Fall 2019
Sébastien Combéfis

I5020 Computer Security

Coding 3: Input validation

This assessment evaluates the following competencies:

- *CS003 – Identify weaknesses in a computer system or infrastructure and propose solutions*
- *CS204 – Discuss about general design principles for protection mechanisms*
- *CS201 – Understand software protections that can be installed on a computer system*
- *CS301 – Write robust code that checks precisely all the external data (environment, file, form...)*
- *CS303 – Apply code design principles in developed software*
- *GP301 – Write robust code with good error management*

For this assessment, you have to write a small command line application that asks the user for some (structured) inputs (2–3) and check them thoroughly with several check levels (syntax with regular expression, correct type, domain for accepted values, presence in a database of valid values, etc.)

Pay attention to the following elements:

- The design and content of the application is not important.
- Send good and relevant messages to the user to help him/her understand what was wrong with his/her inputs.

Prepare yourself for the following manipulations/questions:

- Show several usage scenarios (correct and wrong) of your application
- How can you be sure that you covered all the cases?
- What should be checked when dealing with user inputs?
- What is the drawback of writing more robust code regarding input validation?