SQL Injection Activity

In [ ]:

```
%load_ext sql
%sql sqlite://
```

Table Creation

In [ ]:

```
%sql DROP TABLE IF EXISTS users
%sql CREATE TABLE IF NOT EXISTS users(name VARCHAR(255), password VARCHAR(2
55))
names = ['alice', 'bob', 'chris', 'alex', 'jessie', 'sarah', 'jason']
passwords = ['cs145', 'databases', 'stanford', 'cardinal', 'password', 'abc
123', 'sql']
for (n,p) in zip(names,passwords):
    %sql INSERT INTO users(name, password) VALUES (:n, :p)
```

Sign Up

You can also insert your own login and password! (Note: this is not secure so please don't put any real passwords)

Execute the cell below to create your own login

In [ ]:

```
print "Welcome to our sign up page! Please enter your information below."
username = raw_input("username: ")
password = raw_input("password: ")
%sql INSERT INTO users(name, password) VALUES (:username, :password)
print "Sign up successful! Please try logging in below"
```

Check to see your login info should now be in the table!

In [ ]:

```
%sql SELECT * FROM users
```

Login

Below is a *highly* simplified view of the backend of a website login service.

Run the cell below to test it out!

In [ ]:

```
username = raw_input("username: ")
password = raw_input("password: ")
result = %sql SELECT password FROM users WHERE name= :username
if (username != "" and password != "" and len(result) > 0 and result[0][0] =
= password):
    print "Login successful!"
else:
    print "Go away hacker!" #probably do something more menacing in product
ion
```

Now time for some hacking! Well, sort of. Notice that the value for "username" is directly substituted into the sql expression above for checking the user's password. So what would happen if we use the value

> `username:` ' ' OR password='password'
>
> `password:` password

Note: ipython-sqlite does not allow for substitution of whole strings into variables (which is actually a good thing from a security standpoint!), so these exercises may not work if you try to log in with them. For that reason we'll be writing the solution directly into the sql statements below.

In [ ]:

```
# Think about what this query will do before running it (no need to modify
anything, just think then run it)
username = "' ' OR password='password'"
password = "password"

query = "%sql SELECT password FROM users WHERE name=" + username
print query
```

In [ ]:

```
#Paste the code here to run and test it (and think about what the result im
plies)
```

Hack Away!

Now think about how a malicious hacker (not necessarily redundant) can use the idea of sql injection to cause harm to the underlying database. In particular, can you provide a combination of username and password that would lead to

> - `inserting a new tuple`
> - `deleting an existing tuple`
> - `deleting the entire table`

Hint: sql statements are separated by semicolons

Enter the username/password for each of the above 3 exercises below:

In [ ]:

```
#Inserting a new tuple username: 'malicious', password: 'hacker'
#(might be useful if the query is against a secret database users don't usu
ally have access to)
username = ""
password = ""

#Don't modify below this comment
query = "%sql SELECT password FROM users WHERE name=" + username;
print query
```

After running the cell above, copy the output into the cell below and run it!

In [ ]:

```
#Paste the code here to run and test it
```

In [ ]:

```
#Now run this cell to make sure it worked!
%sql SELECT * FROM users;
```

In [ ]:

```
#Deleting an existing tuple (specifically, alice)
username = ""
password = ""

#Don't modify below this comment
query = "%sql SELECT password FROM users WHERE name=" + username;
print query
```

After running the cell above, copy the output into the cell below and run it!

In [ ]:

```
#Paste the code here to run and test it
```

In [ ]:

```
#Now run this cell to make sure it worked!
%sql SELECT * FROM users;
```

In [ ]:

```
#Deleting the entire table
username = ""
password = ""

#Don't modify below this comment
query = "%sql SELECT password FROM users WHERE name=" + username;
print query
```

After running the cell above, copy the output into the cell below and run it!

In [ ]:

```
#Paste the code here to run and test it
```

In [ ]:

```
#Now run this cell to make sure it worked!
%sql SELECT * FROM users;
```

For more info on sql injection, check out https://en.wikipedia.org/wiki/SQL_injection