Welcome to

11. Software Assessment

KEA Kompetence OB2 Software Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github

11-software-assessment.tex in the repo security-courses

Plan for today

Subjects

- Review using the red book, similarities to green book
- Repetition, common problems, how to improve software security
- How to do Review and audit of software
- Attack and Response
- Attack graphs
- Attack surfaces, and reducing them
- Common Vulnerabilities and Exposure CVE
- Common Weakness Enumeration CWE
- MITRE ATT&CK framework

Exercises

- Layout a plan for securing the Juice Shop

Reading Summary

AoSSA chapters 1: Software Vulnerability Fundamentals

AoSSA chapters 2: Design Review

AoSSA chapters 3: Operational Review

AoSSA chapters 4: Application Review Process

Was many pages, skim if you need to.

Goals:

Review using the red book, similarities to green book

Repetition, common problems, how to improve software security

How to do Review and audit of software

Attack and Response

Attack graphs

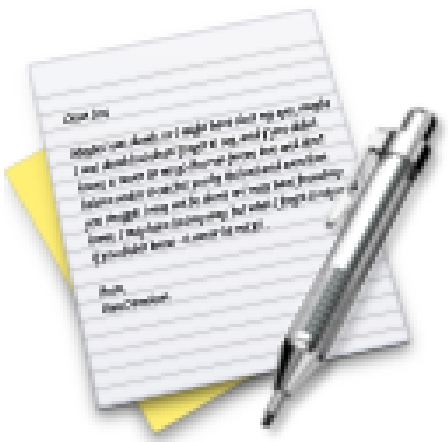
Attack surfaces, and reducing them

Common Vulnerabilities and Exposure CVE

Common Weakness Enumeration CWE

MITRE ATT&CK framework

Exercise

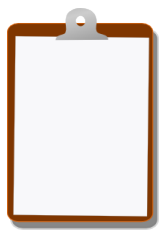


Now lets do the exercise

Securing the JuiceShop

which is number **18** 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!