EXPERT REPORT

on the results of the security assessment

of the external perimeter

Table of Contents

[1. Introduction 3](#_Toc96608894)

[1.1. General provisions 3](#_Toc96608895)

[1.2. Summary 3](#_Toc96608896)

[2. Security assessment principles 4](#_Toc96608897)

[2.1. IS threats 4](#_Toc96608898)

[2.2. Adversary model 4](#_Toc96608899)

[1. Testing results 5](#_Toc96608900)

[1.1. Statistics 5](#_Toc96608901)

[1.2. Summary 5](#_Toc96608902)

[1.3. Found vulnerabilities list 5](#_Toc96608903)

[1.3.1. {name} 5](#_Toc96608904)

[3. Appendix. Security assessment. Background information 8](#_Toc96608905)

[3.1. Security level analysis 8](#_Toc96608906)

[3.2. Vulnerability severity 8](#_Toc96608907)

[3.3. Ease of vulnerability exploitation 8](#_Toc96608908)

[3.4. Vulnerability accessibility 9](#_Toc96608909)

[3.5. Likelihood of exploitation 10](#_Toc96608910)

[3.6. Vulnerability impact 10](#_Toc96608911)

1. Introduction
   1. Project info

Name: {project.name}

Date: {project.startDate} - {project.endDate}

Scope: {project.scope}

Description: {project.description}

* 1. General provisions

{#wiki.byName["General provisions"]}

{@wiki.byName["General provisions"].rendered}

{/}

{^wiki.byName["General provisions"]}

The given expert report represents the results of the security assessment of the group of resources and provides recommendations on how to eliminate discovered vulnerabilities and improve overall security of the System.

{/}

* 1. Summary

{#wiki.byName["Summary"]}

{@wiki.byName["Summary"].rendered}

{/}

{^wiki.byName["Summary"]}

During the assessment, the experts used the model of the external adversary, who has some knowledge about the System. As a result, they discovered one vulnerability of a high severity level. Successful exploitation of the vulnerability can enable the adversary to perform requests on behalf of the user provided that the user has visited a malicious page owned by the adversary. As a result, the adversary can create trading accounts, specify additional email for the user’s account and perform other actions on behalf of the user.

During the assessment, the auditors didn’t find any vulnerabilities that allowed for gaining direct access to the System’s servers.

Below, you can find specification of the discovered vulnerabilities and associated security threats as well as detailed recommendations on how to fix the vulnerabilities.

{/}

1. Security assessment principles
   1. IS threats

{#wiki.byName["IS threats"]}

{@wiki.byName["IS threats"].rendered}

{/}

{^wiki.byName["IS threats"]}

The Company’s information resources may be affected by threats to the following three security areas: confidentiality, integrity, and availability.

The impact on confidentiality implies the disclosure of the Company’s confidential information, i.e. the information becomes available to those who should not have access to it, including the Company’s employees, clients, partners, competitors, and third parties.

The impact on integrity implies the modification of information so that its structure and/or meaning are changed, or information is partially or fully destroyed.

The basic principle of conducting a security audit is to test the possibility of carrying out the aforementioned threats against the System’s information resources according to a chosen adversary model.

{/}

* 1. Adversary model

{#wiki.byName["Adversary model"]}

{@wiki.byName["Adversary model"].rendered}

{/}

{^wiki.byName["Adversary model"]}

A person or a group who can carry out security threats and attempt to compromise the information resources of the System and damage the Company’s interest, acting in collusion or separately, with or without malicious intent, are considered to be a potential adversary.

By security threats, we consider threats that can lead to violations of confidentiality and integrity of information, as well as the System’s denial of service.

The adversary acting on purpose may pursue the following goals and their possible combinations:

* denial of service;
* privilege escalation;
* unauthorized access to business-critical information.

The security assessment was conducted on the basis of the external adversary model.

{/}

1. Testing results
   1. Statistics

|  |  |
| --- | --- |
| **Total score** | **Amount** |
| High | {issues | where: ‘totalScore === 3’ | length} |
| Medium | {issues | where: ‘totalScore === 2’ | length} |
| Low | {issues | where: ‘totalScore === 1’ | length} |
| **Total detected** | **{issues | prop: ’length’}** |

* 1. Summary

| **Issue name** | **Criticality** | **Probability** | **Total score** |
| --- | --- | --- | --- |
| {#issues | sortByDesc: ’totalScore’}{name} | {#criticalityScore===3}High {/}{#criticalityScore===2}Medium {/}{#criticalityScore===1}Low {/} | {#probabilityScore===3}High {/}{#probabilityScore===2}Medium {/}{#probabilityScore===1}Low {/} | {#totalScore===3}High {/}{#totalScore===2}Medium {/}{#totalScore===1}Low {/}{/} |

* 1. Found vulnerabilities list

{#issues | sortByDesc: 'totalScore'}

* + 1. {name}

Criticality: {#criticalityScore===3}High {/}{#criticalityScore===2}Medium {/}{#criticalityScore===1}Low {/}

Probability: {#probabilityScore===3}High {/}{#probabilityScore===2}Medium {/}{#probabilityScore===1}Low {/}

Total risk: {#totalScore===3}High {/}{#totalScore===2}Medium {/}{#totalScore===1}Low {/}

{#generalDescription.length}

Description

{@generalDescription}

{/}

{#risksDescription.length}

Risks

{@risksDescription}

{/}

{@techOverallLenght = technicalDescription.length + hostnames.length + ips.length + requests.length + attachedImages.length}

{#techOverallLenght}

Technical description

{@allHostsLength = hostnames.length + ips.length}

{#allHostsLength}

Vulnerable host(s):

{#hostnames}

* {.}

{/}

{#ips}

* {.}

{/}

{/}

{#technicalDescription.length}

{@technicalDescription}

{/}

{#requests.length}

HTTP Requests:

{#requests}

Request:

{request}

Response:

{response}

{/}

{/}

{#attachedImages}

{%path}

Figure 1. {caption}

{/attachedImages}

{/}

{#reproduceDescription.length}

Reproduce

{@reproduceDescription}

{/}

{#recommendations.length}

Recommendations

{@recommendations}

{/}

{/}

1. Appendix. Security assessment. Background information
   1. Security level analysis

To analyze the security level of the System, it is necessary to measure severity and likelihood of exploitation of the detected vulnerabilities. The likelihood of exploitation is measured, according to the ease of vulnerability exploitation and the accessibility of a vulnerability.

* 1. Vulnerability severity

The “Severity” property of a vulnerability describes possible results of this vulnerability exploitation, regarding confidentiality, integrity, and availability of information processed on a vulnerable resource. Severity levels are described in the Table A-1.

Table A–1. Severity levels

|  |  |  |  |
| --- | --- | --- | --- |
| Severity level | Confidentiality  violation | Integrity violation | Availability violation |
| None | Doesn’t happen | Doesn’t happen | Doesn’t happen |
| Low | Obtaining access to noncritical information by an attacker through privilege escalation | Integrity violation of noncritical information by an attacker with basic user rights in the System | Short-time denial-of-service of a mission-critical application |
| Average | Confidentiality violation of sensitive data by an attacker with basic user rights in the System | Integrity violation of sensitive data by an attacker with basic user rights in the System | Denial of service of a mission-critical application or a short-time denial of service of the System |
| High | Confidentiality violation of critical information by an attacker with administrator rights in the System | Integrity violation of critical information by an attacker with administrator rights in the System | Denial of Service of the System |

* 1. Ease of vulnerability exploitation

The “Ease of exploitation” property of a vulnerability defines what hardware and software, time and computing resources, and professional skills are required to exploit a vulnerability (Table A-2).

Table A–2. Ease of vulnerability exploitation levels

|  |  |
| --- | --- |
| Level | Description |
| Low | Vulnerability exploitation requires high computing powers, significant time resources, developing new software, configuration analysis of the System, determination and testing possible ways and conditions of successful exploitation of this vulnerability. |
| Average | Vulnerability exploitation requires high-performance computing, extensive time resources, special hardware and software, and analysis of a violated system configuration. An attacker does not have to have deep knowledge of the system or professional skills to perform an attack. |
| High | Vulnerability exploitation does not require the use of any special hardware or software, high-performance computing, time resources or any professional skills to perform an attack. |

* 1. Vulnerability accessibility

The “Accessibility” property of a vulnerability defines what user classes have access to a vulnerable resource (Table A-3).

Table A–3. Accessibility levels

|  |  |
| --- | --- |
| Level | Description |
| Low | Privileged users |
| Average | Registered users |
| High | All users |

* 1. Likelihood of exploitation

The likelihood of exploitation is calculated according to “ease of exploitation” and “accessibility” levels (Table A–4).

Table A–4. Likelihood of exploitation levels

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Likelihood of exploitation | | Ease of exploitation | | |
| Low | Average | High |
| Accessibility | Low | Low | Low | Average |
| Average | Low | Average | High |
| High | Average | High | High |

* 1. Vulnerability impact

Vulnerability impact (for one of the existing threats) is measured, according to vulnerability severity (for one of the existing threats) and the likelihood of exploitation of a vulnerability (Table A-5).

Table A–5. Vulnerability impact levels

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vulnerability impact | | Likelihood of exploitation | | |
| Low | Average | High |
| Vulnerability severity | Low | Low | Low | Average |
| Average | Low | Average | High |
| High | Average | High | High |