecurity / OWASP Core Rule Set.
* Linux Firewall Tools: iptables, UFW.
* Validation Tools: Nmap, Nikto, and custom penetration scripts.

# Financial Proposal

| **SN** | **Particular** | **Qty** | **Rate** | **Amount** |
| --- | --- | --- | --- | --- |
| Vulnerability Assessment and Penetration Testing | | | | |
| 1. | Number of Domains | 1 | 0 | 0 |
| Infrastructure-level security enhancement | | | | |
| 2. | Cloudflare Firewall Configuration + Policy Update | 1 | 0 | 0 |
| 3. | Nginx Security Policy Hardening (ModSecurity, SSL/TLS, headers) | 1 | 0 | 0 |
| 4. | OS-Level Security Hardening (iptables, SSH, logs, monitoring) | 1 | 0 | 0 |
| 5. | Application-Level Security Updates (Post-VAPT Integration) | 1 | 0 | 0 |
| 6. | Documentation & Knowledge Transfer | 1 | 0 | 0 |
| 7. | WordPress plugins, WooCommerce other configurations, and updates | 1 | 0 | 0 |
| VAT (15%) | | | | 0 |
| TAX/AIT (10%) | | | | 0 |
| **Total** = | | | | 0 |

(Note: Cloudflare Pro subscription (~20 USD/month) will be borne by the client.)

| **Total (including VAT & TAX) =** | **0** |
| --- | --- |
| **Taka in Words:** | |

# Payment Terms & Conditions

a) Price: The quoted price is in Bangladeshi Taka (BDT), including VAT (15%) and TAX/AIT (10%).

b) Payment: All payments to be made by A/C Pay Cheque or Pay Order in the name of “Centre for Testing and Advisory Service (CATS)”.

c) Mode of Payment: 50% of the payment will be paid with the Work Order (WO), and the remaining 50% payment will be paid after delivering the final report.

d) Offer Validity: The validity of this offer will be 30 days from the date of the issuance of the proposal.

e) Delivery: The delivery of work will be done according to the methodologies and deliverables mentioned in this proposal.

# Conclusion

Cybersecurity is a continuous process requiring both assessment (VAPT) and preventive measures (infrastructure hardening). By implementing the proposed enhancements, our client will achieve a stronger security posture, minimizing the risk of cyber incidents and ensuring service continuity.

Our balanced and cost-effective approach aligns with industry best practices while considering the client’s operational needs and budgetary constraints.

Confidentiality

All information shared during this engagement will be treated as strictly confidential and handled in accordance with a mutually signed **Non-Disclosure Agreement (NDA)**.

## 

**Hridoy Mustofa**Founder and CEO  
Email: [hridoy@cyberlog.com.bd](mailto:hridoy@cyberlog.com.bd)   
Phone: +880 1864-291014  
Website: [https://cyberlog.com.bd](http://cyberlog.com.bd)