# Secure Software Engineering

**Exercise Sheet 1, Winterterm 25/26**

**Discussion Week:** Wed 22.10.25 to Wed 29.10.25

> 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 looking into the code snippets, if you find any, while doing research. Keep in mind, the entirety of the lecture is relevant for 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 - Terms & Relations

Answer the following sub-tasks:

a) Explain the relationship between a *threat* and an *adversary*.
b) How do we differentiate between *safety* and *security*?
c) What is the problem with absolute statements such as "[software] is secure"?
d) What is the difference between an *attack vector* and a *vulnerability*?
e) What does *CIA* stand for? Give examples of how to achieve each security property.
f) Explain the *AAA principle*.

## Ex. 2 - Software Security

Answer the following sub-tasks:

a) Name and explain 3 things that make up software security?
b) Why is security not just about the technology?
c) What are *Security Maturity Models* for? What are the different levels of the model?

## Ex. 3 - Vulnerability of the Day

In the lecture, we talked about *Cross-Site Request Forgery*. Research an example of this that 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.