Outline

SQL Injection

CSRF

Clickjacking
SQL Injection

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.
SQL Injection Demo Code

initialize.sql

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

AddStudent.php

```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)

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
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.

3. User clicks a button “I Want Free Movies”.
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.