Welcome to

5. Fuzzing Intro

KEA Kompetence OB2 Software Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github
5-fuzzing-intro.tex in the repo security-courses

Plan for today

Subjects

- What is Fuzzing
- Example fuzzers
- Web fuzzing
- Exploitability

Exercises

- Try running brute force and fuzzing
- Try American fuzzy lop http://lcamtuf.coredump.cx/afl/

Reading Summary

AoST chapters 10: Implementing a Custome Fuzz Utility

AoST chapters 11: Local Fault Injection

AoST chapters 12: Determining Exploitability

Goals:

What is Fuzzing

Example fuzzers

Web fuzzing

Exploitability

Exercise

Now lets do the exercise

Try running brute force and fuzzing

which is number **12** in the exercise PDF.

Exercise

Now lets do the exercise

Try American fuzzy lop

which is number **13** 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!