**Assignment 2 – IDATT2503**

**Task 1: PyCalc**

**1.1**

This text is about a found exploit in the PyCalc calculator-script. The exploit makes it possible to reveal the directory in which the script is stored, as well as other directories. With the right knowledge, exploiters could get access to other storage.

**1.2 & 1.3**

Firstly, launch the script of course.

Afterwards, the exploit can be reproduced as a Python injection concealed as an expression.

If the user writes “op \_\_import\_\_(“subprocess”).getoutput(“ls”)”, the entire directory is listed out in order. This would again give the possibility to read all files, change directories without protection, and so on.

**1.4**

I found the right injection after around 2 hours, and I am not an experienced exploiter. If the exploiter had more knowledge, this could probably have been cracked in a very small amount of time. So the exploit is pretty severe in that sense.