Secure Software Engineering

Exercise Sheet 4, Winterterm 25/26

Discussion Week: Tue 18.11.25 to Fri 21.11.25

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 - Risk Assessment

Answer the following sub-tasks:

a) How is risk calculated? What is important to be kept in mind?

b) Think of an account that is important to you and one that is less important. Discuss the risk assessment for both and explain it.

c) Explain the differences between abuse cases and risk assessment.

Ex. 2 - Protection Poker

In this exercise you will be conducting a risk assessment using protection poker. The given tables are given to you and should fill in the blanks **as needed**.

As a reminder, these are the Fibonacci Numbers up to 100: 1, 2, 3, 5, 8, 13, 21, 34, 55, and 89.

Asset Value	Data	Used in Feature
	Name of employee	
	Address of employee	
	Employee ID	
	Banking info of employee	
	Personal email of employee	
	Work email of employee	
	Social security number of employee	
	Insurance info of employee	
	User access of employee	
	Accommodations of Employee	

Feature #	Feature	Total Value Points	Ease Points	Security Risk
1	Work group			
2	Change of employee personal information			
3				

Based on your assessment: Which feature seems to have the highest risk?

Ex. 3 - Risk-Driven Test Planning (RDTP)

Answer the following sub-tasks:

a) What are the goals of RDTP?
b) Explain how *Top-Down Test Planning* works.
c) Explain how *Buttom-Up Security Test Planning* works.

Ex. 4 - Vulnerability of the Day

In the lecture you have talked about *log overflow* and *path traversal*. Research an example of these which were 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.)