Request of Proposal

Purpose

General objective of the penetration test is to identify existing vulnerabilities, determine possibilities of use/exploitation, assess associated business risks and provide recommendations.

General Scope

N	Name	Q-ty	Type of Test
1	Applications	12	Black Box Security Testing according to OWASP top 10

During the Black Box penetration test, the stopping point is determined when an illegitimate entry into the system occurs.

Black Box penetration testing steps should include given steps:

1. Reconnaissance - Process of gathering preliminary information about the target system;
2. Scanning & Enumeration – Discovering systems on the network and looking at what ports are open as well as applications that may be running;
3. Vulnerability Discovery – Identifying potential weakness and security loopholes present in target systems network or/and applications;
4. Exploitation - Establishing access to a system by bypassing security restrictions and exploiting found vulnerabilities.
5. Privilege Escalation – Trying to gain elevated access to resources that are normally protected from an application or user.

Reporting requirements and Deliverables

Final Report

The full report should be presented in English language and should contain at least the following:

- Executive summary;
- Risk analysis;
- Recommendations;
- Detailed description of carried out actions and findings

Penetration Testing Methodologies and Standards

The Vendor shall provide automated, manual or hybrid penetration testing Services, as requested. The Vendor shall provide penetration test Services following appropriate industry wide, highly recognized methodologies and standards:

- Payment Card Industry Data Security Standard (PCI DSS)
- National Institute of Standards and Technology (“NIST”) SP 800-115
- Open Web Application Security Project (“OWASP TOP 10”)
- Massachusetts Institute of Technology Research and Engineering (MITRE ATT&CK)

The vendor must use the CVSS (Common Vulnerability Scoring System) to evaluate the identified vulnerabilities. The Vendor shall follow the most recent version of the methodologies and standards when providing Services.

General Requirements on Penetration Testing Services

The Vendor shall ensure the following Services are covered in each individual request for Service:

- Confirm and obtain Client's approval on scope of Service including a test plan in writing prior to Service commencement;
- The vendor should not engage a subcontractor without agreement with the client. Engage Client prior tactual test to confirm logistics arrangement, understand test goals and objective Client would like to achieve as a result of the test;
- Discuss and confirm with Client on its risk tolerance and culture to ensure Client approve the test approach;
- Establish a communication plan as to what the Client's organization will know about the test;
- Establish an incident and escalation management process to handle issues that may happen during the test;
- Identify information to be provided by Client based on the nature of test being performed reporting to Client as further stated;
- Provide the follow up retest of the fixed critical and high vulnerabilities;

The Vendor shall ensure Client's system being tested will not suffer (i.e., put Client system at risk or impact Client system's stability) as the result of the testing, unless with Client's prior written approval.

Penetration Testing Services Clean Up

The Vendor shall clean up properly after penetration testing Services completion ensuring Client's environments are not impacted as a result of the penetration testing Services, the cleanup activities include but are not limited to the following:

- Update and/or removal of test accounts added or modified during testing;
- Update and/or removal of database entries added or modified during testing;
- Uninstall test tools or other artefacts as applicable;
- Restoring security controls that have been altered for testing;
- Provide Clients with necessary information and/or guidance on how to verify Client's environments have been restored;
- Provide Client with confirmation that the environments have been cleaned and restored;

In situations where Client finds issues after Services have been completed, the Vendor shall return and fix the issue, for free, for the Client ensuring Client satisfaction.

Logs

The Vendor shall log and trace each activity and information sent and received between the Vendor's and Client environments as it pertains to the Service activities. This log shall be provided to Client upon request in a format that is approved by Client.

Penetration Testing Services Reporting and Presentation

The Vendor shall provide Client with a report for each Service completed, the report shall include the following information at a minimum:

- Executive Summary;
- Scope of Service;
- Identification of critical components and explanation of why these components were tested;

- Methodologies and tools used to conduct the testing;
- Any constraints that impacted the testing (e.g., specific testing hours, bandwidth, special requirements);
- Description of the progression of the test and issues encountered during the testing with timelines;
- Findings from the tests (e.g., exploitation, severity) with details;
- Affected targets in Client's environments;
- Detailed Recommendations on remediation;

From time to time, Client may require the Vendor to meet in person and/or via teleconference and webinar to explain the findings and/or present the report. The Vendor shall support Client with such request.

Selection Criteria

Deadline: 25.06.2024

Following documentation is required to be submitted in paper/online form:

- Description of the methodology used;
- Experience in penetration testing:
    - Candidate or (subcontractor) should have certifications issued by trusted certification bodies in this field, like (OSCP, CEH), at least 5 years of experience in relevant field and should provide short description, scale and number of implemented penetration testing projects.
    - Minimum 1 recommendation letter about successful implementation of similar project (would be a plus).
- Project timeline (by each scope) and completion time;
- Total price of the project;
- Price breakdown by each scope;