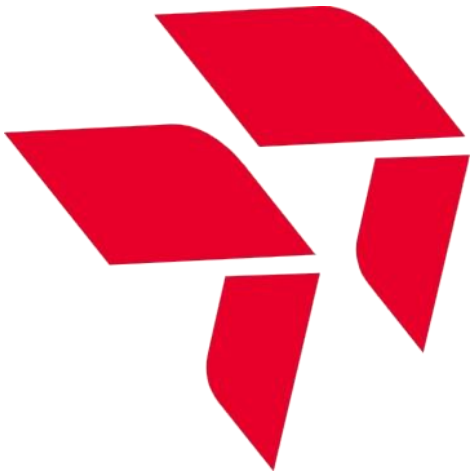

REQUEST FOR PROPOSAL (RFP)

Title: Vulnerability Assessment & Penetration Testing (VAPT)
Platform: Prime Bank FinTech Digital Wallet
Date: Monday, April 6, 2026

Table of Contents

1. Introduction

Prime Bank FinTech Limited (PBFTL) invites proposals from experienced cybersecurity service providers to conduct **Vulnerability Assessment and Penetration Testing (VAPT)** for its **Prime Bank FinTech Digital Wallet platform**, including web applications, APIs, infrastructure, and mobile applications.

The engagement aims to proactively identify security vulnerabilities, assess risks, and recommend mitigation measures to ensure the platform remains secure, compliant, and resilient against cyber threats in line with Bangladesh Bank guidelines and industry best practices.

2. Objective of the Assignment

The objective of this assignment is to perform a comprehensive and controlled security assessment of the Digital Wallet ecosystem. The selected vendor will be responsible for identifying vulnerabilities, validating exploitability, and providing actionable recommendations.

The engagement will follow recognized standards such as **OWASP Top 10, API Security Top 10, and NIST guidelines**, ensuring alignment with regulatory expectations and fintech security requirements.

3. Scope of Work

The scope of VAPT will cover the complete Digital Wallet ecosystem, including **web applications, APIs, backend infrastructure, and mobile applications**.

3.1 Infrastructure & Network

The assessment will include production servers and supporting infrastructure components such as database servers, application servers, API servers, WAF, VPN, and other critical systems. Testing will primarily follow a **gray-box approach** and will be conducted in controlled windows to avoid operational disruption.

3.2 Web Application & API

The Digital Wallet platform consists of multiple web applications including customer-facing portals, administrative interfaces, and integration layers. These applications are tightly coupled with a large API ecosystem supporting financial transactions and business operations.

The assessment will focus on:

- Web application security vulnerabilities (authentication, session, input validation)
- API security (authentication, authorization, data exposure, rate limiting)
- Business logic vulnerabilities (transaction flow manipulation, fraud scenarios)

3.3 Mobile Application

The Digital Wallet ecosystem includes multiple mobile applications (customer, agent, merchant, distributor, and DSO). These applications will be tested for client-side vulnerabilities, insecure storage, API interaction flaws, and authentication weaknesses.

Testing will follow a **black-box approach** with emphasis on real-world attack simulation.

3.4 Coverage Areas

The assessment is expected to cover, but not be limited to:

- Authentication and authorization controls
- Data protection and encryption mechanisms
- API security and access control
- Network-level vulnerabilities
- Configuration weaknesses in servers and security devices
- Common attack vectors such as injection, XSS, CSRF, and session hijacking
- Business logic flaws specific to digital financial services

3.5 Scope Summary

The following asset inventory will be considered for VAPT:

Asset Category	Description	Total Count
Web Applications	Customer portal, admin portal, API gateway, frontend systems	**5**
APIs endpoint	Backend APIs supporting wallet, onboarding, payments, reporting, etc.	**300+**
Mobile Applications	Customer, Agent, Distributor, DSO, Merchant apps (Android & iOS)	**5**
Infrastructure	Servers, DB, WAF, VPN, API nodes	**20+**

* Final scope will be validated during kickoff and may be adjusted with mutual agreement.

3.6 Engagement Approach

The VAPT engagement will be conducted in the following phases:

- Planning & Scope Finalization
- Information Gathering & Reconnaissance
- Vulnerability Assessment
- Penetration Testing & Exploitation
- Reporting & Risk Analysis
- Revalidation & Closure

Testing must be performed in a controlled and coordinated manner with prior approval from PBFTL.

4. Deliverables

The selected vendor will provide structured and actionable deliverables that support both technical remediation and management decision-making. All vulnerabilities must include:

- CVSS Score
- Business Impact
- Reproducible steps
- Recommended fix

4.1 Reporting

- Detailed Vulnerability Assessment Report with severity classification
- Penetration Testing Report including exploitation evidence
- Executive Summary highlighting key risks and business impact
- Risk-based remediation plan with prioritization
- Revalidation report confirming closure of identified vulnerabilities

4.2 Knowledge Transfer

The vendor will conduct sessions with PBFTL teams to explain findings, remediation strategies, and recommended best practices.

5. Functional Requirements

The vendor is expected to evaluate the system against standard security scenarios including password strength validation, application security weaknesses, operating system vulnerabilities, and network-level threats.

The assessment should also validate the platform's resilience against common attack techniques such as injection attacks, spoofing, denial-of-service simulations, and unauthorized access attempts.

The assessment must include validation of financial transaction integrity, prevention of unauthorized fund movement, bypass of transaction limits, and abuse scenarios in wallet, recharge, and disbursement flows.

6. Vendor Eligibility Criteria

6.1 Mandatory Requirements

- The bidder must be a registered company operating in Bangladesh or internationally with local presence/representation
- Minimum **3 years of experience** in cybersecurity or VAPT services
- Experience in at least:
  - ✓ 5 Banks / NBFI / Fintech / Digital platforms
- Ability to perform VAPT for **web, API, and mobile applications**

6.2 Technical Requirements

- Availability of qualified security professionals with industry-recognized certifications such as CEH / Security+ / equivalent
- At least one senior resource with experience in information security assessments
- Familiarity with standard tools and frameworks for VAPT
- Ability to perform both automated and manual testing
- Experience in reporting aligned with industry standards (OWASP, CVSS, etc.)
- The vendor must demonstrate capability to test high-volume API-based systems and financial transaction platforms.

7. Evaluation Method

The evaluation will follow a **Quality and Cost Based Selection (QCBS)** approach.

- Technical Proposal: 70%
- Financial Proposal: 30%

Technical evaluation will consider methodology, relevant experience, team capability, and understanding of the assignment. Only bidders scoring minimum 50 out of 70 in technical evaluation will be considered for financial evaluation.

7.1 Technical Evaluation Criteria

Criteria	Marks
Methodology	20
Experience	15
ISO Certification	5
Tools	5
Senior Resource	10
Certified Team	15
Total	**70**

8. Financial Proposal

The bidder shall submit a detailed financial proposal covering all components of the VAPT scope including web applications, APIs, infrastructure, and mobile applications.

The proposal should clearly mention:

- Total cost excluding VAT
- Applicable VAT and taxes
- Total cost including VAT

9. Timeline & SLA

The engagement is expected to be completed within a reasonable timeframe, typically ranging between **3 to 5 weeks**, including assessment, reporting, and revalidation.

Remediation expectations should follow industry practices, where critical findings are addressed on priority, followed by high and medium risks within agreed timelines.

Phase	Timeline
Kickoff	Within 3 working days from award
Assessment	2 weeks
Reporting	5 days

Phase	Timeline
Revalidation	5 days

10. Compliance & Regulatory Alignment

The vendor must ensure that all activities comply with applicable laws and regulatory requirements including:

- Bangladesh Bank ICT Security Guidelines
- Cyber Security Act 2023
- Digital Security Rules

11. Submission Guidelines

The proposal should be submitted in two separate parts:

- Technical Proposal
- Financial Proposal

Both documents must be duly signed and submitted within the specified deadline.

12. Terms & Conditions

- The selected vendor must sign a Non-Disclosure Agreement (NDA) prior to commencement
- Testing activities must be conducted in a controlled manner without disrupting production services
- The authority of PBFTL reserves the right to relax, change or drop any of the terms and conditions of the schedule without any further notice.
- PBFTL reserves the right not to accept the lowest Tender and to reject any Tender, part thereof, or all Tenders without assigning any reason whatsoever.
- Submission of declaration regarding bidder (s) has the legal capacity to enter the contract under the applicable law of Bangladesh, and the bidder (s) shall not be barred as per the law of the land that may be subject to legal proceedings of any kind.
- The rates must be quoted in figures as well as in words. All the prices should be mentioned in Bangladesh Taka (BDT). The payment will also be made in BDT.
- Please submit commercial bid in company letterhead pad (PDF Copy).
- Quotation validity: Quotation shall remain valid for a minimum of 30 (thirty) calendar days from the Quotation Submission Date.
- Delivery Terms: Partial delivery is allowed.
- Place of delivery: Prime Bank FinTech Limited, Prime Aspire, CES (A) 48 (Old 98/A), Gulshan Avenue, Gulshan, Dhaka 1212, Bangladesh.

12.1 Payment Terms

- **20%** upon submission of initial VAPT report
- **30%** upon submission of final report with management summary
- **50%** after successful revalidation and formal acceptance by PBFTL

13. Confidentiality & Data Handling

- All data accessed during VAPT must be treated as confidential.
- The vendor must not retain, share, or reuse any data obtained during the engagement.
- All test data, logs, and reports must be handed over to PBFTL and deleted from vendor systems after completion.

14. Sub-Contracting

The selected bidder shall not subcontract or permit anyone other than its personnel to perform any of the work, services, or other obligations required under the contract without the prior written consent of Prime Bank FinTech Limited.

15. Request for Quotation Schedules

RFP Reference No.	Tender Ref: PBFTL/RFP/2026/004
Last date for submitting Queries by vendor	April 12, 2026
Last date for submission of response to RFP	April 14, 2026

16.1 Submission & Communication Guidelines

Any bid received by PBFTL after the specified deadline for submission shall be rejected and/or returned unopened to the bidder, if so requested.

For any clarification regarding this RFP, bidders are requested to communicate with:

Name: Munir Hossain Mallick
Designation: Senior Manager, Supply chain & Procurement
Phone: +8801711-504711 (During Office Hour From: 10.00 AM To: 5 PM)

PBFTL will endeavor to respond to all reasonable queries received within the stipulated timeline. Queries received after the specified deadline may not be considered.

PBFTL reserves the right to seek additional information, clarification, or documents from any bidder after submission of proposals. Such information shall be treated as part of the bidder's response.

16.2 Tender Preparation & Submission

- The proposal must be submitted using a two-envelope system, consisting of:
  - ✓ Technical Proposal
  - ✓ Financial Proposal
- Each proposal must be clearly marked as "*Technical Proposal*" and "*Financial Proposal*" on the respective envelopes.
- Both envelopes shall be enclosed within a third outer envelope, which must be properly sealed and signed.
- In addition to the physical submission, bidders must also submit a softcopy (PDF format) of both Technical and Financial Proposals via email to: procurement@pbftl.com

- The softcopy must be identical to the physical submission. In case of any discrepancy, bidder will be disqualified.
- All submissions must be complete in all respects and comply with the instructions provided in this RFP.

17. Declaration

The bidder must confirm that:

- They are not blacklisted by any regulatory or financial institution
- All submitted information is accurate and verifiable
- They agree to comply with all terms and conditions of this RFP

ANNEXURE - A: SELF DECLARATION OF NON-BLACKLISTING

To
The Chairman
Procurement Committee
Prime Bank FinTech Limited (PBFTL)
Prime Aspire (Level-3)
CES(A) 48 (Old 98/A), Gulshan Avenue, Gulshan
Dhaka-1212, Bangladesh

Subject: Self Declaration Regarding Non-Blacklisting

Dear Sir/Madam,

We hereby declare and certify that **[Company Name]**, having its registered office at **[Company Address]**, has **not been blacklisted, debarred, or otherwise restricted** from participating in any tender, contract, or procurement process by any:

- Government authority
- Regulatory body
- Financial institution (Bank/NBFI/MFS)
- Public sector organization
- International organization

either in Bangladesh or abroad, as on the date of submission of this proposal.

We further confirm that:

- There are no pending investigations or legal proceedings against our organization that would materially impact our ability to perform the services outlined in this RFP.
- All information provided in our proposal is true, complete, and accurate to the best of our knowledge.

We understand that if any information provided herein is found to be false or misleading at any stage, **Prime Bank FinTech Limited (PBFTL)** reserves the right to:

- Disqualify our proposal
- Terminate any contract awarded
- Take appropriate legal or administrative action

Yours sincerely,

Signature: _____
Name: _____
Designation: _____
Company Name: _____
Date: _____
Company Seal: _____

ANNEXURE - B: EXPERIENCE DETAILS

Details of VAPT Assignments Carried Out

(Documentary proof such as Work Order / Completion Certificate must be attached)

SL No.	Client Name	Organization Type (Bank / NBFI / Fintech / MFS / Others)	Scope Covered (Web / API / Mobile / Infra)	PO Date	Completion Date	Status (Completed / Ongoing)	Contact Person of Client
1							
2							
3							
4							
5							

Documentary proofs are to be enclosed to substantiate the claims made.*

Date:

_____

Seal and Signature of Bidder

Instructions to Bidders

- Provide details of **relevant VAPT projects only** (preferably BFSI / Fintech / Digital platforms).
- Each project must be listed in a **separate row**.
- Attach **supporting documents** (Work Order / Completion Certificate).
- PBFTL reserves the right to **verify the information** with the provided client references.
- Incomplete or unverifiable information may lead to **disqualification**.

ANNEXURE - C: TEAM EXPERIENCE DETAILS

Details of Proposed Project Team Members

(Documentary proof such as CV, certifications must be attached)

SL No.	Name of Resource	Role in Project (PM / Team Lead / Security Analyst / Tester)	Educational Qualification	Professional Certifications (CEH / OSCP / CISSP / etc.)	Total Experience (Years)	Relevant VAPT Experience (Years)	Experience in BFSI / Fintech (Years)	Number of Similar Projects	Key Areas of Expertise (Web / API / Mobile / Infra)	Employment Type (Full-time / Contract)
1										
2										
3										
4										
5										

Documentary proofs are to be enclosed to substantiate the claims made.*

Date:

_____

Seal and Signature of Bidder