Welcome to

2. Initial Overview of Software Security

KEA Kompetence OB2 Software Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github

2-initial-overview-sw-security.tex in the repo security-courses

Plan for today

Subjects

- Introduction to Methods
- Strategies for Security Testing
- Design vs Implementation
- Common Secure Design Issues
- Poor Use of Cryptography
- Input Validation
- Basic Cryptography introduction
- Symmetric Cryptosystems
- Data Encryption Standard (DES) / Advanced Encryption Standard (AES)
- Public Key Cryptography
- Stream and Block Ciphers

Exercises

- sslscan scan various sites for TLS settings, Qualys SSLLabs

Reading Summary

AoST chapter 1: Case Your Own Join: A Paradigm Shift from Traditional Software Testing

AoST chapter 2: How Vulnerabilities Get into All Software

Goals:

Introduction to Methods

Strategies for Security Testing

Design vs Implementation

Common Secure Design Issues

Poor Use of Cryptography

Input Validation

Basic Cryptography introduction

Symmetric Cryptosystems

Data Encryption Standard (DES) / Advanced Encryption Standard (AES)

Public Key Cryptography

Stream and Block Ciphers

Exercise

Now lets do the exercise

SSL/TLS scanners 15 min

which is number **9** in the exercise PDF.

For Next Time

Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books
Most days have less than 100 pages, but some days may have more!

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools

Buy the books!