

## System and Web Security – Homework 10

### Problem 1: SQL Injections, CSRF

#### a) Adding new users

A form to add new users was added to the provided web application. The form is very basic and consists of fields to enter the new user's name and password, as well as a drop-down menu to select the new user's privilege level. The new GUI can be seen on the following screenshot:

**SEC Intranet - Admin Area**

[Return to home](#)

id	username	password	signed_up	privileges
1	administrator	nobody_knows	1970-01-01	all
23	bob	bob\$passwd0rd	2011-05-02	user
42	alice	verysecret	2012-06-04	user
66	testuser	utestusr	2018-06-28	all
77	erguj	joiwefjowiefj	2018-07-01	user
80	heinz	n1xd0rf	2013-02-03	user
85	newuser	foobar	2019-07-01	all
86	newuser2	12345892	2019-07-01	user

Never store passwords in plain text as we do in this example!

[RESET DATABASE](#)

**Create new user:**

Username:

Password:

Privileges:  
All

Please refer to the source file `sec-intranet-upgraded.py` for implementation details.

Please also note that the database's structure has been changed slightly: instead of writing logic for creating the user ids manually, the database was altered to make the id column the user table's primary key, and the column set to auto-increment, which is a common pattern.

This has the distinct advantage of ids being unique in that table, as well as the database automatically providing new ids once a new user is created.

Please refer to the file `users-upgraded.sql` for the updated user table's structure.

#### b) Protecting the SQL queries

The SQL queries were changed to parameterized queries, please refer to `sec-intranet-upgraded.py` for the implementation.

#### c) CSRF attack

The file `csrf-exploit.html` contains an attack that logs visitors to that page into the SEC intranet application as the user "heinz". This is done via a manipulated hidden form that is triggered by JavaScript, which causes a forged log in request from the user's browser.

#### d) CSRF defense

A session-dependent nonce approach was implemented, which rejects requests with an invalid nonce in the form with the following error message:

← → ↻ ⓘ localhost:8081

**SEC Intranet**

Invalid nonce! Go away hackers!

Please again refer to the source file `sec-intranet-upgraded.py` for implementation details.