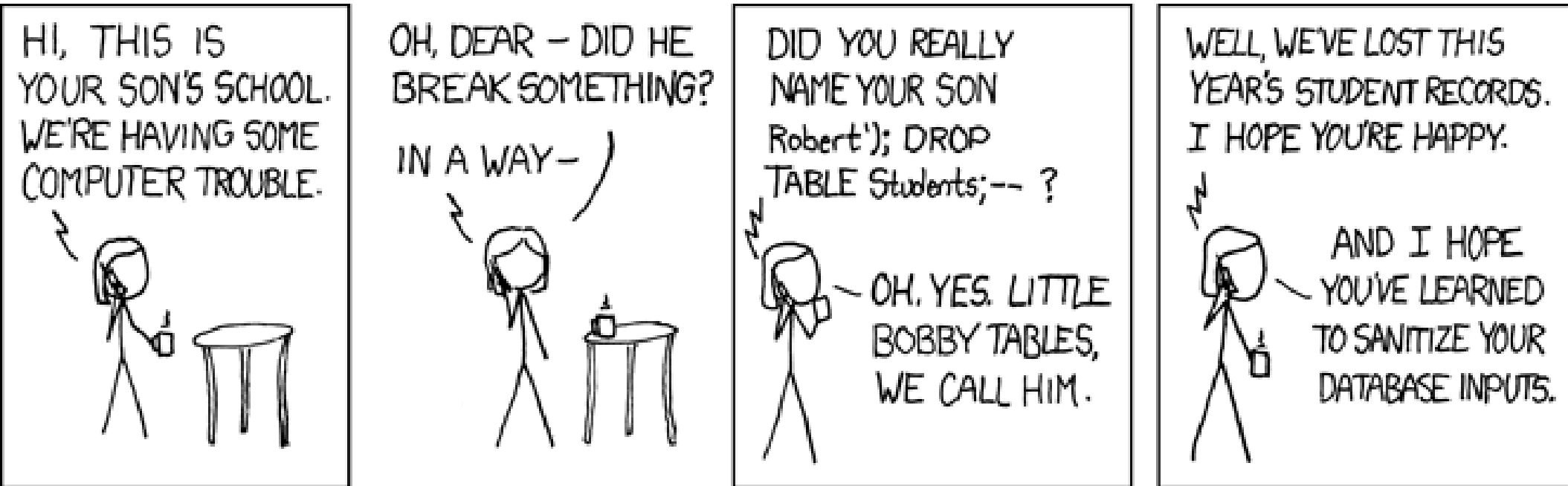


CSCI 3330 Cybersecurity



Word of the day

NO-OP n.,v. 1. A machine instruction that does nothing... 2. Any operation or sequence of operations with no effect, such as circling the block without finding a parking space, or putting money into a vending machine and having it fall immediately into the coin-return box, or asking someone for help and being told to go away. “Oh, well, that was a no-op.”

Review: in-band signals

- Phone phreaking (data: voice, control: tones)
- Directory traversal (data: names, control: /)
- Command line injection (data: arguments, control: spaces/punctuation)
- SQL injection (data: values, control: punctuation)

Phone phreaking

- What was the control signal that allowed you to get free phone calls?

Directory traversal

- `readfile("images/" . $input)`
- What is the control character?
- What `$input` gives you a path to `/etc/shadow`?

Command line injection

- `os.system("wget -Opage.html " + input)`
- What are the control characters?
 - Command line parsing (getopt)
 - Shell
- How do we overwrite a file?
- How do we run “printf CLI”?

SQL injection

- "SELECT * FROM users WHERE password = ' " + input + " ' "
- What are the control characters?
- What input creates a tautology that is a grammatically correct statement?

Mitigations?

```
"SELECT FROM users WHERE password = ' " +  
password + "'"
```


Escaping

- addslashes()
- “Magic quotes”
- mysql_escape_string()
- mysql_real_escape_string()

Prepared statements

- Remove the in-band signaling!
 - 1) Prepare (leave placeholders for parameters)
 - 2) Bind parameters
 - 3) Execute statement

Other techniques

- `sql("SELECT * FROM stuff WHERE thing = %d", 3);`

SQL exfiltration

- UNION: Combine two result sets
- SELECT ... UNION SELECT ...
- Demo

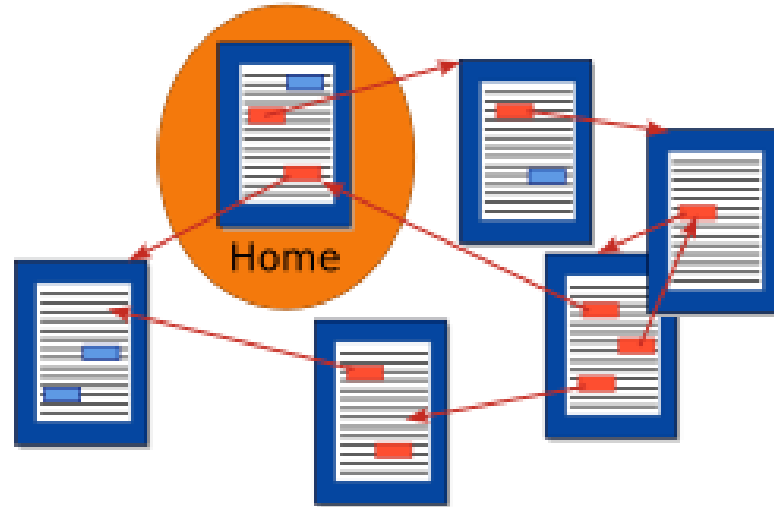
Web security

- The World Wide Web (WWW)



History

- Hypertext (1967)



History

- HyperCard
- Bill Atkinson, Apple 1987



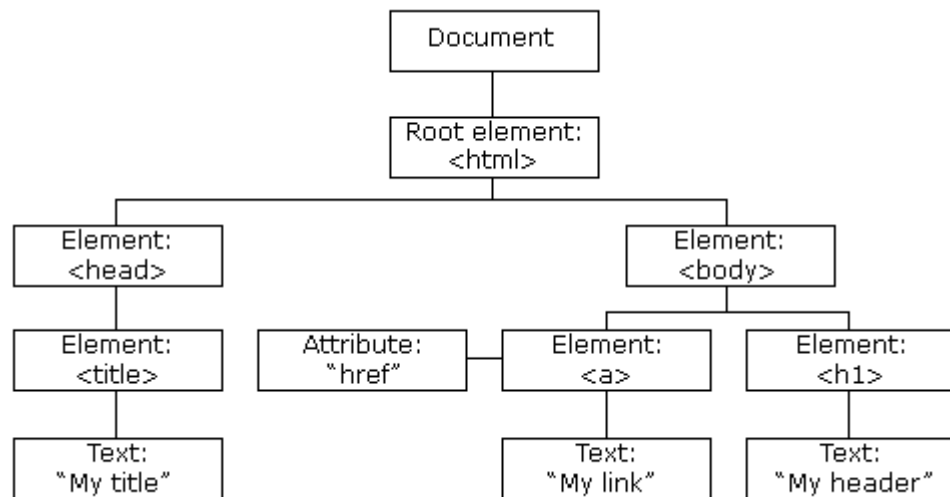
Web security

- The World Wide Web (WWW)
- Tim Berners-Lee
- 1989 (CERN)



HTML

- HyperText Markup Language



Minimal example

```
<html>  
<head>  
<title>Page Title</title>  
</head>  
<body>  
  
<h1>This is a Heading</h1>  
<p>This is a paragraph.</p>  
  
</body>  
</html>
```

Tags

- Each page consists of multiple elements
- `<html></html>`: root element
- `<head></head>`: header elements
- `<title></title>`: title of document (goes in head)
- `<body></body>`: document body elements

Headers

- h1, h2, h3, h4, h5, h6: header levels
- <p></p>: paragraph
- ...: unordered list
- ...: ordered list
- <hr></hr>: horizontal rule

Headers

- `<b></b>`, `<strong></strong>`: **bold**
- `<i></i>`, `<em></em>`: *italic*

Tables

- `<table>`
 - `<thead>` [optional]
 - `<tr>`
 - `<th>`
 - `<td>`
 - `</tr>`
 - `<tbody>` [optional]

Media and hyperlinks

- ``: images
- `<audio src="[url]" />`: audio
- `<video src="[url]" />`: audio
- `<a href="[url]" />`: **hyperlink**

CSS

- Cascading style sheets

```
<style>
```

```
    html { background-image: url("stars.gif") }
```

```
    p { font-size: 11pt }
```

```
</style>
```

```
<p style="font-family:monospace">...</p>
```


Create a quick web page

- Use tags `<h1>`, `<h2>`, `<a>`, `<b>`, `<i>`, `<img>`, `<hr>`
- Use CSS to create a background image

```
<html>
<head>
<title>Page Title</title>
</head>
<body>

<h1>This is a Heading</h1>
<p>This is a paragraph.</p>

</body>
</html>
```

Cookies

- Allow sites to remember / track you
- Permits, e.g., logging in
- Session cookies
- Persistent cookies
- Key-value pairs



DOM demo

- Let's look at cookies, DOM, and CSS!
- <https://news.ycombinator.com>

In-class Exercise

- <https://www.nytimes.com/2023/07/26/technology/russia-censorship-ukraine-war.html>
- **Minimum:** Get rid of “Create a free account” popup
- **Expected:** Get rid of grey gradient shading
- **Cool:** restore article scrolling
- **Hint:** existence of CSS property “overflow: hidden” disables scrolling
- **Hint #2:** ctrl+z undo, refresh page if you really mess up

Assignment 2

- Deadline: September 25, 2025, 10:00pm
- Setuid binaries, directory traversal, command line injection

<https://tildesites.bowdoin.edu/~j.knockel/csci3330f25/assignment2.pdf>