Request for Proposal (RFP) for External Vulnerability Assessment and Penetration Testing (VAPT)

1. Introduction

Tpl Trakker invites qualified and experienced cybersecurity firms to submit proposals for an External Vulnerability Assessment and Penetration Testing (VAPT) project. The primary focus will be on assessing the security of our externally facing assets to identify and mitigate potential vulnerabilities.

The assets in scope for this assessment include:

- **Websites**: 9
- **Mobile Applications**: 4 (3 Android and 1 iOS)
- **APIs**: 5
- **Database Servers**: 5
- **Web Servers**: 5

2. Objectives

The objectives of this project include:

I. External Vulnerability Assessment and Penetration Testing (White Box and Black Box)

Comprehensive Vulnerability Assessment

- Conduct a thorough vulnerability assessment of all externally facing assets.
- Identify and document vulnerabilities, weaknesses, and potential threats associated with these assets.
- Evaluation of Security Policies (in scope of VAPT)

Review and assess the organization's current security policies, procedures, and controls related to external assets.

- Ensure alignment with industry best practices and regulatory requirements.
- Examination of External Network Architecture

Perform a detailed examination of the external network architecture, focusing on publicly accessible components, including:

- Websites
- Mobile applications
- APIs
- Database servers
- Web servers

- Ensure each component's security is evaluated based on its configuration, connectivity, and exposure to the internet.

Analysis of Component Configuration

- Analyze the configuration and interconnectivity of external components to detect misconfigurations, security gaps, and vulnerabilities that may exist due to improper settings or insecure network design.

Threat Susceptibility Assessment

- Assess the external assets' exposure to both common and emerging cyber threats, including advanced persistent threats (APTs) and zero-day vulnerabilities.
- Simulate real-world attack scenarios to gauge the effectiveness of current security measures.

i. Documentation:

- Provide detailed assessment reports for each specified component.
- Deliver a comprehensive remediation guide for identified vulnerabilities.

3. Scope of Work

The selected vendor will be required to:

- Perform an in-depth external vulnerability assessment of the specified components.
- Conduct comprehensive penetration testing on the specified externally facing assets.
- Collaborate with our IT and security teams throughout the project.
- Deliver comprehensive reports detailing the findings of the VAPT, including a prioritized list of vulnerabilities and weaknesses.
- Present clear and actionable recommendations for addressing each identified issue, accompanied by a detailed remediation plan.
- Document the entire assessment process, ensuring transparency and traceability in understanding the rationale behind recommendations and remediation steps.

i. Clarification on Assessment Boundaries:

The assessment should be conducted exclusively on the specified scope.

ii. Legal and Compliance Requirements:

The assessment must adhere to relevant legal, regulatory, and compliance requirements, including but not limited to local cybersecurity laws, data protection regulations, and industry standards.

iii. Confidentiality Agreement:

The selected vendor must sign a confidentiality agreement to protect sensitive company information that might be exposed during the VAPT.

iv. Incident Response Plan:

Vendors are required to provide their protocol for incident response in case a critical vulnerability or breach is discovered during testing.

v. Communication Plan:

Outline how communication will be managed throughout the project to keep all stakeholders informed of progress, findings, and remediation efforts.

4. Proposal Submission Guidelines

Interested vendors are requested to submit their proposals by 11th October 2024. Proposals should include:

- Overview of the vendor's experience in external vulnerability assessments and penetration testing, with a focus on similar externally facing assets.
- Proposed methodology for conducting the VAPT for the specified components and tools.
- Detailed breakdown of costs, including fees, expenses, and any additional charges.
- References from previous clients with similar project requirements.

5. Evaluation Criteria

Proposals will be evaluated based on the following criteria:

- Relevant experience and expertise in external vulnerability assessments and penetration testing.
- Proposed methodology and approach tailored to the provided scope.
- Cost and value for money.
- References and client testimonials.

6. Timeline

The project will follow these phases:

- **Proposal Submission Deadline:** 1st Nov 2024
- **Vendor Selection and Contract Award:** 15th Nov 2024

The revalidation phase will involve a follow-up assessment to ensure all recommended security measures have been effectively implemented and are functioning as intended. This phase is crucial to validate the remediation steps and to confirm the closure of identified vulnerabilities.

7. Proposal Submission

Please submit your proposal by 1st Nov 2024 to:

Name: Shaharyar Asif

Title: Team Lead Information Security

Company: TPL Corp

Contact Number: +92-301 8582325

Email Address: shaharyar.asif@tpltrakker.com

Name: Farjad Feroz

Title: Group Head of Information Security

Company: TPL Corp

Contact Number: +92-313-2191538

Email Address: farjad.feroz@tplcorp.com

Tpl Trakker reserves the right to reject any or all proposals and to negotiate with the selected vendor.

Thank you for considering our request.