

week 10, continued

`$_SESSION`

Ajax

quiz I

Wed 11/20

pset8

```
earth.getLayerRoot().enableLayerById(earth.LAYER_BUILDINGS, true);
```

```
earth.getLayerRoot().enableLayerById(earth.LAYER_BUILDINGS, false);
```

# CS50 Hackathon

Wed 12/4 – Thu 12/5



# CS50 Fair

Mon 12/9

final project

Alltel: #####@message.alltel.com  
AT&T: #####@txt.att.net  
MetroPCS: #####@mymetropcs.com  
Nextel: #####@messaging.nextel.com  
Powertel: #####@ptel.net  
Sprint: #####@messaging.sprintpcs.com  
SunCom: #####@tms.suncom.com  
T-Mobile: #####@tmomail.net  
US Cellular: #####@email.uscc.net  
Verizon: #####@vtext.com  
Virgin Mobile: #####@vmobl.com

textmarks.com

parse.com

# CS50 ID

[manual.cs50.net/id](https://manual.cs50.net/id)

# web hosting

[cs50.net/hosting](https://cs50.net/hosting)

SSL



security



Installer is trying to install new software. Type your password to allow this.

Name: malan

Password:

Cancel

Install Software

Cancel

Install Software

## Enter your Online ID

Sign In



☐ Save this Online ID

Select account location



▶ [Help/options](#)

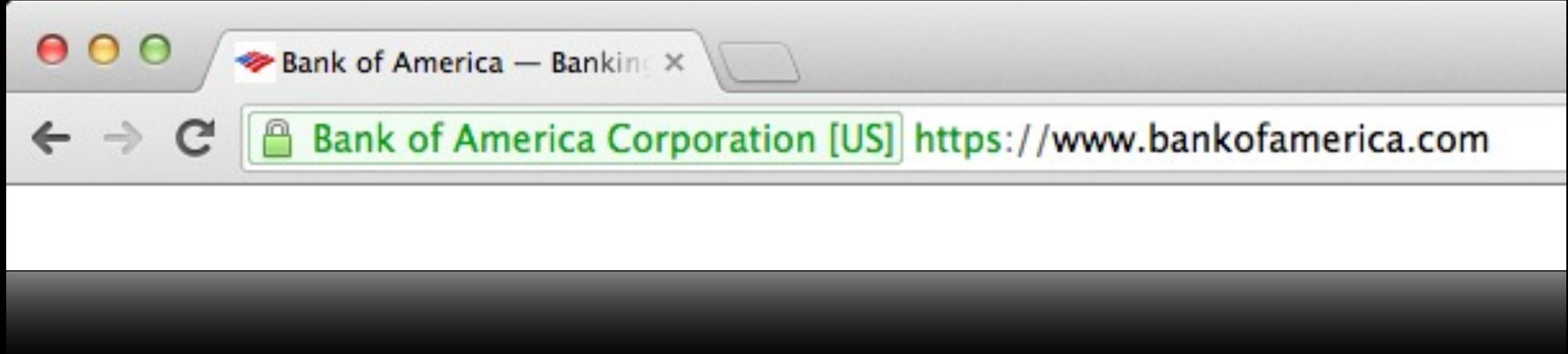
Enroll

▶ [Help/options](#)

Enroll

Select account location





session hijacking

SSL?

# 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?](#)

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?](#)

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='1' 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='1\' OR \'1\' = \'1'");
```

HI, THIS IS  
YOUR SON'S SCHOOL.  
WE'RE HAVING SOME  
COMPUTER TROUBLE.



OH, DEAR — DID HE  
BREAK SOMETHING?

IN A WAY —



DID YOU REALLY  
NAME YOUR SON  
Robert'); DROP  
TABLE Students; -- ?



OH, YES. LITTLE  
BOBBY TABLES,  
WE CALL HIM.

WELL, WE'VE LOST THIS  
YEAR'S STUDENT RECORDS.  
I HOPE YOU'RE HAPPY.



AND I HOPE  
YOU'VE LEARNED  
TO SANITIZE YOUR  
DATABASE INPUTS.

V IIII

V IIII

V

ME CALL HIM.

V

DATABASE INPUTS.

to be continued...