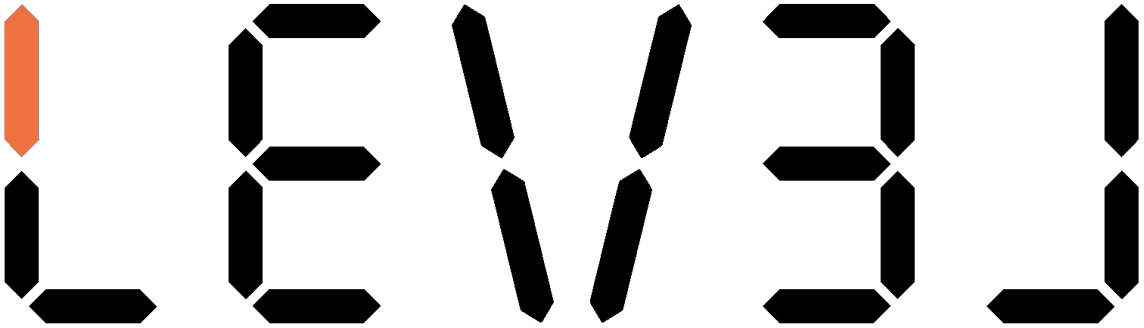


$Kundenname
$Projektname
Penetrationstest Report
$Datum

Dokumentenversion

Version	Datum	Author	Kommentar
1.0	202X-0X-0X	Samuel Alp	Initiale Dokumentenversion

Inhaltsverzeichnis

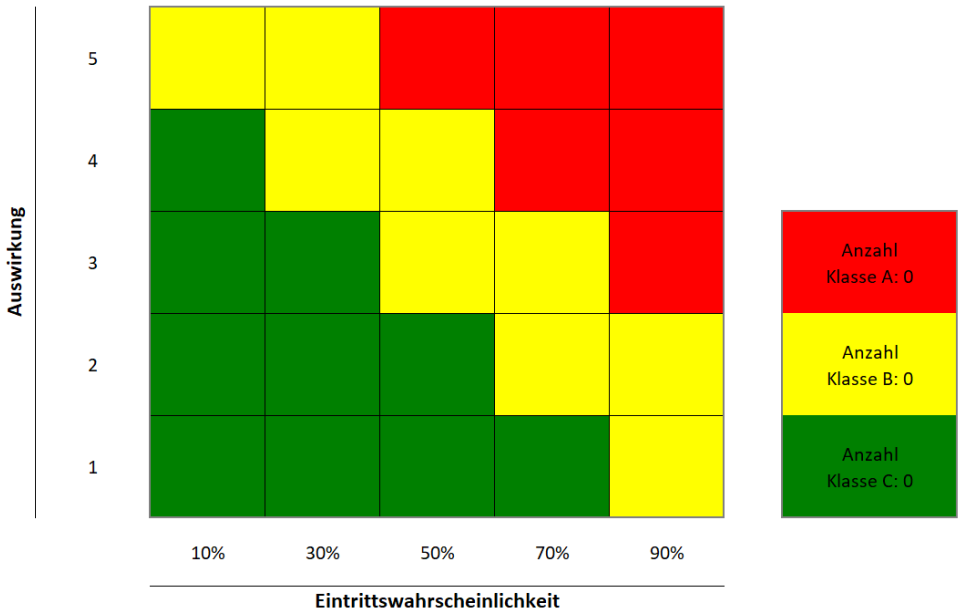
Executive Summary

Test Parameter

Test Ref.	$Testref
Datum	$TestDate
Testzeiten	$TestTimes
Testarten	$TestTypes
Limitationen	Kein Denial of Service Kein Social Engineering
Personal	Samuel Alp (CAP, CompTIA Sec+, CISSP)

Übersicht

Risiko	Funde
Kritisch	0
Hoch	1
Medium	0
Niedrig	1
Empfehlungen	2
Gesamt	**4**



Zusammenfassung

Die **LEV3L GmbH** führte eine umfassende Sicherheitsbewertung von **$kundenname** durch, um bestehende Schwachstellen zu identifizieren und das aktuelle Sicherheitsrisiko im Zusammenhang mit der Umgebung und den eingesetzten Technologien zu ermitteln. Diese Bewertung nutzte gängige **Penetrationstest-Techniken**, um dem Management von **$kundenname** ein Verständnis für die Risiken und die Sicherheitslage ihres Unternehmensumfelds zu vermitteln.

Im Rahmen des Tests konnten sowohl sicherheitsrelevante Schwachstellen als auch Konfigurationsschwächen identifiziert werden. Die Befunde variieren in ihrer Kritikalität und betreffen unterschiedliche Bereiche der geprüften Umgebung. Zusätzlich wurden Maßnahmen zur Härtung einzelner Komponenten empfohlen, um das allgemeine Sicherheitsniveau weiter zu verbessern. Die Ergebnisse unterstreichen die Bedeutung regelmäßiger Sicherheitsüberprüfungen und bieten konkrete Anhaltspunkte zur Risikominderung.

LEV3L führte einen Penetrationstest der Anwendungen von **$kundenname** durch. Dieser wurde aus einer authentifizierten Perspektive durchgeführt und orientierte sich an anerkannten Sicherheitsstandards. Insgesamt zeigte sich, dass die Sicherheitslage der Anwendung verbesserungswürdig ist. Es wurden mehrere Schwachstellen mit hohem und mittlerem Risiko identifiziert, die die Integrität der Anwendung und ihrer Daten gefährden können und zeitnah behoben werden sollten.

Übersicht der Funde

Beschreibung	Risikobewertung	Ref
Veraltete Software Bibliotheken	Hoch	H-001
Schwache SSL Cipher Suites	Niedrig	N-001
Fehlende Cookie Flags	Empfehlung	E-001

Test-Rahmen

Scope

Der Penetrationstest wurde vom **$StartDate** bis zum **$EndDate** zu üblichen Geschäftszeiten (**10 Uhr – 17 Uhr**) ausgeführt.

Ziel des Tests waren:

- **https://$kundenwebsite.com**
    - Homepage
- **https://api.$kundenwebsite.com**
    - API
- **https://portal.$kundenwebsite.com**
    - Kundenportal

Die Untersuchungen erfolgten aus einer **Grey-Box-Perspektive**: Es wurde kein direkter Zugriff auf Quellcode oder interne Systeme gewährt, allerdings standen eingeschränkte Dokumentation und vorkonfigurierte Benutzerkonten für die Prüfung zur Verfügung. Diese Vorgehensweise erlaubt realistische Angriffe mit teilweise validen Zugangsdaten und spiegelt Angriffsvektoren wider, die einem authentifizierten Angreifer offenstehen könnten.

Im Rahmen des Tests genutzte Anmeldeinformationen

Benutzername	Passwort	Beschreibung
admin1@kunde.com	Passwort123!	Org 1 Admin Benutzer
editor1@kunde.com	Passwort123!	Org 1 Editor Benutzer
user1@kunde.com	Passwort123!	Org 1 Normaler Benutzer
admin2@kunde.com	Passwort123!	Org 2 Admin Benutzer
editor2@kunde.com	Passwort123!	Org 2 Editor Benutzer
user1@kunde.com	Passwort123!	Org 2 Normaler Benutzer

Limitationen

Im Rahmen dieses Penetrationstests wurden **Distributed-Denial-of-Service- (DDoS-)** Angriffe sowie **Social-Engineering-Methoden** bewusst nicht durchgeführt.

Beide Testarten lagen außerhalb des vereinbarten Leistungsumfangs und waren nicht Teil der durchgeführten Prüfaktivitäten. **DDoS-** und **Social-Engineering-Tests** erfordern besondere Abstimmungen, da sie mit erheblichen Risiken für den laufenden Betrieb beziehungsweise für Mitarbeitende verbunden sein können. **DDoS-Simulationen** bergen das Risiko von Ausfällen produktiver Systeme und werden deshalb nur unter streng kontrollierten Bedingungen durchgeführt.

Social-Engineering-Methoden wie Phishing oder Pretexting betreffen personenbezogene Daten und ethische Fragestellungen und setzen eine gesonderte Freigabe sowie vorbereitende Maßnahmen voraus. Aus diesen Gründen sind sie in regulären Penetrationstests nicht enthalten und werden nur bei ausdrücklicher Beauftragung separat durchgeführt.

Methodik

Der Penetrationstest kombinierte automatisierte Scans mit gezielten manuellen Prüfungen, um ein realistisches Bild der Sicherheitslage der geprüften Anwendungen zu erhalten.

Vorgehensweise in Kurzform:

- **Informationsbeschaffung:** Erfassung öffentlicher Informationen, Fingerprinting der Zieloberflächen und Ermittlung erreichbarer Eingabepunkte.
- **Erkennung und Analyse:** Einsatz von Schwachstellenscannern und manueller Prüfung zur Validierung potenzieller Befunde.
- **Verifikation / (gezielte) Ausnutzung:** Wo risikoverträglich, wurde die praktische Ausnutzbarkeit (Exploitation) geprüft, um tatsächliche Auswirkungen zu bestätigen. Produktive Störungen wurden vermieden.
- **Auswirkungsanalyse:** Bewertung der Vertraulichkeit, Integrität und Verfügbarkeit betroffener Komponenten sowie Einordnung möglicher Geschäftsfolgen.
- **Dokumentation und Empfehlungen:** Erstellung nachvollziehbarer Reproduktionsschritte, Risikoeinschätzungen und priorisierter Maßnahmen zur Behebung.

Die Prüfungen orientierten sich an anerkannten **Branchen- und Best-Practice-Leitfäden** sowie am zuvor vereinbarten Umfang, Zeitfenster und Testlevel. Alle eingesetzten Tools und Signaturen waren zum Testzeitpunkt auf aktuellem Stand. Nach Abschluss empfehlen wir **Nachtests** zur Verifikation umgesetzter Maßnahmen.

Die identifizierten Befunde wurden anhand der **OWASP Risk Rating-Methodik** bewertet. Dabei flossen Faktoren wie Exploitierbarkeit, Auftretenshäufigkeit, Entdeckbarkeit, technische Auswirkungen und geschäftliche Folgen in die Einstufung ein. Jeder Befund enthält deshalb eine **OWASP-konforme Risiko-Kategorie** sowie priorisierte Handlungsempfehlungen zur Minderung des jeweiligen Risikos.

Die Schwachstellen wurden mit dem **CVSS v3.1-Basiswert** bewertet (**Common Vulnerability Scoring System**). Zur Einordnung wurden die resultierenden **Basis-Scores** wie folgt kategorisiert:

0.0–3.9 (Niedrig) | 4.0–6.9 (Medium) | 7.0–8.9 (Hoch) | 9.0–10.0 (Kritisch)

Berichtete **CVSS-Werte** und die zugrundeliegenden **Vektor-Strings** sind pro Befund dokumentiert, um Nachverfolgbarkeit und Vergleichbarkeit sicherzustellen.

Funde

H-001: Veraltete Software Bibliotheken

Beschreibung

I

Risiko

OWASP Rating: High

CVSS Rating: 8.2

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N

Details

CVE-2020-11023

CVE-2020-11022

CVE-2020-7656

CVE-2018-18405

Empfehlung

Im Rahmen des Tests wurde festgestellt, dass in der Anwendung eine veraltete Version einer Softwarebibliothek verwendet wird. Der Einsatz veralteter Abhängigkeiten stellt ein grundsätzliches Sicherheitsrisiko dar, da ältere Versionen häufig bekannte Schwachstellen, Inkompatibilitäten oder nicht behobene Fehler enthalten können. Darüber hinaus verlieren viele Bibliotheken mit der Zeit den offiziellen Support, was bedeutet, dass sicherheitsrelevante Updates und Fehlerkorrekturen nicht mehr bereitgestellt werden.

Die Verwendung veralteter Komponenten erschwert nicht nur die Wartung und Weiterentwicklung der Anwendung, sondern erhöht auch die Angriffsfläche. In einigen Fällen sind für die identifizierte Version bereits öffentlich dokumentierte Sicherheitslücken bekannt. Zudem wird die betroffene Bibliothek in einem sicherheitsrelevanten Bereich der Anwendung eingesetzt.