CSE 484 / CSE M 584 Computer Security: Lab 2 review

TA: Viktor Farkas

vfarkas@cs

Logistics / Reminders

- Lab 2 is out, due Nov 21 5pm
- Fill out the sign up form to form groups
- Make sure to submit necessary files to dropbox (your attack strings, explanations, any additional files)

Lab 2

- 3 types of attacks:
  - 6 XSS attacks + 2 Extra credit
  - 2 SQL Injection attacks + 1 Extra credit
  - 1 CSRF attack + 1 Extra credit

http://www.owasp.com

OWASP Top 10 Web Vulnerabilities

1. Injection
2. Broken Authentication & Session Management
3. Cross-Site Scripting
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery
9. Using Known Vulnerable Components
10. Unvalidated Redirects and Forwards

XSS review

- Allows the attacker to inject JavaScript into web pages viewed by other users.
- JavaScript can do a lot of things, like reading cookies and ex-filtrating them.
- Sanitize/validate your input
- Browser detection

Basic setup

- Give the bot (codered.cs) a link with a XSS vulnerability.
- Bot will visit this link with cookie set, and cookie will be stolen.
- The process of stealing cookie involves sending it to a place **you** control.
- Save the cookie, read it, and use it.
- Easy!

What you will need

- Firefox, latest version should be OK
  - Chrome won’t work
- Firebug add-on for Firefox
- Setup a location to collect your ~~stolen~~ liberated cookies
  - Good place is homes.cs
- URL encoder (converts characters into a format for transmission over the internet)

PHP review

- A **server**-side programming language
- File extension is .php
- Before a webpage is sent to you, PHP code is executed by the server
- You won’t see the PHP code, only html
- PHP can be use to set and read cookies for authentication
- You will need a basic PHP script to receive captured cookies

SQL Injection

- SQL Injection allows the attacker to insert malicious SQL statements
- Usually caused by incorrect filtering of user input

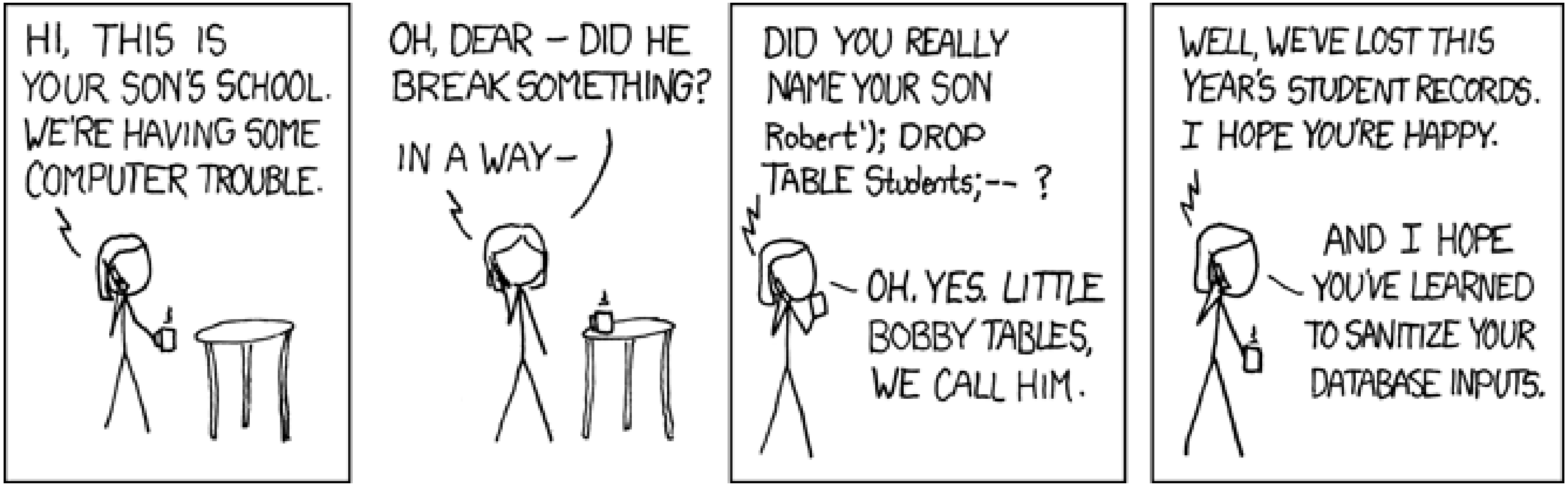
SQL Review

- Structured Query Language (SQL) used to communicate with databases
- Standard SQL commands SELECT, INSERT, UPDATE, DELETE, DROP

Select

- Used to select (read) data from a database
- SELECT *column_name*,*column_name*
FROM *table_name*
WHERE *column_name operator value*;

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.

HTTP://XKCD.COM/327/

Helpful resources

- SQL Injection – OWASP https://www.owasp.org/index.php/SQL_Injection
- Cross-site Scripting (XSS) https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Overview of setup

codered.cs

Hacker (you)

homes.cs

Tips

- Be mindful of Same Origin Policy
  - Don’t redirect codered
- Run JavaScript locally before sending to codered
- When URL encoding, be careful of new-lines in XSS
  - Browser might stop executing at newline
- Talk to us if something feels wrong / confusing

Insert

- Insert new records in a table
- INSERT INTO *table_name*
  VALUES (*value1*,*value2*,*value3*,...);
- INSERT
  INTO *table_name* (*column1*,*column2*,...)
  VALUES (*value1*,*value2*,...);