1. Customer Notice – Penetration Test

This document describes the results of the penetration tests conducted for lawcode GmbH (in the following also called „lawcode“). The purpose of the penetration tests was to obtain an overview of the current security posture of the Hintbox web application and its underlying IT infrastructure. The goal was to identify security issues, give an overview of identified vulnerabilities and to issue recommendations for the mitigation of these risks.

The following tests were conducted within the project scope:

» **Penetration test of web applications** from the perspective of an external attacker with and without valid credentials (grey-box), including an automated vulnerability scan.
  – Pentest-ID: LAWCODEPT-7
  – Scope: Hintbox web application
  – Application-URL: https://2022-q2-pentestfactory.hintbox.de/
  – Testing period: 31.05.2022 - 03.06.2022

» **Re-Test** of findings identified in the previously conducted penetration test of web applications to verify the effectivity of implemented mitigation measures.
  – Pentest-ID: LAWCODEPT-8
  – Scope: Hintbox web application
  – Application-URL: https://2022-q2-pentestfactory.hintbox.de/
  – Testing period: 22.06.2022

1.1. Risk Assessment – Hintbox Web Application

The illustration on the left depicts the overall risk of the analysed test object after the re-test. Since all previously identified vulnerabilities have been mitigated completely, the overall risk rating is considered „**VERY LOW**“.

A successful compromise of the Hintbox web application is thus considered to be very unlikely.

Pentest Factory GmbH – Geldern, 22.06.2022

Andres Rauschecker
Digitally signed by Andres Rauschecker
DN: cn=Andres Rauschecker, c=DE, o=Pentest Factory GmbH, email=andres.rauschecker@pentestfactory.com
Reason: I am the author of this document
Date: 2022.06.22 16:06:27 +02'00'

Andres Rauschecker
[Senior Penetration Tester]

Laurent Vetter
Digital signiert von Laurent Vetter
DN: cn=Laurent Vetter, c=DE, o=Pentest Factory GmbH, email=laurent.vetter@pentestfactory.com
Datum: 2022.06.22 15:45:35 +02'00'

Laurent Vetter
[Senior Penetration Tester]

2. Assignment and Background

2.1. Project Background

lawcode 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 including a re-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 within the Hintbox web application and its underlying IT infrastructure.

Grey-box 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).

Re-Test

The re-test included a verification of mitigation measures of the findings identified in the previously conducted penetration test.

2.3. Methodology

Within infrastructure tests, the following tests were performed:

» Passive analysis of publicly available information about the target organization

» Identification of available network services & manual security analysis of identified services

» Automated vulnerability scans of the infrastructure defined in the scope of the project

» Manual verification of the findings identified in the vulnerability scan

For application testing, all typical tests of the OWASP Guide (v4)[1] have been performed, including:

» Information gathering

» Testing configuration and deployment management

» Identity and Access Management (IAM) testing, tests of authentication procedures, authorization & session management

» Input and output validation tests

» Testing vulnerabilities that lead to privilege escalation

» Cryptography, Error handling & Plausibility checks

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