1. Kundenmitteilung Penetrationstest

Dieses Dokument beschreibt die Ergebnisse des Penetrationstests für die lawcode GmbH (im Folgenden auch als „lawcode“ bezeichnet). Zweck des Penetrationstests war es, einen Überblick über den aktuellen Sicherheitsstatus der „Hintbox“ Webanwendung und unterliegenden IT-Infrastruktur von lawcode zu erhalten. Das Ziel bestand darin, Sicherheitsmängel zu identifizieren, eine Übersicht über die erkannten Schwachstellen zu erstellen sowie Empfehlungen zur Minimierung dieser Risiken zu geben.

Die folgenden Tests waren Bestandteil des Projekts:

» **Penetrationstest von Webanwendungen** aus der Perspektive eines externen Angreifers mit und ohne Zugangsdaten (Grey-Box) inklusive eines automatisierten Schwachstellenscans.
  – Pentest-ID: LAWCODEPT-10
  – Prüfumfang: „Hintbox“ Webapplikation
  – Anwendungs-URL: https://pentestfactory-q2-2023.hintbox.de
    – inklusive einer Überprüfung des SSO-Mechanismus über eine beispielhafte Keycloak Instanz unter: https://keycloak-staging.hintbox.eu
  – Durchführungszeitraum: 14.06.2023 bis 16.06.2023

1.1. Risikobeurteilung – Webanwendung

Die nebenstehende Illustration stellt das Gesamtrisiko des getesteten Prüfobjekts zum Zeitpunkt des Penetrationstests dar und basiert auf der höchsten Risikoeinstufung „**SEHR GERING**“ einer identifizierten Feststellung.

Während unserer Tests wurden keine Sicherheitsprobleme mit einem mittleren, hohen oder kritischen Risiko identifiziert. Eine erfolgreiche Kompromittierung der Hintbox Webanwendung ist demnach als unwahrscheinlich anzusehen.

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 15:16:05 +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 15:15:13 +02'00'

Laurent Vetter
[Team Lead Pentesting]

2. Auftrag und Hintergrund

2.1. Projekthintergrund

Die lawcode GmbH möchte die Vertraulichkeit, Integrität und Verfügbarkeit ihrer IT-Assets innerhalb der IT-Infrastruktur sicherstellen. Zur Ermittlung des aktuellen Sicherheitsstands der „Hintbox“ Webanwendung wurde die Pentest Factory GmbH mit der Durchführung eines Penetrationstests beauftragt.

2.2. Ziel, Umfang und Methodik des Projekts

Das Ziel des Tests bestand darin, mögliche Sicherheitsschwächen zu identifizieren, welche Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit, der innerhalb der „Hintbox“ Webanwendung und unterliegenden IT-Infrastruktur verarbeiteten Informationen haben.

Penetrationstest von Webanwendungen

Der Penetrationstest beinhaltete eine umfassende Sicherheitsanalyse der „Hintbox“ Webanwendung auf Anwendungs- und Netzwerkebene. Unsere Tests auf Netzwerkebene beinhalteten einen automatisierten Schwachstellenscan sowie eine manuelle Analyse aller bereitgestellter Netzwerkdienste aus der Perspektive eines externen Angreifers (Black-Box). Die Tests auf Anwendungsebene wurden mit einem semi-manuellen Ansatz mit und ohne gültige Nutzerzugangsdaten (Grey-Box) durchgeführt.

2.3. Angewandte Methodiken bei der Durchführung des Penetrationstests

Innerhalb von Infrastrukturtests wurden die folgenden Tests durchgeführt:

» Identifikation von verfügbaren Netzwerkdiensten

» Manuelle Sicherheitsanalyse der identifizierten Netzwerkdienste

» Automatisierte Schwachstellenscans der im Umfang des Projekts definierten Infrastruktur

» Manuelle Verifizierung der im Schwachstellenscan identifizierten Feststellungen

Für Anwendungstests wurden alle Tests des OWASP Testing Guides[1] durchgeführt:

» Informationsbeschaffung

» Testen des Konfigurations- und Bereitstellungsmanagements

» Testen des Identitätsmanagements, Session-Managements und Authentifizierungsverfahren

» Tests der Berechtigungen, Kryptographie und Fehlerbehandlung

» Tests der Eingabe- und Ausgabevalidierung

» Plausibilitätsprüfung und Tests der Client-Seite

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