1. Kundenmitteilung Penetrationstest

Dieses Dokument beschreibt die Ergebnisse des Penetrationstests für die lawcode GmbH (im Folgenden auch als „lawcode“ bezeichnet). Zweck der Penetrationstests war es, einen Überblick über den aktuellen Sicherheitsstatus der „lawcode Suite“ und unterliegenden IT-Infrastruktur zu erhalten. Die Plattform besteht aus drei Anwendungskomponenten namens „Hintbox“, „Supplier Manager“ und „CSRD“. 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:

» **Penetrationstests von Webanwendungen** aus der Perspektive eines externen Angreifers mit und ohne Zugangsdaten (Grey-Box), inklusive eines automatisierten Schwachstellenscans.

- Pentest-IDs: LAWCODEPT-12, LAWCODEPT-13, LAWCODEPT-14, LAWCODEPT-15
- Prüfumfang: lawcode Suite (Hintbox, Supplier Manager, CSRD)
- Anwendungs-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)
- Durchführungszeitraum: August 2024 und Oktober 2024

1.1. Risikobeurteilung – lawcode Suite

Die nebenstehende Illustration stellt das Gesamtrisiko des getesteten Prüfobjekts nach Durchführung der Pentests dar.

Während unserer Überprüfungen wurden keine Sicherheitsprobleme in der lawcode Suite identifiziert. Eine erfolgreiche Kompromittierung der lawcode Suite gilt demnach als sehr unwahrscheinlich und wird mit dem Risiko „**SEHR GERING**“ bewertet.

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 09:42:12 +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 09:47:54 +01'00'

Andres Rauschecker
[Senior Penetration Tester]

2. Auftrag und Hintergrund

2.1. Projekthintergrund

Die lawcode GmbH möchte die Vertraulichkeit, Integrität und Verfügbarkeit seiner IT-Assets innerhalb seiner IT-Infrastruktur sicherstellen. Zur Ermittlung des aktuellen Sicherheitsstands seiner lawcode Suite wurde die Pentest Factory GmbH mit der Durchführung von 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 lawcode Suite und unterliegenden IT-Infrastruktur verarbeiteten Informationen haben.

Penetrationstests von Webanwendungen

Die Penetrationstests beinhalteten eine umfassende Sicherheitsanalyse der „lawcode Suite“ auf Anwendungs- und Netzwerkebene. Die Plattform besteht aus drei Anwendungskomponenten namens „Hintbox“, „Supplier Manager“ und „CSRD“. 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