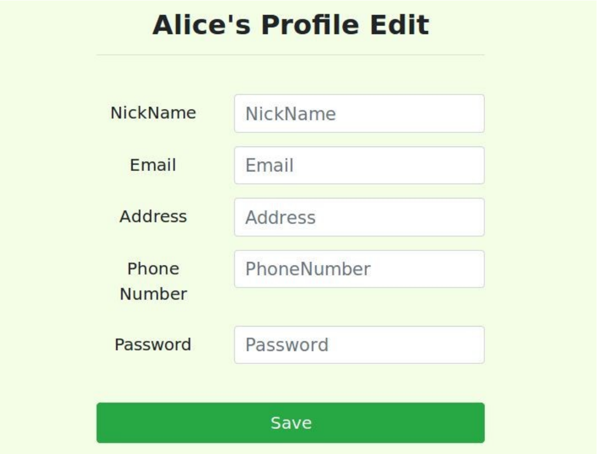
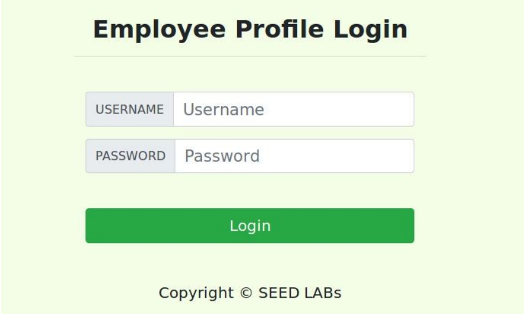
Reverse Identity Theft

Alice is an employee with a lot of debt due to some shady activities that she did. Also, Alice really hates Boby. In this task, Alice wants to transfer all her debt and issues to the company to Boby. To do so, she wants to perform several SQL injections in order to modify the profile of Boby and make it show all Alice information. She hopes that in this way, when the IRS comes for taxes recollection, they will frame Boby instead of her.

The following images describe the 2 forms which can be used to inject malicious inputs:



Form 1



Form 2

Thus, each field of Boby information should reflect the Alice's ones (i.e., only Employee ID, Salary, Birth and SSN. What would happen if we changed also ID and Name?). You can check the state of the database to retrieve Alice information (see below for instructions).

For each of the fields, indicate:
- which of the two is the form to be used;
- the malicious input for the exploit;
- in which field to inject it.

Basic instructions for containers

1) Build and turn on containers (`dcbuild`, `dcup`);

2) If for any reason it does not work, shut down all containers and remove them with the following commands

```
docker stop $(docker ps -a -q)
docker rm $(docker ps -a -q)
```

3) Clean up the `mysql-data` folder to get a fresh new db

```
rm -rf mysql-data/*
```

4) Get back to step 1;

If the system is correctly working, you should reach login page at: http://www.seed-server.com/

and you should be able to login with user `Alice` and pwd `seedalice`.

For networking reasons, **USE CHROMIUM** browser **INSTEAD OF FIREFOX**! Otherwise, you won't be able to reach the website.

Basic instructions for mysql usage

If you want to check the state of the database to assess the attacks you perform were successful, here you have how to do so:

1) Use `dockps` to know the identifier of the mysql container;
2) Use `docksh` to open a shell within the mysql container (first two chars of the container id should be enough as argument);
3) `$ mysql –u root –pdees`
4) Select the right db: `mysql> use sqllab_users;`
5) Check for tables: `mysql> show tables;`
6) Perform the query.

Keep in mind that the password per each user is seed<Name> (i.e. Name=”alice”, password=”seedalice”).