DAR Project 2

Tamara Rezk and Nataliia Bielova

This document defines the project and the evaluation rules for the TPs that you have to implement within the second part of the course "Développement d'applications web (Architecture des Applications Réticulaires - AAR)". In case of doubts, please contact the teachers (by email) as soon as possible for clarifications.

1 Organisation

1.1 Groups

Each TP is done by the group of 1 or 2 students, while the project is to be done by the group of maximum 3 students. The groups are defined in `https://goo.gl/erceQg` and have been fixed since 14/12/2015 (the day of the last TP).

1.2 Originality

All the code in the project has to be written by the students of the groups. The usage of public libraries is authorised, though in this case a detailed explanation of the functionality of the library has to be provided.

1.3 Report

The report of the project has to be submitted in the same time as the code of the project. It should contain:

- Precise description of use cases and the necessary code to replay the XSS and CSRF attacks if found.
- Explanation of the implementation of the assigned web tracking technique and cookie stealing attempt.
- Detailed explanation of a protection mechanism implemented in the project against XSS and CSRF.
- Proposed solution against a web tracking technique that a group-counterpart has implemented, and was added in a shape of advertisement on the main page of your project ("main page" is the first that the user sees after he logged in).
- Proposed solution against cookie stealing.

The clarity and clearness of the report will be taken into account during evaluation. There will be no exam or presentation in person for this project.

1.4 Submission

The TPs have to be submitted the latest on the day indicated below, the latest at 23h59 (Paris time):

- TP1: 1 December 2015
- TP2: 8 December 2015
- TP3: 15 December 2015
- TP4: 20 December 2015

The Part 1 of the project must be submitted by 12/01/2016, and the Part 2 must be submitted by 19/01/2016. Both deadlines are at 23h59 (Paris time). The submission must contain:

- link for the old code, and to the new code (zip, github, ...)
- link for the old application and the new application (url)
- link to the report (pdf)

- names of the participants, group number and a counter-group number.

In case you delay the submission of the TP or of the project, the following rule will apply with respect to the amount of delay:

- 0-24 hours of delay: 2 points less (out of 20),
- 1-7 days of delay: 5 points less (out of 20),
- +7 days of delay: mark is set to 0.

1.5 Evaluation rules

Every TP and the project will be evaluated by maximum 20 points (a mark is denoted by TP_i) with some extra bonus points, and each project is evaluated by maximum 20 points as well (a mark denoted by *Project*). The final grade will be calculated using the following formula:

$$Final = \frac{2}{5} \cdot \big(\sum_{i=1..4} \frac{1}{4} \cdot TP_i \big) + \frac{3}{5} \cdot Project$$

For example, if a student gets the following marks for 4 TPs: 19, 17, 18, 14 and the mark 20 for the Project, then the final mark is

$$Final = \frac{2}{5} \cdot \big(\frac{1}{4} \cdot (19 + 17 + 18 + 14)\big) + \frac{3}{5} \cdot 20 = \frac{2}{5} \cdot 17 + 12 = 18.8$$

This final mark will count as 40% of the final mark of the whole DAR course.

2 Project description

2.1 Part 1

- Security:
  - Describe the procedure (a use case) to find an XSS vulnerability in your existing application. Explain the result of this analysis and why XSS attack is possible (or is impossible).
  - Describe the procedure (a use case) to find an CSRF vulnerability, in your existing application. Explain the result of this analysis and why CSRF attack is possible (or is impossible)
  - For each possible attack, provide a code that can be used to replay the attack.
- Privacy:
  - Implement a web tracking technique associated to your group (see `https://goo.gl/erceQg`).
  - Implement a solution to steal the session cookies.
  - Include both implementations in an advertisement and place it on your project's server.
  - Send a URL of an advertisement to your counter-group.

The deadline for sending the URL to your counter-group is 12/01/2016, at 23h59 (Paris time). In the subject of the email put "[DAR2015] Part1 name1, name2" and add in the CC two addresses: `nataliia.bielova@inria.fr` and `tamara.rezk@inria.fr`.

If the counter-group delays by n days the delivery of the URL, the receiving group will have extra n days to submit Part 2 of the project without penalty. In this case, the counter-group will receive a penalty for the Part 1 of the project (even in case if Part 2 of the project is submitted on time).

2.2 Part 2

- Security:
  - Implement protection from XSS and CSRF vulnerabilities found in your project. If a vulnerability is not found, describe the general procedure to ensure that XSS and CSRF are indeed impossible.

  If at least one vulnerability is found, update the web application and the code accordingly.
- Privacy:

- Include the advertisement code you received from your counter-group in the page of your project after the user logged in.
- Implement a solution to protect the client from being tracked. Explain why the tracking is not possible anymore.
- Propose an existing solution to the client (such as changing his browser preferences, installing browser extension) and explain how it protects the client from being tracked.
- Implement a protection from cookie stealing in your project. Check whether the advertisement code can steal the cookies and explain how the protection makes the cookie stealing impossible.

Update your web application and the code with all the demanded implementations.

The deadline for the project is 19/01/2016, at 23h59 (Paris time). In the subject of the email put "[DAR2015] Project name1, name2".