1. Client Notification: Penetration Test

This document summarizes the results of performed penetration tests for lawcode GmbH (in the following also called „lawcode“). The purpose of the penetration tests was to gain an overview of the current security status of the lawcode Suite and its underlying IT infrastructure. The platform consists of three application components, namely “Hintbox”, “Supplier Manager” and “CSRD”. 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 tests of web applications** from the perspective of an external attacker with and without access credentials (grey-box), including an automated vulnerability scan.
  – Pentest-IDs: LAWCODEPT-12, LAWCODEPT-13, LAWCODEPT-14, LAWCODEPT-15
  – Scope: lawcode Suite (Hintbox, Supplier Manager, CSRD)
  – Application URLs:
    ○ https://2024-q3-pentest.lawcode.cloud/hbx/ (49.12.21.166)
    ○ https://2024-q3-pentest.lawcode.cloud/suma/ (49.12.21.166)
    ○ https://2024-q3-pentest.lawcode.cloud/csrd/ (49.12.21.166)
  – Testing period: August 2024 and October 2024

1.1. Risk Assessment – lawcode Suite

The illustration on the left represents the overall risk of the analyzed test object after conducting the penetration tests.

During our assessment, no remaining security issues were identified in the lawcode Suite. A successful compromise of the lawcode Suite is therefore considered very unlikely and is rated as “**VERY LOW**” risk.

Pentest Factory GmbH
Frankfurt am Main – 06.11.2024

Laurent Vetter
Digitally signed by Laurent Vetter
DN: cn=Laurent Vetter, c=DE, o=Pentest Factory GmbH, email=laurent.vetter@pentestfactory.com
Reason: I am approving this document
Date: 2024.11.06 09:49:29 +01'00'

Laurent Vetter
[Team Lead Pentesting, ppa.]

Andres Rauschecker
Digitally signed by Andres Rauschecker
DN: cn=Andres Rauschecker, c=DE, o=Pentest Factory GmbH, email=andres.rauschecker@pentestfactory.com
Date: 2024.11.06 09:48:35 +01'00'

Andres Rauschecker
[Senior Penetration Tester]

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 lawcode Suite, Pentest Factory GmbH was hired to perform multiple penetration tests.

2.2. Project Goal, Scope and Methodology

The objective of these penetration tests 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 tests of web applications

The penetration tests included a comprehensive security analysis of the “lawcode Suite” web application at the network and application level. The platform consists of three application components called “Hintbox”, “Supplier Manager” and “CSRD”. 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).

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