Fall 2019
Sébastien Combéfis

I5020 Computer Security

Coding 5: XSS attack

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 website that allows the user to inject scripts written in JavaScript and that can be executed by users that come to visit the webpage. Also show how to protect your application against XSS attacks.

Pay attention to the following elements:

- The design and content of the application is not important.
- An example of XSS attack could be that the user is able to insert a code that redirect the visitor to a malicious website.

Prepare yourself for the following manipulations/questions:

- Show the malicious input that is executed.
- How can you protect against XSS attacks and why it works?
- What are the specific functions from the programming language/library you choose that are used to prevent XSS attacks?
- What is the drawback of writing more robust code regarding XSS attacks?