Duale Hochschule Baden-Württemberg
Mannheim

Pentest Report

Pentesting Project X

Studiengang Cyber Security

Verfasser:	Luka Tsipitsoudis
Matrikelnummer:	4110112
Kurs:	TINF20CS1
Abgabedatum:	18.04.2023
Betreuer:	Pr. Dr. Johannes Bauer

Unterschrift: _____

Abstract

Deutsche Version

Englische Version

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

1 Introduction

1.1 Scope

Who gave the assignment? What is the Device under Test (DUT)? What have you received for the test (hardware, information, etc.)? Add email with hash sum of the mail to the report.

1.2 Severities

For each vulnerability you uncover in your testing, you typically provide: The likelihood of exploitation, taking into account how easy it is to discover and exploit The impact on the control you get once exploited Suggested remediation Suggested validation of remediation effectiveness

Low Moderate High Severe Critical

1.3 Classification

1.4 Effort to Fix

Low Moderate High

2 Management Summary

Short Summary for non technical people. what are key takeeaways and recommendations? how urgent is acting neccessary?

3 Technical Summary

summery for technical people

3.1 Findings Overview

table that contains the findings you'll describe later, sorted by severity Helps quickly triage results

3.2 Used Tools

4 Findings

4.1 Finding 1 - Name

Information Disclosure RCE (Remote Code Execution) DoS (Denial of Service) Key reuse/sharing Weak cryptography

Classification: **CVE:** **Severity:**

4.1.1 Finding Description

4.1.2 Finding Impact

4.1.3 Finding Cause

4.1.4 Finding Details

4.1.5 Evaluation of Results

Effort to Fix:

How do you judge the individual technical findings (severity, likelihood)? What is your suggested remediation, if there is one? How can the customer validate their remediation is effective once implemented?

5 Results