1. Client Notification: Penetration Test

This document summarizes the results of a performed penetration test for lawcode GmbH (in the following also called „lawcode “). The purpose of the penetration test was to gain an overview of the current security status of the “Hintbox” web application and its underlying IT infrastructure. The goal was to identify vulnerabilities, give an overview of the identified findings and to give a recommendation for minimizing these risks.

The following tests were included in the project scope:

» **Penetration test of web applications:** From the perspective of an external attacker with and without access credentials (grey-box), including an automated vulnerability scan.

- Pentest-ID: LAWCODEPT-10
- Scope: „Hintbox“ web application
- Application URL: https://pentestfactory-q2-2023.hintbox.de
  - including an assessment of the SSO mechanism using an exemplary Keycloak instance at: https://keycloak-staging.hintbox.eu
- Testing period: 14.06.2023 until 16.06.2023

1.1. Risk Assessment – Web Application

The illustration on the left represents the overall risk of the analyzed test object and is based on the highest risk rating "**VERY LOW**" of an identified finding.

During the test, no vulnerabilities with a medium, high, or critical risk were identified. A successful compromise of the „Hintbox” web application is therefore considered unlikely.

Pentest Factory GmbH – Geldern, 19.06.2023

Andres Rauschecker
Digitally signed by Andres Rauschecker
DN: cn=Andres Rauschecker, c=DE, o=Pentest Factory GmbH, email=andres.rauschecker@pentestfactory.com
Date: 2023.06.19 15:11:32 +02'00'

Andres Rauschecker
[Senior Penetration Tester]

Laurent Vetter
Digitally signed by Laurent Vetter
DN: cn=Laurent Vetter, c=DE, o=Pentest Factory GmbH, email=laurent.vetter@pentestfactory.com
Date: 2023.06.19 15:14:18 +02'00'

Laurent Vetter
[Team Lead Pentesting]

2. Assignment and Background

2.1. Project Background

lawcode GmbH wants to ensure confidentiality, integrity and availability of IT-assets within their IT-infrastructure. To determine the current security level of the “Hintbox” web application, Pentest Factory GmbH was hired to perform a penetration test.

2.2. Project Goal, Scope and Methodology

The objective of this penetration test was to identify potential security vulnerabilities that could impact the confidentiality, integrity and availability of information processed by the target IT infrastructure or asset in scope. This chapter describes the services performed within the project.

Penetration test of web applications

The “Penetration test of web applications” included a comprehensive security analysis of the “Hintbox” web application at the network and application level. Our tests at the network level included an automated vulnerability scan as well as a manual analysis of all network services provided by the application server from the perspective of an external attacker (black box). The application-level tests were performed using a semi-manual approach with and without valid user access credentials (grey-box). The execution of our tests did not interfere with public services or business operations.

2.3. Applied Methodologies for Penetration Tests

When carrying out penetration tests, Pentest Factory GmbH follows the proven test specifications of OWASP and OSSTMM.

Within infrastructure tests, the following tests were performed:

» Passive analysis of publicly available information about the target organization

» Identification of available network services and manual security analysis

» Automated vulnerability scans of the target infrastructure and verification of findings

For application testing, all typical tests described in the OWASP Testing Guide (Version 4) [1] have been performed, including:

» Information gathering

» Testing configuration and deployment management

» Identity & Access Management (IAM), Session and Authentication testing

» Input and output validation tests

» Privilege escalation, cryptography, error handling and plausibility checks

[1] https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents