LEXFO

Audit Report

Retest #2

KIZEO

Ref KIZ20201125

DOCUMENT REFERENCES

Document status		
Version	Date	Status
V 1.0	2020-07-17	Valid document
V 1.1	2020-11-09	Retest #1
V 1.2	2020-11-25	Retest #2

Contacts		
LEXFO contacts	Position	Email
Samuel DRALET	CEO	s.dralet@lexfo.fr
Hugo CHAUVIERE	Head of Operations	h.chauviere@lexfo.fr

TABLE OF CONTENTS

1 Introduction

1.1 Context and objectives

CLIENT wishes to ensure that the security of **KIZEO** does not introduce vulnerabilities in its network environment.

For this purpose, the **LEXFO** auditors carried out the necessary tests to:

- Check that the software does not reduce the security of the environment.
- Verify that data input may not compromise the application.
- Verify that data used by the component may not be compromised by an attacker.

1.2 Organization

This **initial audit** was performed **from the 6th to the 10th of July 2020**.

This audit, was followed by two retests:

- **The first retest** was performed **on the 11th of November 2020**
- **The second retest** was performed **on the 24th of November 2020**

The application analysis was divided into features in order to follow the end-to-end process and ensure vulnerability assessment could be done in all security mechanisms and protections.

Our experts analyzed the application with a black-box approach, i.e. without knowing any login nor authentication information. Then, they followed a grey-box approach using credentials provided by **KIZEO**.

Regarding retests, those are aimed at verifying the proper mitigation of vulnerabilities that were initially discovered. As these are targeted tests, the application has not been fully re-audited during this process (e.g.: added or updated functionalities).

1.3 Scope

The audit scope included the following resources:

- https://accounts-preprod-wip.kizeo.com/
- https://forms-preprod-wip.kizeo.com/

1.4 Tools and methodology

LEXFO uses manual techniques during all security audits (information gathering, research and development, intrusion testing, etc.). Most of the tools are either freely available on the Internet -grabbed from the hacking community- or specifically developed for the mission, therefore included in the Appendix part of this report.

2 Synthesis

2.1 Executive summary

During the security assessments 5 vulnerabilities were found. Namely 2 high and 3 medium risks. The overall security level was ranked as improvable.

During the following retests, all issues that were discovered in the initial audit and the first retest were mitigated.

The overall security level is now ranked as **excellent**.

2.2 Positive results

During the assessment, the following positive elements have been encountered.

TITLE	DESCRIPTION
Lack of SQL injection	The application is based on the Laravel framework, and the filtering of input parameters used in SQL queries seems to be done correctly. No SQL injection was found during the assessment.
Lack of XXE	The application rarely uses XML format in the HTTP requests and whenever it does, it was found that the parsing is done securely, no XXE vulnerabilities were found.

3 Tests description

3.1 Discovery phase

3.1.1 Description

LEXFO auditors simulate the actions of an attacker wishing to obtain a maximum of technical information on the internal network of the audit. This information may allow the attacker to discover a forgotten source code archive, displaying a vulnerable version of technology or simply to facilitate a future attack by targeting the different technologies discovered.

3.1.2 Tests

During this phase, the following security tests are performed (non-exhaustive listing):

- TCP/UDP scans;
- ICMP exchanges (Traceroute, Ping);
- Network cartography;
- Detection of reverse proxies, WAF, load balancers

3.2 Black-box phase

3.2.1 Description

LEXFO auditors simulate the actions of an attacker wishing to attack the internal network without knowledge of the network architecture. The only information known is the one obtained during the discovery phase.

3.2.2 Tests

During this phase, the following security tests are performed (non-exhaustive listing):

- HTTP methods;
- Banner and version grabbing;
- Resource listing;
- SSL configuration;

3.3 Grey-box phase

1.1.1 Description

LEXFO auditors simulate the actions of an attacker wishing to attack the application with valid credentials.

1.1.2 Tests

During this phase, the following security tests are performed (non-exhaustive listing):

- Analysis of information leaks:
  - Comprehensive search of directories and files;
  - Analysis of HTTP error codes (version fingerprint, WAF detection);
  - Backup file test;
  - Search of application framework interfaces;
  - Search of applications (owner spider);
  - Search of domains (HTTP and DNS owner spiders).

These analyses give information on the different scripts of the application. The following tests specific to Web applications are performed on these scripts to discover vulnerabilities:

- Tests for *path traversal*;
- Tests for *directory listing*;
- Path disclosure;
- SQL Injection;
- HTTP Splitting;
- Cross-Site Scripting;
- CSRF;
- Sensitive data interception;
- Data partition check;
- Etc.

Vulnerabilities affecting the remote environment are also tracked on dedicated websites, such as: http://cve.mitre.org and http://www.cvedetails.com.

4 Matrix description

4.1 Vulnerability table

Vx	Vulnerability	**RISK** Level of risk
CONSEQUENCES *Short description of potential and direct consequences related to the vulnerability.*		
APPLICATION(S)/SERVER(S) *List of affected servers or applications.*		
MITIGATION *Recommendations mitigating the issue*		
EXPLOITABILITY *(see below)*	**IMPACT** *(see below)*	**CORRECTION DIFFICULTY** *(see below)*

4.2 Metrics

Global security level (used in the executive summary)	
Excellent	**No vulnerability or only one low-level vulnerability** was found on the audited scope because of the effective implementation of security mechanisms.
Acceptable	**Only low-level vulnerabilities** were identified during the audit. The overall security level of the audited scope prevents compromise of data even by an experienced attacker.
Improvable	**One or more medium-level vulnerabilities** were discovered during the audit. These vulnerabilities could be exploited by an experienced attacker wishing to damage the client's image.
Insufficient	**One or more high-level vulnerabilities and/or only one critical vulnerability** were identified during the audit. The impacts for the client may be important (data theft, brand image damage, etc.), but do not lead to the compromise of the audited scope.
Critical	**One or more critical vulnerabilities** leading to a total compromise of the audited scope and/or with significant impacts, whether technical (total unavailability of the service, data confidentiality, etc.) or business impacts (brand image or financial damages, etc.) were found.

Correction difficulty	
Complex	Sharp computer skills, a lot of time or important financial resources are needed.
Moderate	Comprehensive computer knowledge, a little time and limited financial means are necessary.
Simple	Little knowledge, resources and time are required.

Impact	
Insignificant	The impacts can be overcome without difficulty.
Limited	The impacts can be overcome with some difficulties.
Important	The impacts can be overcome with serious difficulties.
Critical	Impacts are potentially insurmountable.

Exploitability	
Very difficult	Exploitation of unpublished vulnerabilities requiring security expertise of information systems and the development of specific and targeted tools.
Difficult	Exploitation of public vulnerabilities requiring security expertise of information systems and the development of simple tools.
Moderate	Exploitation requiring simple techniques and/or publicly available tools.
Easy	Trivial exploitation, without any specific tools.

Risk level (calculated according to likelihood and impact)	
Critical	Critical risk for the information system and requiring an immediate correction or imposing an immediate stop of the service
High	Major risk on the information system requiring a short-term correction
Medium	Risk moderated on the information system and requiring a medium-term correction
Low	Low risk on the information system and being able to require a correction

4.3 Risk computing

		Exploitability			
		Very Difficult	Difficult	Moderate	Easy
Impact	Insignificant	Low	Low	Medium	High
	Limited	Low	Medium	Medium	High
	Important	Medium	High	High	Critical
	Critical	Medium	High	Critical	Critical