Homework 5: Security assessment

This assignment is independent of others, but the solution would definitely benefit from the knowledge and experience you gained from the earlier assignments.

In this homework, you will do a security assessment of a online voting system written in PHP. The application can be obtained at `https://bitbucket.org/coltekin/dbweb-assignment5`. The application has at least 10 security holes built in (some of them repeat in multiple times). Note that some of the security problems may not be possible to exploit in some PHP/web server environments (but they still are examples of insecure programming practices).

Ideally, you should install the program somewhere, and try, for example, the following:

- Can unauthorized users change votes cast by others?
- Can a user damage the database? (remember little Bobby Tables)
- Does the application allow unauthorized access to any files?
- Can you bypass authentication somehow?
- Can you impersonate others without knowing their password?
- Can you steal and use the passwords stored in the system?
- . . . more: think like someone who wants to tamper with the elections.

For most of the questions, you should see that answer is ‘yes’.

The security problems should be (or intended to be) local, that is, accessing or harming other applications or data on the web server should not be possible through this application. Nevertheless, if you try it out, **DO NOT leave it installed on a publicly accessible web server**.

You can complete this assignment one of two ways:

- Modify the source code, fix the problems, and send me your changes via email in `git diff` format. For each change, include a brief comment indicating why you made the change.
- Write a report on your assessment, indicating where the security problems are, and what should be done to fix them.

If you send in your homework before January 15th 2014, you will receive feedback about your security assessment or fixes. The absolute deadline for this homework, like anything else in the course, is January 31, 2014.