YELO BANK OJSC, PENETRATION TESTING SERVICE

TENDER REQUEST

FOR MOBILE APPLICATION

1. Black box analysis. Mobile App. Yelo Bank. (IOS, Android)

The Analysis of a mobile application's security using the black box method should identify and search for flaws. The flaws use of which allows an attacker who does not have any information and logical access to the mobile application to implement the following classes of threats:

• Obtaining full or partial control over the mobile application;
• Obtaining unauthorized access to information processed by the mobile application;
• Using a mobile application to organize attacks on users;
During this stage, methods and tools should be used to identify the following classes of vulnerabilities:
• Errors in the implementation of user authentication mechanisms;
• Errors in the implementation of authorization and access control mechanisms;
• Lack or inadequacy of mechanisms to counter attacks on mobile application users (cross-site scripting, request forgery, etc.)
• Vulnerabilities leading to a violation of the logic of the operation of the mobile application;
• Storing sensitive information in a clear form;
• Possibility of unauthorized access to critical functions of the mobile application (for example, to conduct financial transactions);
• Disclosure of configuration information, including - disclosure of information about the features of the implementation of the functions of the mobile application, the software components used, and other information that makes it easier for the attacker to organize an attack;
• Errors in the implementation of the functions of the mobile application available to the user;
• Disadvantages of the protocol of interaction between the server and client parts of the application;
Other security vulnerabilities and weaknesses according to OWASP Top 10 and OWASP Top 10 Mobile Risks.

Searching for the exploitation of vulnerabilities in an application should combine instrumental analysis methods and manual examination of application components by experts.

Also, Analysis of the server-side of the Mobile application:

- A comprehensive analysis of the security of the server-side of a mobile application should include:
- Instrumental Analysis of the protection of the server-side of the mobile application;
- Manual Analysis of the protection of the server part of the mobile application.
- Instrumental Analysis within this stage aims to detect the most common vulnerabilities in the server-side of a mobile application that can be detected by automated means. The work should be carried out using the black box method.

2. White box analysis. Mobile App. Yelo Bank. (IOS, Android)

At this stage, the Analysis of the source code of the mobile application should be carried out.

In the course of work, the specialists of the Contractor will be provided with:

• Information about the operating environment of the mobile application (used versions of OS, services, and software, information directly related to the architecture and functioning of the mobile application);

• Source code of the analyzed mobile application.

Results:

A report is provided, which should contain:

- General information about the conducted security analysis;
- The results of the checks carried out;
- Conclusions (brief for guidance and detailed technical)
- The list of identified vulnerabilities should contain a description, indication of corresponding CVE identifiers (where applicable), and ranking according to severity level (according to the CVSS rating system);
- Recommendations for eliminating the identified vulnerabilities, including - recommendations for changing the configuration and settings of equipment, used protective mechanisms and software protection tools, for installing the necessary updates for the software used, etc.;
- Examples of exploiting vulnerabilities.
- The report must be submitted in Russian and English.

Staff:

- Bidder should provide a staff portfolio (successful projects and certifications) of the penetration test team involved in the process.