Assignment 1

In this assignment, you will demonstrate your ability to use SQL injection.

You have to:

1. Download and install VirtualBox on your computer
2. Download and run the virtual machine (VM) that was created for this homework. The link is published on BBLearn
3. Open a web browser on your computer (the "host machine")
4. Navigate to http://192.168.3.77
5. A web server that is installed on the VM will return the "main page" of a small information system. The page allows you to search for classroom assignments of a few courses. You can enter a course number in the textbox, click the button, and the web page will show the classroom assignment for that course
6. Click on the "login" link that you find on the classroom assignment page. You will be presented with a login form
7. You must find a way to go past the login form. The username is "me" (without quotes). More on going past the login form is below. When you succeed, you will be presented with another page (the "oracle" page) that contains a textbox and a button
8. Enter in the textbox the "challenge string" provided by BBlearn on your Assignment 1 page and click the button. A new page will be loaded, which shows a "response string"
9. Take a screenshot of this page and save it for later
10. Copy the response string in BBlearn's "response string" box
11. Attach a screenshot of the "response string" page
12. Include a description of the steps you took to go past the login form. We will use this description to (1) evaluate your work and (2) ensure that no cheating occurred, so be diligent in providing suitable information

Going past the login form

This is the real challenge of this assignment. By "going past the login form" we mean successfully authenticating in order to reach the "oracle page".

Unfortunately, you do not know the password for user "me". The passwords are stored in table "Users" of database "Application", which is installed on the VM. The same database is used by the "main page" to retrieve the classroom assignments. The room assignments are stored in table "RoomAssignments".

Most likely, to succeed in the assignment, you will need to use another VM, the "sandbox VM", which is also provided to you. You are given the login information, so that you can log into the VM (e.g., via console or ssh) and explore the VM. The login information is:

Root password: <root password here>

Password for VM's user "me": <me's password here>

Note: these credentials are different from those for the VM used in the assignment, so cannot use them to explore the assignment VM.

The web pages that are served to your browser by the web server are located at /path/to/files. It is recommended that you study the files that you find there in order to understand how the database is accessed and what the names of the fields are. You are expected to be able to use the name of a field to make hypotheses on how its content is encoded and used.