Secure Software Engineering

Exercise Sheet 8, Winterterm 25/26

Discussion Week: 12.01.26 to 16.01.26

> We highly encourage you to do the assignments yourselves, as all the exercises are relevant for the exam. It is also recommended to visit the tutorial, as there will be a discussion about the exercises, not just the solutions. For the *Vulnerability of the Day* exercises, we recommend examining the code snippets, if any, while conducting your research. Keep in mind that the entirety of the lecture is relevant to the exam. If a topic or some details are not specifically talked about or mentioned in the exercises, that does **not** mean that it will not be part of the exam!

If you have any questions, please do not hesitate to ask your tutor Aura, Kati or Lukas. (Hint: the mails are embedded in the names.)

Good luck and have fun! :)

Ex. 1 - DOs and DON'Ts of Code and Connections

Answer the following sub-tasks:

a) Secure connections should be encrypted, authenticated and tamper-proof. Explain why and how this is achieved.
b) Name some problems that can occur when sanitizing data.
c) Why is sanitization of debug / logging output important as well?

Ex. 2 - Cryptography

Answer the following sub-tasks:

a) Explain how a *symmetric encryption* works.
b) Explain how an *asymmetric encryption* works.
c) Compare *stream cipher* with *block ciphers*.

Ex. 3 - Message Authentication Codes (MAC) and Signatures

Answer the following sub-tasks:

a) How do MACs work and what are they used for?
b) How do signatures work and what are they used for?

Ex. 4 - RTFM

In the lecture, two papers were cited on why no one reads the manual. Answer the following sub-tasks:

a) What are common alternatives to reading the manual that users used?
b) Why were manuals not used?
c) What makes a good manual?

Ex. 5 - Vulnerability of the Day

In the lecture you have talked about *hard-coded credentials* and *unsalted hashes*. Research an example of this which was not discussed and explain what happened, how it happened and how it was dealt with. In addition to that, explain which of the CIA properties were affected. (You can look up a CVE, in case you cannot find an attack on a company or something similar.)