ONSEC

Web/mobile application white-box security audit methodology

Intro **3**

Attacker model **3**

The scope of work **3**

Detailed description of the scope of work **4**

Collecting information about the app 4

Manual application security analysis 4

Application security analysis using automated tools 4

Preparation of a report on the results of security analysis 4

Verification of the remediation of detected vulnerabilities (optional) 5

Service conditions **5**

ONSEC

Intro

The methodology is a sequence of actions carried out by the Contractor to perform an analysis of the security level of information resources of the Customer (The System).

It also implies the use of other Contractor's methodologies to analyze the security level of information systems and the application of the following international standards and practices:

- Penetration Testing Execution Standard (PTES);
- Special Publications NIST 800-115 Technical Guide to Information Security Testing and Assessment;
- Open Source Security Testing Methodology Manual (OSSTMM);
- Information Systems Security Assessment Framework (ISSAF);
- Web Application Security Consortium (WASC) Threat Classification;
- Open Web Application Security Project (OWASP) Testing Guide;
- Open Web Application Security Project (OWASP) Code Review Guide;
- Payment Card Industry Data Security Standard (PCI DSS);
- Center for Internet Security (CIS) standards;

While audit is conducted both manual checks of possible vulnerabilities and automated checks with the use of special tools are used.

Security analysis is aimed at identifying weaknesses and exploitable vulnerabilities that lead to unauthorized access to private components of applications or increase privileges in Customer applications.

Attacker model

In the course the work, the Contractor's specialists simulated the process of analyzing applications by an attacker, whose purpose is to damage the System, or gain access to reading and changing confidential information of the Customer. It is assumed that the attacker is a highly qualified specialist with skills comparable to those of the Contractor's specialists.

As part of the ongoing work on the analysis of the security of web applications by the "white box" method, the executor implements the intruder model-an attacker with a full set of knowledge about the system under study and full access to all its components.

The scope of work

As part of the ongoing work on the analysis of the security of information resources, the Contractor performs the following stages of testing:

- Collecting information about the app
- Manual application security analysis
- Application security analysis using automated tools
- Preparation of a report on the results of web application security analysis

Detailed description of the scope of work

Collecting information about the app

- Analysis of application features and business rules;
- Exploring the context within which the application operates;
- Identify information whose disclosure or leakage is critical to the application;
- The study of existing user roles and access rights;
- Study the type of application and the technology stack used;
- The study of the architecture of the application;
- Familiarization with the standards of the Customer's company applied in relation to the studied application;
- The definition of the attack surface of an application.

Manual application security analysis

- Analysis of the validation of input data;
- Analysis of authentication mechanisms;
- Analysis of session management mechanisms;
- Analysis of authorization mechanisms;

- Analysis of cryptographic tools used;
- Analysis of error handling mechanisms;
- Analysis of logging mechanisms;
- Analysis of code compliance with existing application business logic;
- Analysis of the security application configuration;
- Application network architecture analysis;
- Code quality analysis;
- Analysis of the security of external application dependencies.

Application security analysis using automated tools

- Analysis of ascending call graphs from unsafe functions to user data;
- Analysis of descending call graphs from user data to unsafe functions;
- Perform tests to cover application calls based on role model and call graph;
- Testing call trees for a web application (by access roles) with a dynamic analyzer;
- Static and dynamic analysis of unsafe call map.

Preparation of a report on the results of security analysis

- General information about the testing;
- Goals and objectives;
- Testing conditions;
- Information about vulnerabilities that lead to the possibility of obtaining critical Customer data;
- Expert assessment of the current security level of the web application;
- General recommendations to address identified vulnerabilities;
- Detailed information about the vulnerabilities found, including a detailed description, severity level, location of detection, operating example, and Troubleshooting recommendations;
- The results of the study of the web application.

Verification of the remediation of detected vulnerabilities (optional)

Service conditions

On the Customer side, a responsible person is allocated for interaction with the Contractor. Interaction includes coordination of the inspections carried out during the performance of works. The responsible person provides contact information to the Contractor for the possibility of operational interaction.

In case of detection of vulnerabilities that may affect system availability, checks and time slots for testing are negotiated separately with the Customer.

If necessary, the Customer forms a description of the limits of the objects included in the work.

The Contractor's specialists check the vulnerabilities described in the report after a specified number of days from the completion of the main testing. Based on the results of the recheck, a final report is generated containing the status of each previously detected vulnerability.