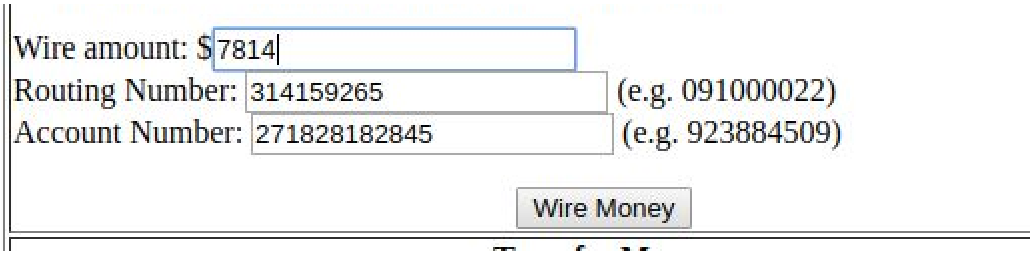
SQL Injection Instructions

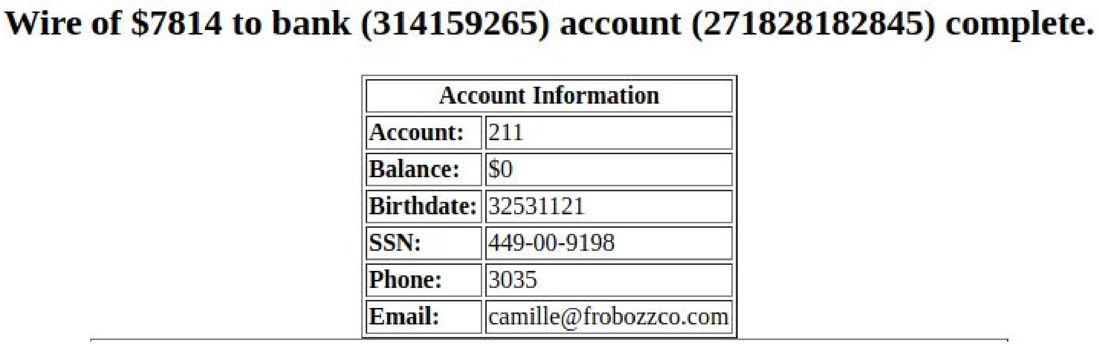
1. To login into an account without previous knowledge of an id: `1 OR 1=1 --` and password: j
2.
3. In order to wire money, enter the routing number, account number and amount left in the account to be sent.



Wire amount: $7814

Routing Number: 314159265 (e.g. 091000022)

Account Number: 271828182845 (e.g. 923884509)



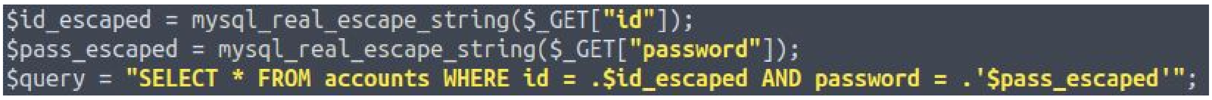
Wire of $7814 to bank (314159265) account (271828182845) complete.

Account Information	
Account:	211
Balance:	$0
Birthdate:	32531121
SSN:	449-00-9198
Phone:	3035
Email:	camille@frobozzco.com

4. We can't create a new account because the code uses the sql statements only as queries and they are passed into the query function which should not be able to update or add anything. Again, to create a new account we will need more knowledge of the database and how it is structured, that is, how the passwords are encrypted and the likes.

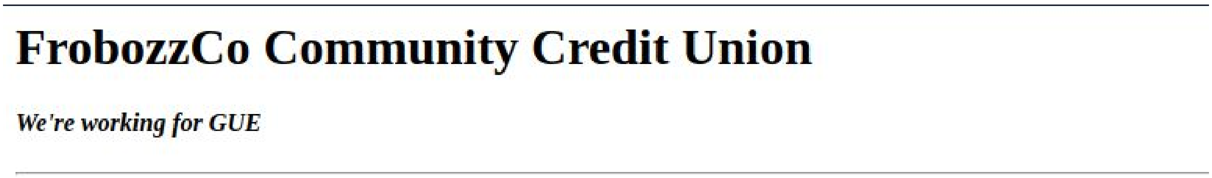
Patch

1. Using the string escape approach, I initialized both id and password. Hence, both integers and strings are escaped with 'mysql_real_escape_string' as seen in the photo below:



```
$id_escaped = mysql_real_escape_string($_GET["id"]);
$pass_escaped = mysql_real_escape_string($_GET["password"]);
$query = "SELECT * FROM accounts WHERE id = .$id_escaped AND password = .'$pass_escaped'";
```

2. So trying the same attack on the page we are denied access.



FrobozzCo Community Credit Union

We're working for GUE