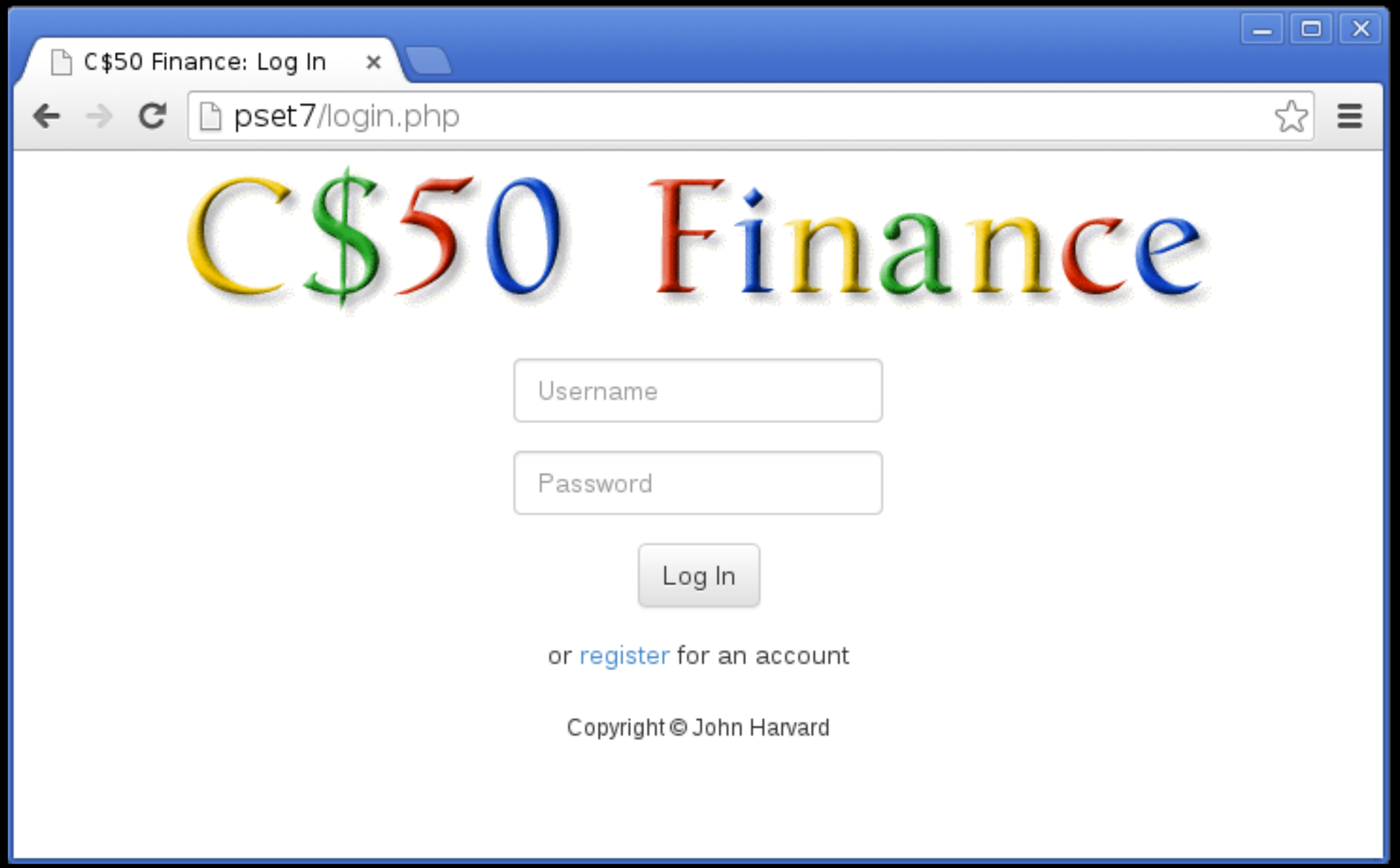
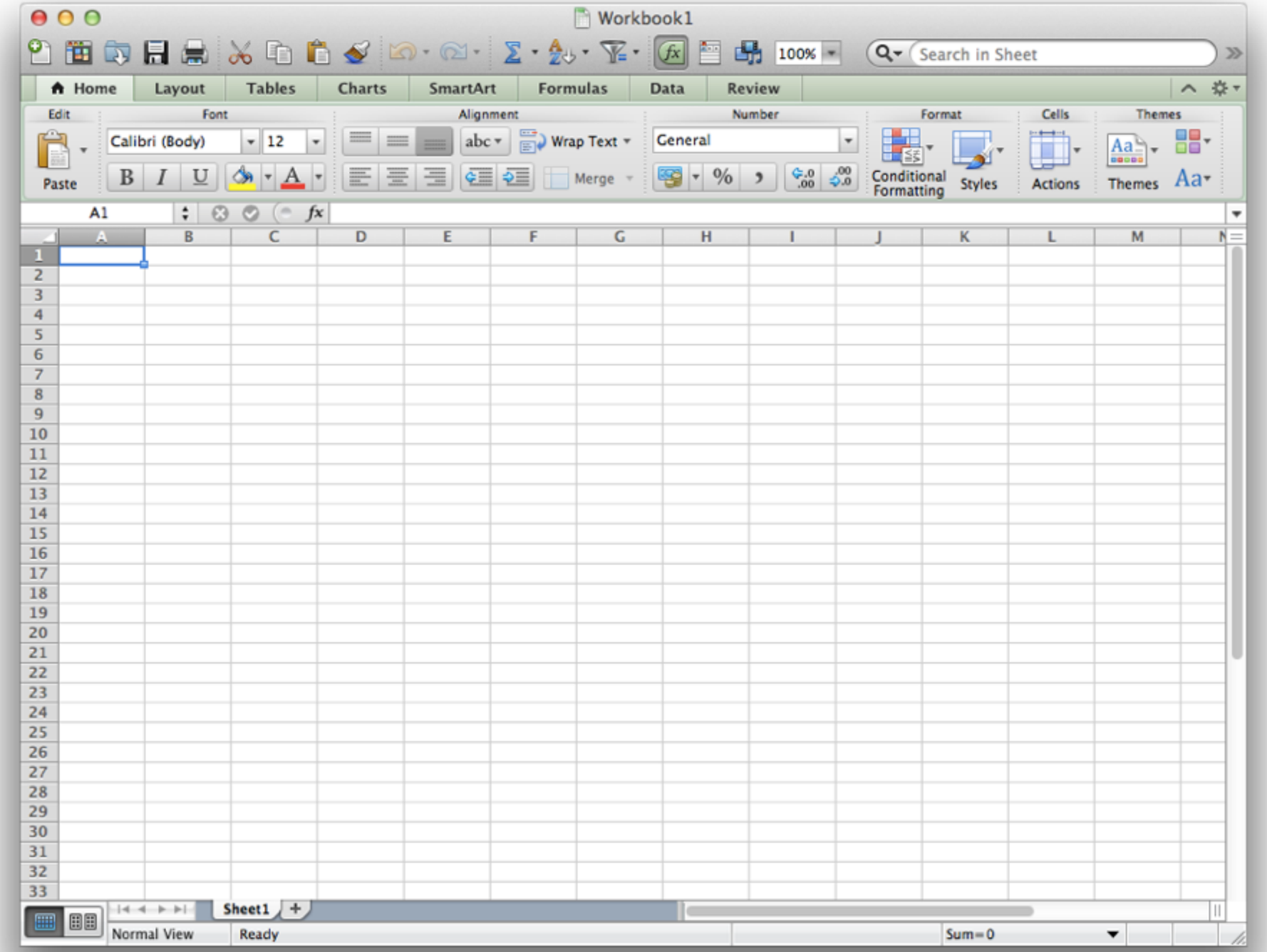

C$50 Finance: Log In
pset7/login.php
C$50 Finance
Username
Password
Log In
or register for an account
Copyright © John Harvard

SQL


Workbook1
100%
Search in Sheet
Home
Layout
Tables
Charts
SmartArt
Formulas
Data
Review
Edit
Font
Alignment
Number
Format
Cells
Themes
Paste
Calibri (Body)
12
Wrap Text
General
Merge
Conditional Formatting
Styles
Actions
Themes
A1
Sheet1
Normal View
Ready
Sum=0

SQL

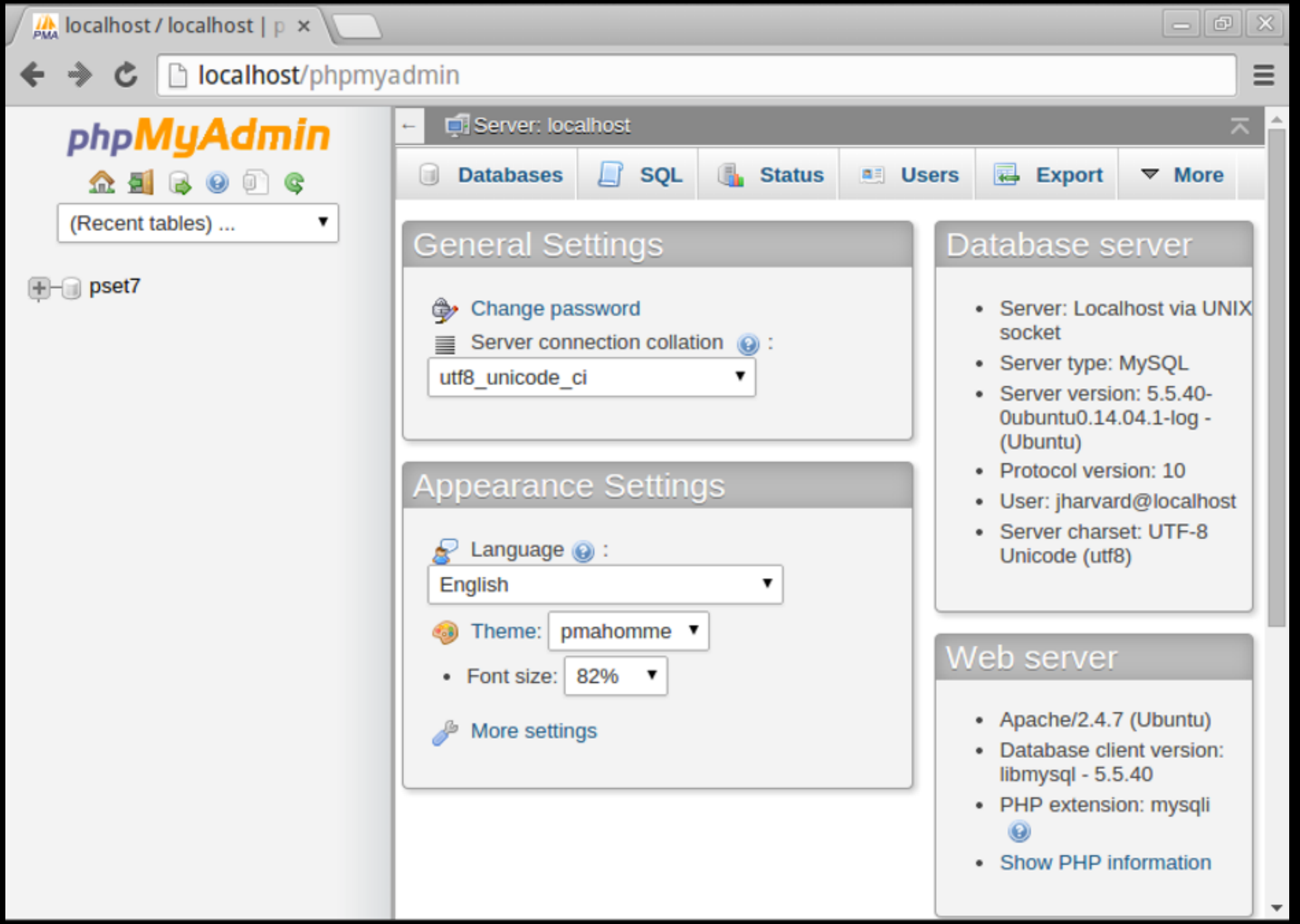
```
DELETE

INSERT

UPDATE

SELECT

...
```


localhost / localhost | p
localhost/phpmyadmin
phpMyAdmin
(Recent tables) ...
pset7
Server: localhost
Databases
SQL
Status
Users
Export
More
General Settings
Change password
Server connection collation :
utf8_unicode_ci
Appearance Settings
Language :
English
Theme: pmahomme
Font size: 82%
More settings
Database server
Server: Localhost via UNIX socket
Server type: MySQL
Server version: 5.5.40-0ubuntu0.14.04.1-log - (Ubuntu)
Protocol version: 10
User: jharvard@localhost
Server charset: UTF-8 Unicode (utf8)
Web server
Apache/2.4.7 (Ubuntu)
Database client version: libmysql - 5.5.40
PHP extension: mysqli
Show PHP information

types

CHAR

VARCHAR

INT

BIGINT

DECIMAL

DATETIME

...

indexes

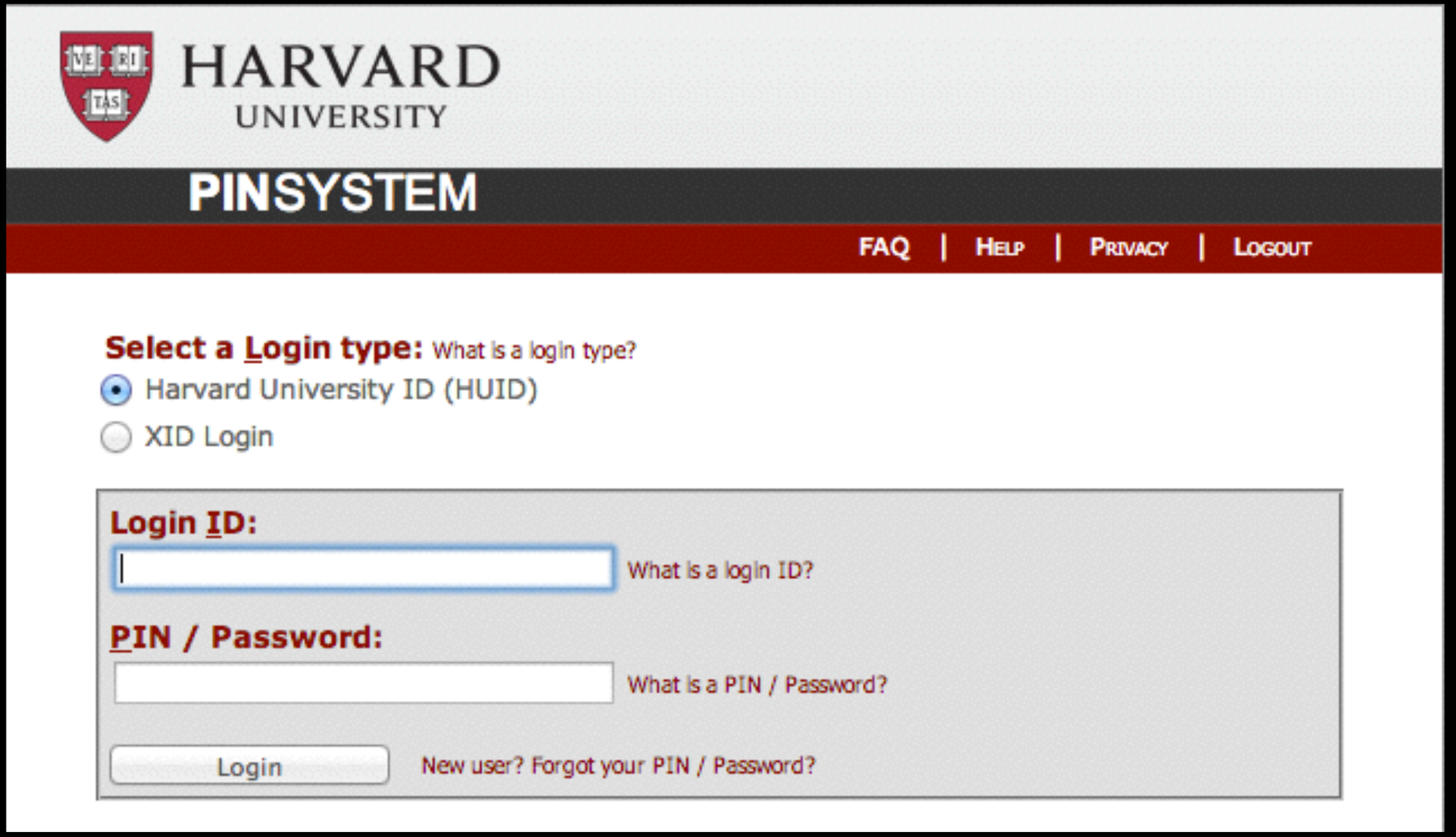
PRIMARY

INDEX

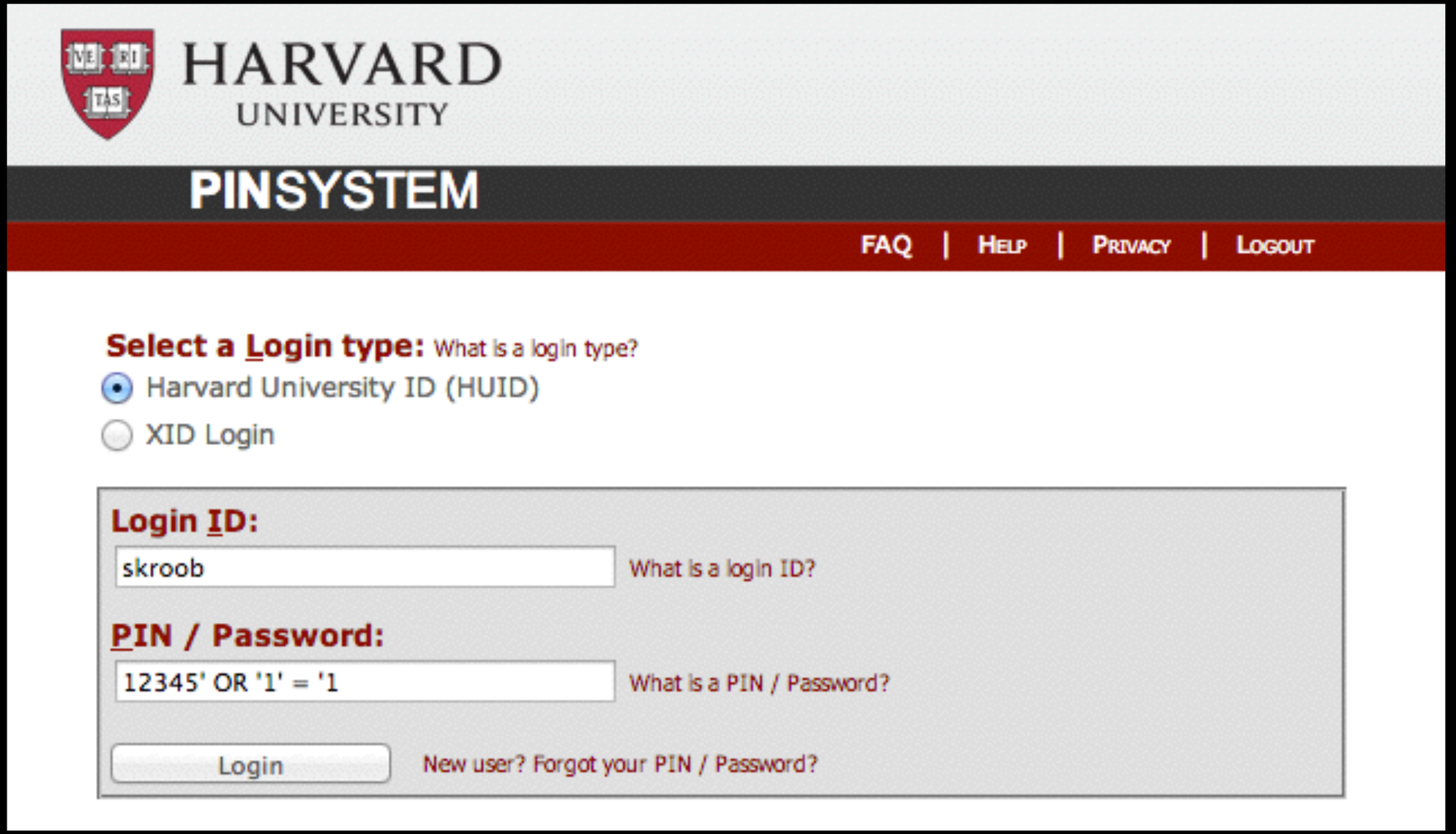
UNIQUE

FULLTEXT

SQL injection attack


HARVARD
UNIVERSITY
PINSYSTEM
FAQ | HELP | PRIVACY | LOGOUT
Select a Login type: What is a login type?
Harvard University ID (HUID)
XID Login
Login ID:
What is a login ID?
PIN / Password:
What is a PIN / Password?
Login
New user? Forgot your PIN / Password?

```
$username = $_POST["username"];
$password = $_POST["password"];
query("SELECT * FROM users WHERE username='{$username}' AND password='{$password}'");
```


HARVARD
UNIVERSITY
PINSYSTEM
FAQ | HELP | PRIVACY | LOGOUT
Select a Login type: What is a login type?
Harvard University ID (HUID)
XID Login
Login ID:
skroob
What is a login ID?
PIN / Password:
12345' OR '1' = '1
What is a PIN / Password?
Login
New user? Forgot your PIN / Password?

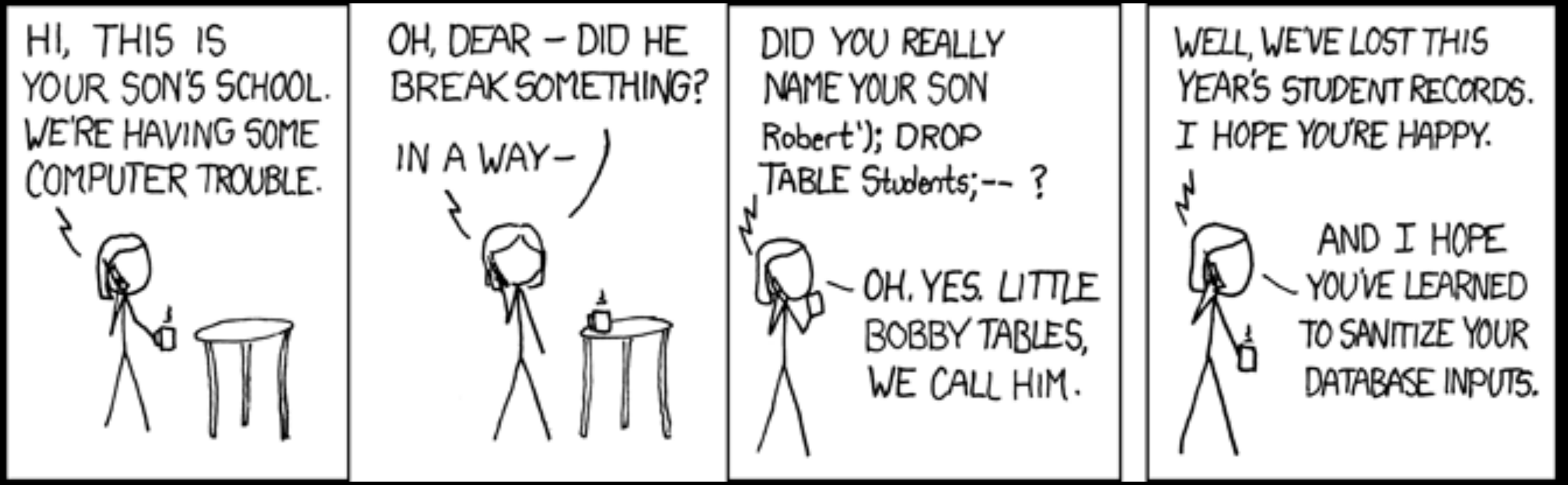
```
$username = $_POST["username"];
$password = $_POST["password"];
query("SELECT * FROM users WHERE username='{$username}' AND password='{$password}'");
```

```
$username = $_POST["username"];
$password = $_POST["password"];
query("SELECT * FROM users WHERE username='skroob' AND password='12345' OR '1' = '1'");
```

```
$username = $_POST["username"];
$password = $_POST["password"];
query("SELECT * FROM users WHERE username=? AND password=?", $username, $password);
```

```
$username = $_POST["username"];
$password = $_POST["password"];
query("SELECT * FROM users WHERE username='skroob' AND password='12345\' OR \'1\' = \'1'");
```


ZU 0666', 0, 0); DROP DATABASE TABLICE;



http://xkcd.com/327/

final project


PHILIPS

```
PUT /api/newdeveloper/lights/1/state HTTP/1.1

{"on":true, "bri":255, "transitiontime":0}
```


ARDUINO
UNO
DIGITAL (PWM~)
POWER
ANALOG IN
Genuino
UNO
DIGITAL ~ PWM~
POWER
ANALOG IN