**IFA**

**Penetration Test Report**

IFA

Informatiktechniker TS – Modul Cyber Security, 2024

Datum: xx.xx.2024

Dozent: Roman Camenzind

Verfasser / Student: x

# Inhaltsverzeichnis

[1. Inhaltsverzeichnis 2](#_Toc180945342)

[2. Executive Summary 3](#_Toc180945343)

[3. Scope 4](#_Toc180945344)

[4. Methode 5](#_Toc180945345)

[4.1 Ansatz 5](#_Toc180945346)

[4.2 Testebenen 5](#_Toc180945347)

[4.3 Testarten 5](#_Toc180945348)

[5. Findings 6](#_Toc180945349)

[5.1 Uebersicht 6](#_Toc180945350)

[5.2 Detailbeschreibung der Findings 6](#_Toc180945351)

[6. Risk Assessment 7](#_Toc180945352)

[6.1 Uebersicht 7](#_Toc180945353)

[7. Empfehlungen 8](#_Toc180945354)

[7.1 Empfohlene Sofortmassnahmen 8](#_Toc180945355)

[7.2 Langfristige Massnahmen 8](#_Toc180945356)

[7.3 Regelmässige Massnahmen 8](#_Toc180945357)

[8. Abbildungsverzeichnis 9](#_Toc180945358)

[9. Anhang 10](#_Toc180945359)

[9.1 Risikobewertungssystem 10](#_Toc180945360)

# Executive Summary

[Hauptinhalte:

Überblick über die Tests und deren Ergebnisse.

Priorisierung von Sicherheitsmaßnahmen.

Gesamtrisikoübersicht.

Zielgruppe: Management und Entscheider.]

# Scope

[Zielsystem: Definierte Anwendungen, Server und Netzwerke.

Testart: White-Box, Black-Box, oder Gray-Box Testing.

Testumgebung: Produktions- oder Staging-Systeme.

Ausnahmen und Einschränkungen: Angriffs- und Schwachstellen, die ausgeschlossen sind..]

# Methode

## Ansatz

[Testing Guidelines zum Beispiel: NITS SP 800-15 oder OWASP]

## Testebenen

[Getestete Ebenen zum Beispiel nach Schichten beschreiben z.Bsp: Netzwerkebene, Anwendung, Datenbank ]

## Testarten

[White-Box, Gray-Box, Black-Box ]

# Findings

## Uebersicht

|  |  |  |
| --- | --- | --- |
| Kategorie | Beschreibung / Bilder | Mitigation |
|  | Abb 5‑1; Attacke xy Diagramm |  |
|  |  |  |

## Detailbeschreibung der Findings

# Risk Assessment

## Uebersicht

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risiko ID | Beschreibung | Wahrscheinlichkeit | Auswirkung | Gesamt Risiko | Mitigation |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Empfehlungen

## Empfohlene Sofortmassnahmen

## Langfristige Massnahmen

## Regelmässige Massnahmen

# Abbildungsverzeichnis

Abb 5‑1; Attacke xy Diagramm 6

# Anhang

## Risikobewertungssystem

Die Bewertung der Risiken erfolgt anhand der Kombination aus **Likelihood (Wahrscheinlichkeit)** und **Impact (Auswirkung)**. Jede Schwachstelle wird auf einer Skala von **1 (niedrig)** bis **9 (hoch)** sowohl für die Wahrscheinlichkeit als auch die Auswirkung bewertet. (OWASP-Methode)

Die Gesamtbewertung ergibt sich durch Multiplikation dieser beiden Faktoren:

**Niedriges Risiko (<=20):** Schwachstellen mit geringer Wahrscheinlichkeit und/oder geringen Auswirkungen. Die Behebung kann in zukünftigen Wartungszyklen erfolgen.

**Mittleres Risiko (21-39):** Schwachstellen, die ein erhöhtes Risiko darstellen und im nächsten Patch-Zyklus behoben werden sollten.

**Hohes Risiko (<=40):** Kritische Schwachstellen, die unmittelbare Aufmerksamkeit erfordern, um potenzielle Angriffe zu verhindern.

Bewertungskriterien

**Wahrscheinlichkeit:** Diese Kategorie bewertet, wie wahrscheinlich es ist, dass eine Schwachstelle ausgenutzt wird. Zu den Faktoren gehören:

* **Entdeckbarkeit:** Wie einfach ist es für einen Angreifer, die Schwachstelle zu erkennen?
* **Exploitierbarkeit:** Wie leicht kann ein Angreifer die Schwachstelle ausnutzen?

**Auswirkung:** Diese Kategorie bewertet die Schwere der Folgen, falls eine Schwachstelle ausgenutzt wird. Hierzu gehören:

* **Vertraulichkeit:** Zugriff auf vertrauliche Daten.
* **Integrität:** Manipulation von Daten oder Systemen.
* **Verfügbarkeit:** Beeinträchtigung der Serviceverfügbarkeit.

Beispielhafte Risikobewertung

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risiko ID** | **Beschreibung** | **Wahrscheinlickeit** | **Auswirkung** | **Gesamt-Risiko** | **Risikolevel** |
| 1 | SQL-Injection | 8 | 6 | 48 | Hoch |
| 2 | Cross-Site Scripting (XSS) | 6 | 4 | 24 | Mittel |
| 3 | Veraltete SSL-Versionen | 4 | 6 | 24 | Mittel |
| 4 | Fehlende Sicherheitsheader | 3 | 3 | 9 | Tief |

**Risikobewertung:**

Punkte 0-9: Tief-Sehr hoch

**Riskolevel-Klassifizierung:**

Hoch: > 40

Mittel: 21-39

Tief: <=20

**Risikobewertungsdetails:** In der obigen Tabelle sehen Sie eine Bewertung basierend auf der Wahrscheinlichkeit und der Auswirkung der Schwachstelle. SQL-Injection wird als hoch bewertet, da sie sowohl leicht entdeckt als auch einfach ausnutzbar ist und schwerwiegende Auswirkungen haben kann.