Fall 2019
Sébastien Combéfis

I5020 Computer Security

Coding 4: SQL injection

This assessment evaluates the following competencies:

- *CS003 – Identify weaknesses in a computer system or infrastructure and propose solutions*
- *CS201 – Discuss about general design principles for protection mechanisms*
- *CS202 – Understand software protections that can be installed on a computer system*
- *CS302 – Write robust code that resists to SQL, PHP injections and XSS attack*
- *CS303 – Apply code design principles in developed software*
- *CS401 – Identify vulnerabilities in a system and propose countermeasures for them*

For this assessment, you have to write a small command line application that allows the user to query the content of a database. The input of the user should be inserted inside an SQL request and it should be able to attack the database through an SQL injection. Also show how to protect your application against SQL injection attacks.

Pay attention to the following elements:

- The design and content of the application is not important.
- An example of SQL injection could be that the user is able to filter returned data or is able to remove data in a table.

Prepare yourself for the following manipulations/questions:

- Show the malicious input that the user has to use and print the resulting SQL query that will be executed.
- How can your protect against SQL injection and why it works?
- What are the specific functions from the programming language/library you choose that are used to prevent SQL injection?
- What is the drawback of writing more robust code regarding SQL injection?