Uni App Security Notes

Felix Pojtinger

October 5, 2021

Contents

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

2 Organization

- 60 Minutes of test at the end
- Will have practical examples
- Threat detection plays a fundamental role in tests

3 Overview

3.1 Elements of a Secure Development Process

Primary purpose: Analysis of the data flow; data is both protected by the GDPR and represents value of the coporation

- **Requirements**
  - Security-Requirements
  - Anti-Requirements
  - Abuse cases
  - Protection poker
  - → **Security analysis/architecture analysis**
- **Draft**
  - AuthN/AuthZ
  - Drafting concepts
  - **Risk modelling**
- **Implementation**
  - Secure implementation guidelines
  - **Code review, dynamic analysis**
- **Tests**
  - Security testing plans
  - Security testing cases
  - **Ethical hacking, pentesting, dynamic analysis**
- **Operations/Maintenance**
  - Secure initial settings
  - Assumptions of runtimes
  - Observation of logs
  - **Processes for management and reaction to breaches**
- **Documentation**
  - Installation
  - Configuration
  - Customization
  - Operations
  - → **Impact area of security incidents must be visible***

3.2 Support Hierarchy

- **Level 1**: Direct support with customers; call center, non-technical
- **Level 2**: People who know about typical problems with the software

- **Level 3**: Developers of the software