## Introduction

A customer wants a security test of the web application "Poetry". "Poetry" is a paid web service that allows registered users to publish poems to an open audience. The application is based on a MySQL database. Among many other tests, the behavior of the web service in case of SQL injections attacks has to be tested.

The resources section contains a test environment of the application including test data. Under the URL "/_task" the test environment provides a possibility to reset the database. Do not test this part of the application since this functionality is only for your convenience. If needed, call the page "/_task" and follow the instructions to reset the database to its initial state.

## Goals and Tasks

Perform the following tasks and record all your results including the attack vector and the applied SQL injection strings in a written report.

- Retrieve the names of all database tables.
- Retrieve the credit card details (type, number, name, validity) of the user with the username hostettler.therese.
- Retrieve the social security number (AHV), address and the date of birth of the user with username wyss.sara.
- Replace the password of all users with the valid hash $2y$10$92IXUNpkjO0rOQ5byMi.Ye4oKoEa3Ro9llC/.
  which corresponds to the string password in plain text.
- Login as user wittwer.michael@example.net with the changed password password and get the emergency code of the user's profile.

## Submission

Submit a written report as PDF document, containing your answers and all details on how you retrieved the information. Make sure that you also list the way of injection as well as the injected SQL queries.