
Uni App Security Themes

Themes for the Anwendungssicherheit (app security)
course at HdM Stuttgart

Felicitas Pojtinger

2022-02-01

Contents

| | | |
|----------|------------------------|----------|
| 1 | Introduction | 3 |
| 1.1 | Contributing | 3 |
| 1.2 | License | 3 |
| 1.3 | Themes | 4 |

1 Introduction

1.1 Contributing

These study materials are heavily based on [professor Heuzeroth's "Anwendungssicherheit" lecture at HdM Stuttgart](#).

Found an error or have a suggestion? Please open an issue on GitHub (github.com/pojntfx/uni-appsecurity-notes):



Figure 1: QR code to source repository

If you like the study materials, a GitHub star is always appreciated :)

1.2 License



Figure 2: AGPL-3.0 license badge

Uni App Security Themes (c) 2022 Felicitas Pojtinger and contributors

SPDX-License-Identifier: AGPL-3.0

1.3 Themes

Please check out [Jakob's notes](#) for more detailed study materials!

- Basics and Security Objectives (8 points)
 - CIA triad
 - Definition of security & safety
 - Definition of software security & safety
 - How do software security issues occur, and what are their causes?
 - What are risks, threats and vulnerabilities? (from the basics slides)
 - Ranking risks
 - Contradictions in software security (security vs vulnerability)
- Secure Development Process (4 points): Data flow diagram (see STRIDE) and modelled system are given, analyze the secure development principles
- Buffer Overflow (10 points):
 - Screenshots from SL-Mail exploit are given, explain step by step (with parameters and tool names)
 - Include buffer overflow cheat sheet
 - Unique string search vs binary search
- Security of Web Applications (13 points):
 - OWASP Top 10 (names, explanation and example)
 - 2x: Bad example code is given, find, describe and execute possible attacks, show counter-measures
 - Attack vector is given, execute attack
 - Explain countermeasure to one of the OWASP 2021 attacks
- Secure Coding (10 points):
 - Explanation of program is given, find and fix the vulnerability
- Authentication and Authorization (5 points):
 - Authentication vs Authorization
 - Methods of authentication (knowledge, ownership or attributes)
 - What are OAuth2 refresh & access tokens?