YELO BANK OJSC, PENETRATION TESTING SERVICE

TENDER REQUEST

FOR INTERNET BANKING APPLICATION

1. **Gray box analysis for Internet Bank. (Using Test User Accounts)**

The Analysis of an internet banking application's security using the grey box method should identify and search for flaws. The flaws use of which allows an attacker who has partial information and user access to Internet banking to implement the following classes of threats:

• Gaining full or partial control over the application;
• Obtaining unauthorized access to information processed by the application;
• Using the 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 insufficient mechanisms to counteract attacks on application users (cross-site scripting, request forgery, etc.)
• Vulnerabilities leading to a violation of the logic of the application;
• Storage of sensitive information in a clear form;
• Possibility of unauthorized access to critical functions of the application (for example, to conduct financial transactions);
• Disclosure of configuration information, including - disclosure of information about the implementation features of the application functions, used software components, and other information that makes it easier for the attacker to organize an attack;
• Errors in the implementation of the functions available to the user of the application;
• Disadvantages of the protocol of interaction between the server and client parts of the application;
Other vulnerabilities and weaknesses of security mechanisms according to OWASP Top 10 and TOP 20.

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

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.

Staff.

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