1. Kundenmitteilung Penetrationstest

Dieses Dokument beschreibt die Ergebnisse der Penetrationstests für die lawcode GmbH (im Folgenden auch als „lawcode“ bezeichnet). Zweck der Penetrationstests war es, einen Überblick über den aktuellen Sicherheitsstatus der Hintbox Webanwendung sowie der 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:

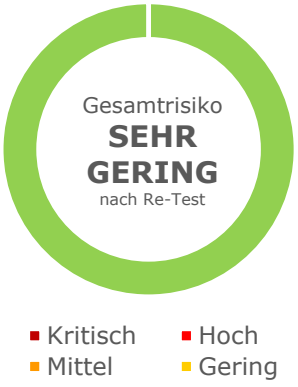
» **Penetrationstest von Webanwendungen** aus der Perspektive eines externen Angreifers mit und ohne Zugangsdaten (Grey-Box), inklusive eines automatisierten Schwachstellenscans.

- Pentest-ID: LAWCODEPT-7
- Prüfumfang: Hintbox Hinweisgebersystem
- Anwendungs-URL: https://2022-q2-pentestfactory.hintbox.de/
- Durchführungszeitraum: 31.05.2022 bis 03.06.2022

» **Wiederholungsprüfung (Re-Test)** des zuvor durchgeführten Penetrationstests von Webanwendungen zur Verifizierung der Effektivität von Behebungsmaßnahmen.

- Pentest-ID: LAWCODEPT-8
- Prüfumfang: Hintbox Hinweisgebersystem
- Anwendungs-URL: https://2022-q2-pentestfactory.hintbox.de/
- Durchführungszeitraum: 22.06.2022

1.1. Risikobeurteilung – Hintbox Webanwendung



Die nebenstehende Illustration stellt das Gesamtrisiko des getesteten Prüfobjekts nach Durchführung der Wiederholungsprüfung dar. Da alle zuvor identifizierten Schwachstellen vollständig behoben wurden, wird eine Risikoeinstufung von „**SEHR GERING**“ vergeben.

Eine erfolgreiche Kompromittierung der Hintbox Webanwendung ist demnach als sehr unwahrscheinlich anzunehmen.

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 16:06:50 +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 15:45:47 +02'00'

Laurent Vetter
[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 der Hintbox Webanwendung wurde die Pentest Factory GmbH mit der Durchführung eines Penetrationstests inklusive Wiederholungsprüfung 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 darunterliegenden 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.

Wiederholungsprüfung (Re-Test)

Die Wiederholungsprüfung beinhaltete die Verifizierung durchgeführter Maßnahmen zur Behebung identifizierter Schwachstellen des zuvor durchgeführten Penetrationstests.

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