Web Security

Carl Jackson ’13

Today:

1. XSS

2. CSRF

Today:

3. SQL Injection
4. Password Security
5. Shell Injection

Be Ethical

Don’t Try This At Home

Haxxr

A Twitter Clone

http://hax.avtok.com

(use private browsing)

XSS

XSS

- Cross-Site Scripting
- Insert Malicious Javascript
- *Persistent* vs *Non-Persistent*

Try it out!

- `alert("oh hai");`
- Post something
- Write a worm
- Steal someone's cookies

Prevent XSS

- Sanitize user input. In PHP, `htmlspecialchars`
- Escape attributes too!

CSRF

CSRF

What if I could make requests to your bank on your behalf?

```
<img src="http://bank.com?
transfer=1000000&to=carl" />
```

Stop CSRF

- Put a token on every page
- Send the token every req.
- Only pages on your site know the token!

SQL Injection

SQL Injection

- Trick database into running malicious queries
- Steal data or be destructive

SQL Injection

```
"SELECT * FROM users WHERE
name='$name'"
```

```
$name="' OR ''='"
```

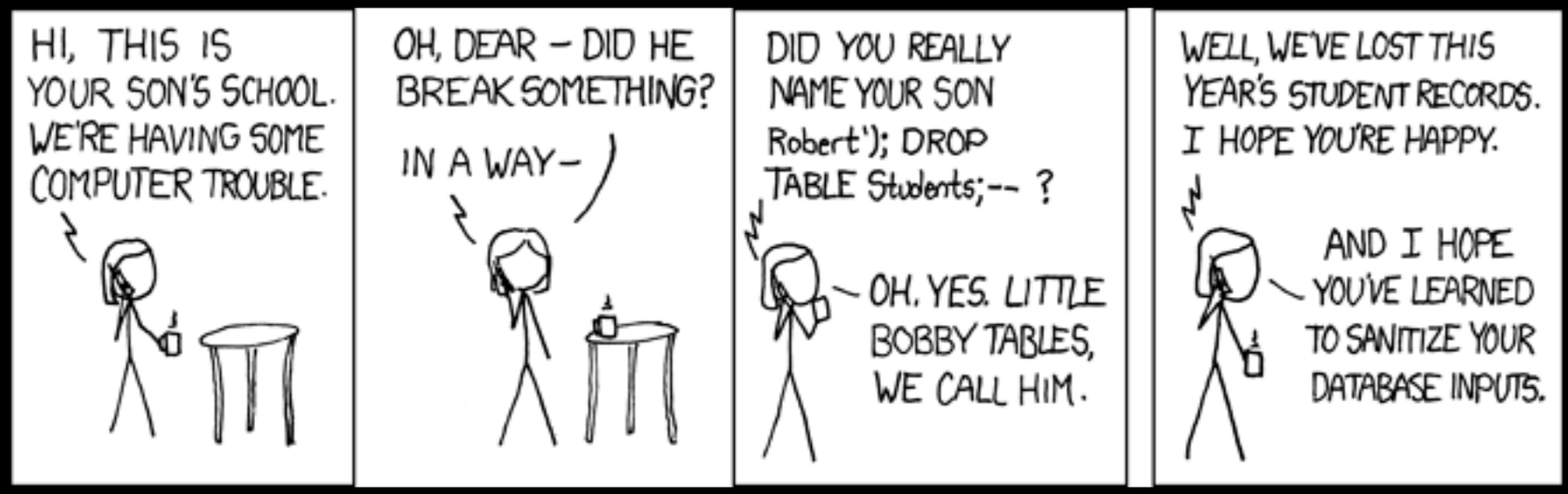
```
"SELECT * FROM users WHERE
name='' OR ''=''"
```

SQL Injection

```
"SELECT * FROM users WHERE
name='$name'"
```

```
$name="';DROP TABLE users;--"
```

```
"SELECT * FROM users WHERE
name='';DROP TABLE users;--'"
```


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.

Try it out!

- I disabled dropping tables
- Log in as someone else
- Get someone's password

SQL Injection

- Good:
  `mysql_real_escape_string`
- **Better:**
  `PDO::prepare`

SQL Injection

```
$db = new PDO( ... )
$q = $db->prepare("SELECT *
FROM users WHERE name=?")
$q->execute(array('carl'))
$q->fetch() // the result
```

Passwords

NEVER store passwords in plain text

Passwords

- Use a one-way hash

```
sha1($password)
```

Passwords

- Salting:

```
sha1('looo...oong' . $pw)
```

- Harder to precompute
- Random salts are better

Passwords

- Even better: use `crypt`
- Does salting, hashing, but *thousands* of times

Shell Injection

Shell Injection

- Allows anyone to run code on your site
- The hacker has **complete control**. You are f&$#ed.

Shell Injection

- Don't use `eval`
- Don't use `system`
- Don't allow file uploads

Principles

- Never trust the user
- Escape *everything*
- Security is *hard*
- When in doubt, ask

github.com/zenazn/hax

carl@hcs.harvard.edu