CS 155

Section 4, Extra Reference Slides

May 1, 2015

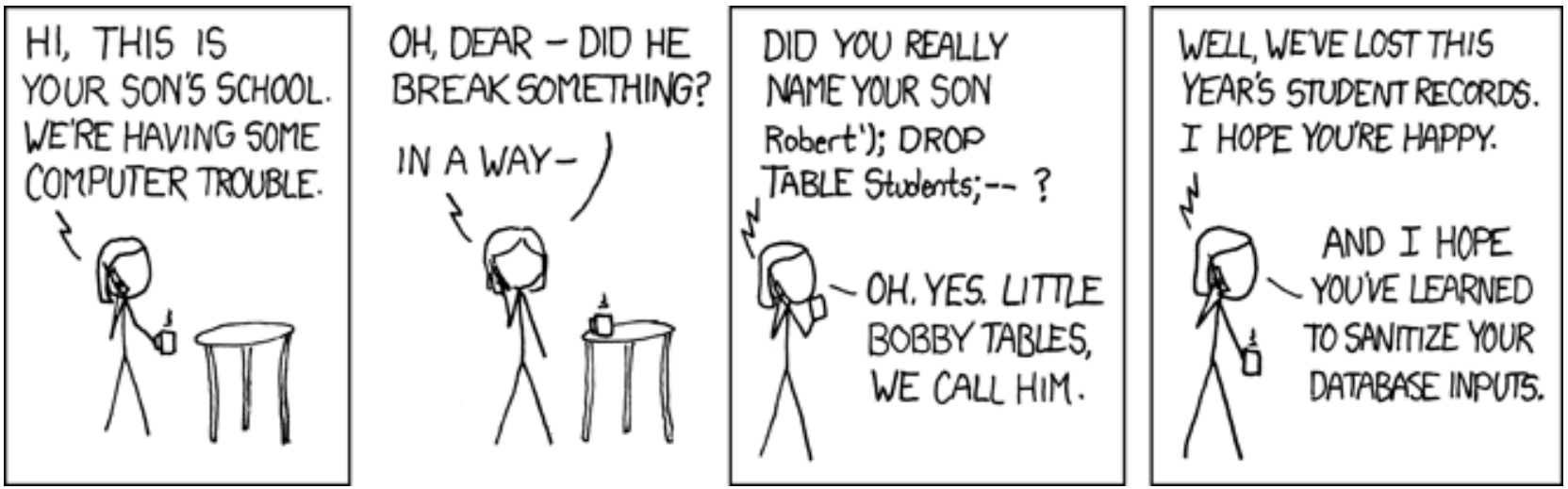
Outline

SQL Injection

CSRF

Clickjacking

SQL Injection



SQL Injection Demo Code

initialize.sql

```
create table STUDENTS(name string);
insert into STUDENTS  VALUES("Albert");
```

AddStudent.php

```
<?php
$handle= new SQLite3("school.db");
$q = "INSERT INTO Students VALUES ('" . $argv[1]    . "')";
$handle->exec($q);
?>
```

Commands to Run

```
sqlite3 school.db  < initialize.sql
php AddStudent.php "Robert'); DROP TABLE STUDENTS; --"
```

http://stackoverflow.com/q/332365

Cross Site Request Forgery (CSRF)

1. User logs into `www.bankofamerica.com`.
2. User visits `www.freemoviesforfools.com`.
3. Javascript submits a form or AJAX request to `www.bankofamerica.com`: "Please transfer $100000 to Bob."
4. Browser generously forwards login credentials along with the request.
5. Bob becomes wealthier. User becomes less wealthy.

`http://stackoverflow.com/q/2581488`

Cross Site Request Forgery (CSRF)

Why doesn't the Same Origin Policy prevent CSRF attacks?

"Under the policy, a web browser permits scripts contained in a first web page to access data in a second web page, but only if both web pages have me origin." – Wikipedia

SOP prevents one website from reading another's data, but does not prevent one website from sending POST requests to another!

`http://en.wikipedia.org/wiki/Same-origin_policy`

Clickjacking - When CSRF Fails

If the victim website implements defenses against CSRF (Project 2, Part 2), then we must enlist more help from the user than just asking him to load our malicious page.

1. User logs into `www.bankofamerica.com`.
2. User visits `www.freemoviesforfools.com`.
3. User clicks a button "I Want Free Movies".
4. Bob becomes wealthier. User becomes less wealthy.

Clickjacking

`www.freemoviesforfools.com` contains an invisible `iframe` containing the Transfer page for Bank of America. This frame is overlayed on top of the button that the user clicked.

Clearly, it can be substantial security flaw to allow yourself to be framed by other pages.

In this project, you will experiment with frame-busting and anti-frame-busting techniques.