A picture containing text, clipart

Description automatically generated

**Request for Proposal for Penetration Testing**

|  |  |
| --- | --- |
| **Issue Date** | November 1, 2023 |
| **Company** | Unibank OJSC |
| **Website** | https://www.unibank.az |
| **Phone Number** | +994 12 541 33 33 ext. 6668 |
| **Address** | Azerbaijan, Baku, Rashid Behbudov str. 55, Uniplaza |
| **Primary Contact Name & Title** | Uzeyir F. Huseynov  Director of İnformation Security department |
| **Primary Contact Email** | uzeyir.huseynov@unibank.az |

# **TABLE OF CONTENTS**

[**Table of Contents 2**](#_Toc113442806)

[**RFP Background 3**](#_Toc113442807)

[Company Background 3](#_Toc113442808)

[Project Overview 3](#_Toc113442809)

[Project Objectives 3](#_Toc113442810)

[Conditions and Disclaimers 3](#_Toc113442812)

[Selection Criteria 4](#_Toc113442813)

[Selection Timeline 4](#_Toc113442814)

**RFP BACKGROUND**

# COMPANY BACKGROUND

Unibank is one of the largest private banks in Azerbaijan.

# PROJECT OVERVIEW

We intend to select a vendor best suited to conduct the following penetration testing services:

|  |  |
| --- | --- |
| **Service** | **Scope** |
| External Penetration Testing | 85.132.77.0/24 - Blackbox |
| Internal External Penetration Testing | Greybox  Attacker models: disloyal employee, disloyal partner (using VPN)  Main target: Domain Admin access |
| Mobile Application and Web Application Penetration Testing | <https://play.google.com/store/apps/details?id=az.unibank.mbanking&hl=en&gl=US>  <https://apps.apple.com/az/app/ubank-by-unibank/id1073632425>  <https://unibank.az/>  <https://online.unibank.az/corporate> |

## PROJECT OBJECTIVES

For External Penetration Testing:

* Search for vulnerabilities (analysis for completeness), their exploitation, development of an attack only within a vulnerable node.

For Internal Penetration Testing:

* Obtaining Domain Admin Privileges.

For Mobile Application Penetration Testing:

* Search for vulnerabilities (analysis for completeness) and their exploitation.

# CONDITIONS AND DISCLAIMERS

Qualification requirements:

Bidder must provide a summary of the project team listing the names of the individuals and their role in the project. The following requirements apply to the project team:

1. The project team must include Offensive Security Certified Professional. Confirmed by electronic certificates.

2. The project team should have experience in finding vulnerabilities in common standard software. Confirmed by links to CVE/Security Advisory, where the name of the specialist and the company are indicated.

3. The project team must have experience of participating in Bug Bounty, which is confirmed by links to the profiles of participants on the websites of the programs, where their successes are visible.

The bidder company must have experience in the banking sector in the direction of Penetration Testing and Application Security, which is confirmed by reference letters. The bidder company must have experience of speaking at practical information security conferences, as well as experience of participating in CTF (confirmed by links to events).

The selected bidding company must not perform any denial-of-service attacks during penetration testing.

# SELECTION CRITERIA

* Pricing of the services to be provided
* Quality and reputation of the services to be provided
* Ability to perform the assessment within the project timeline
* Responsiveness in resolving issues

# SELECTION TIMELINE

The timeline for this project is listed below.

|  |  |
| --- | --- |
| **RFP Issue Date** | November 1, 2023 |
| **Proposal Due Date** | November 14, 2023 |
| **Project Timeline** | November 28, 2023 – December 23, 2023 |
| **Deadline for receiving reports** | December 26, 2023 |