Final Project for the Course on Security of Web Applications

Tamara Rezk

September 30, 2016

This document defines the project and the evaluation rules for the project that you have to implement as part of the course "Security of Web Applications". In case of doubts, please contact me as soon as possible for clarifications.

1 Project Description

You should implement a web application with any desired functionality. The restrictions are:

- A user should be able to create an account and login in the application. A session cookie should be established in the last case.
- There should be more coookies than the session cookie.
- There should be a predefined user (called secretholder) who can see, after logging in, a div with id "secret" with some secret text visible using innerHTML.
- There should be a place where an external URL (code of other server) can be included (before and after login also). You will not have this code while developing your application and you will not know if the URL will point to code providing a file.js or a file.html.

1.1 Part 1: Break it

You should on purpose break your application by introducing:

- 10 vulnerabilities, each of them corresponding to one of the last OWASP top-10 vulnerabilities list
- a path to leak the secret. You can use a combination of OWASP top-10 and/or other vulnerabilities *described during the course or present in the TP.*

You should write a report of max 30 pages, Report 1, describing:

- The functionality of your application (max 2 pages).
- For each OWASP vulnerability: a brief description of the vulnerability, where the vulnerability is in your application, code to replay the attack regarding the vulnerability, possible defenses that could be used to prevent this vulnerability.
- A clear description of the path to leak the secret.

The clarity and clearness of the report will be taken into account during evaluation.

1.2 Part 2: Presentation

The group will be granted 40 minutes (strict) to present all the vulnerabilities and the path to leak the secret. It is desirable that each vulnerability is presented by different members of the group. After this presentation, all the members should answer questions during 40 minutes about any vulnerability exposed for the application.

1.3 Part 3: Fix it

You will be given a URL of the web application of a counter-group. You have two goals:

- Find the OWASP top 10 vulnerabilities
- Find the secret

You should write a report of max 12 pages, Report 2, describing how to find the vulnerabilities and the secret. During this process you will have the opportunity to provide 2 URLs with your code to be included in the application of your counter-group.

1.4 Style

No extra points are given for style and simplicity of the code will be highly appreciated (this does not mean that you should not use CSS, if you want, specially to introduced new XSS attacks).

2 Organization

2.1 Groups

The project is done by a group of 11 students. The groups have to be fixed since 13/10 by sending me an email with complete names of the members of the group.

2.2 Originality

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

2.3 Communication with counter-group

Vulnerabilies and the secret should be found by the students of the group only. Any communication with the counter-group or external help regarding this project, besides the one formally stated in this document, should be avoided.

3 Timeline

- 13/10: Send an email to teacher fixing the group. Each group will have 2 deputies that should communicate with the counter group when needed in the future.
- 14/11: Send an email to teacher with Report 1
- 17/11: Presentation and questions. Provide code to teacher
- 18/11: Send URL of your application to counter-group deputies with teacher in CC
- anytime between 18/11 and 28/11: send (and receive) URLs to counter group deputies in order to include the URLs as external code in the counter group application. A delay of 24 hours should be given to the counter-group to include the URL.
- 01/12 (deadline is extended accordingly to the delays of counter-group):Send to teacher Report 2 and the value of the secret, if found.

4 Evaluation

The project represents one half of the final note for the course. It is possible to obtain a total number of 42 points per member of the group with the project (that will count as a max of 21 points in the final note). Some of the points are granted to the group and some of them only to specific members (in particular, the questions are evaluated individually). The distribution of the points is as follows:

4.1 Positive Points

You can obtain positive points at different stages:

- Part 2 Break it (group) : 3 points max
- Part 2 Bonus (group): 2 points max (one half point for extra vulnerability introduced outside the OWASP list)
- Presentation (group): 5 points max
- Questions (individual): 10 points max
- Part 3 Fix it Finding the OWASP top 10 (group): 5 points max
- Part 3 Fix it Finding the secret of counter-group (group): 4 points max (only if the other team does not find your own secret)
- Part 3 Bonus: 6 points max (individual): one point for each vulnerability found outside the OWASP top 10 and NOT reported by the counter-group

5 Negative points

It is also possible to obtain negative points (only answered questions negative points are individual).

- Unanswered questions during presentation (individual): -5 points max
- Part 3 Fix it Finding the secret of counter-group (group): -2 points max (-1 if no group finds the secret of the counter-group, -2 if the counter-group finds your secret but you don't theirs)
- Part 3 Bonus: -6 points max (one point for each vulnerability found outside the OWASP top 10 and NOT reported by the counter-group)
- Delays: -42 points max, see detail below.

6 Delays

In case you delay your submissions, at any stage, the following rules apply depending on the amount of the delay:

- 0-24 hours: 2 points less
- 1-3 days: 5 points less
- 3-7 days: 10 points less
- +7 days: mark is 0.

In case of absence (and absence of a formal justification), the day of the presentation, -5 points are individually withdrawn to the absent member.