INFO 310

Fall 2016

Week 10 – Lecture 2

HOUSEKEEPING

- Attendance
- Quick Lab Recap

Web Application Security (& friends)

- **Web application security** is a branch of Information Security that deals specifically with security of websites, web applications and web services. At a high level, Web application security draws on the principles of application security but applies them specifically to Internet and. Web systems

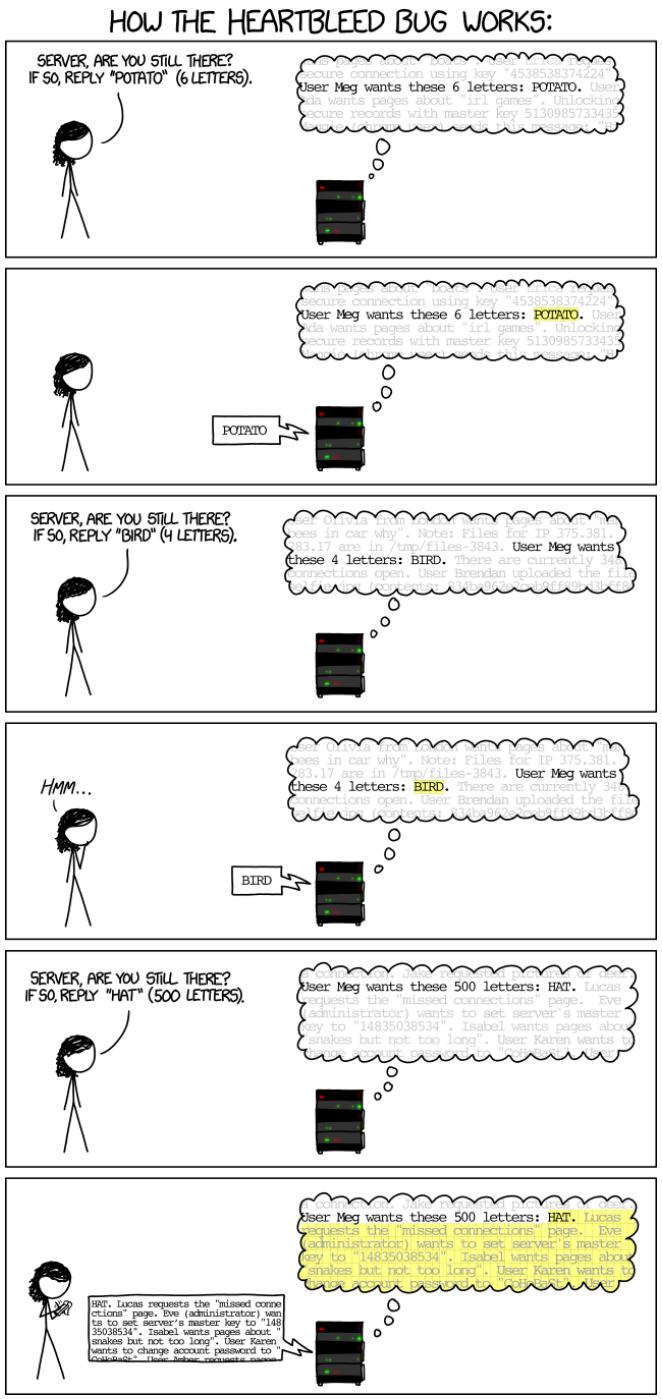
“Named / Branded” Vulnerabilities

- DROWN
  - “Decrypting RSA with Obsolete and Weakened eNcryption”
  - TLS -> SSLv2

- POODLE
  - “Padding Oracle On Downgraded Legacy Encryption”
  - Man-in-the-middle attack on SSL V3.0
- ShellShock
  - BASH – malicious ENV variable to echo malicious command
  - Commonly invoked via CGI

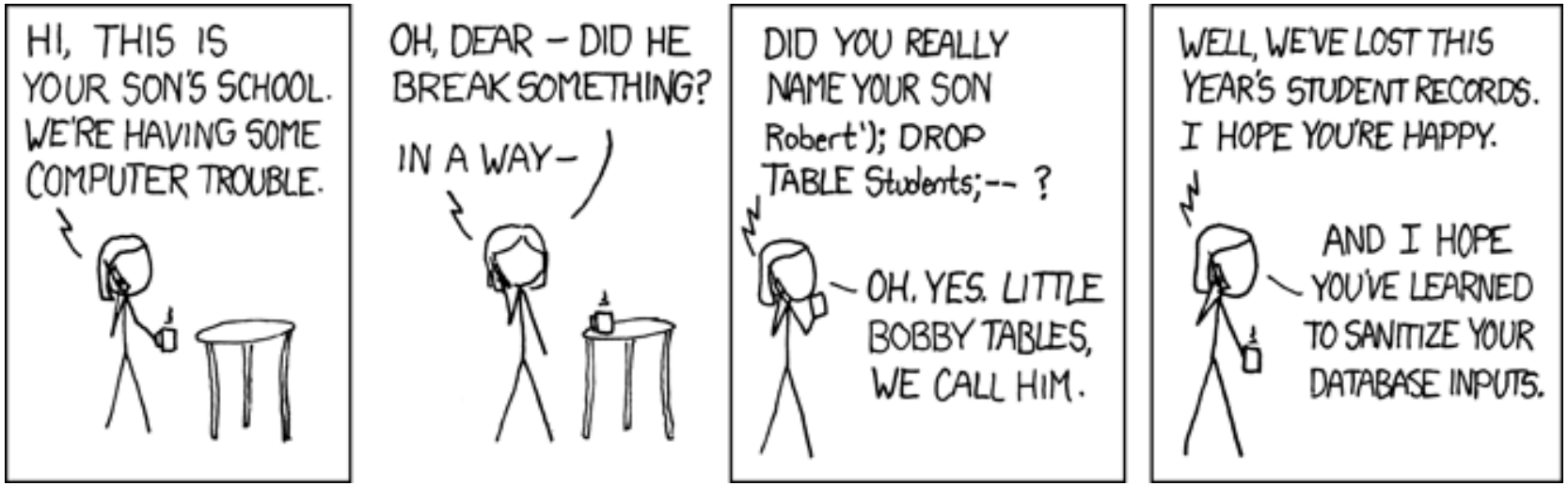
“Named / Branded” Vulnerabilities

- FREAK
  - "Factoring RSA Export Keys“
  - Decrypt session cookies
  - Apple Safari, Google Android, MS IE
- Heartbleed
  - OpenSSL Heartbeat



https://xkcd.com/1354/

SQL Injection (SQLi)



https://xkcd.com/327/

Cross Site Scripting (XSS)

- **Cross-site scripting** (**XSS**) is a type of security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy

Cross Site Request Forgery (CSRF)

- Cross-site request forgery, also known as a one-click attack or session riding, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Unlike cross-site scripting, which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

Other common pitfalls

- Remote File Includes
- Direct Object References
- Misconfigured instances of php, cgi, httpd, etc
- Exposed debug information

What you can do to try to prevent these attacks

- Sanitize Input
- Parameterize Queries
- Patch server side software
- Consider denying legacy clients based on user agent
- Track OWASP (Open Web Application Security Project) “Top 10” list
- Check (and re-check) file and directory permissions:

UNIX File permissions & .htaccess

- UNIX file permissions
  - Very important for web directories
  - Read, Write, Execute
  - Owner / Group / Other (world)
  - Numerical representation: Octal (base8)
    - The read bit adds 4 to its total (in binary 100),
    - The write bit adds 2 to its total (in binary 010), and
    - The execute bit adds 1 to its total (in binary 001).
  - chmod / chown
- .htaccess

```
drwxr-xr-x  2 dfs users 4096 Dec  3 15:59 .
drwx------ 13 dfs users 4096 Dec  3 15:48 ..
-rwxrwxrwx  1 dfs users    0 Dec  3 15:48 index.html
-r--------  1 dfs users    0 Dec  3 15:48 sekrit.html
```

Symbolic Notation	Numeric Notation	English
`----------`	0000	no permissions
`---x--x--x`	0111	execute
`--w--w--w-`	0222	write
`--wx-wx-wx`	0333	write & execute
`-r--r--r--`	0444	read
`-r-xr-xr-x`	0555	read & execute
`-rw-rw-rw-`	0666	read & write
`-rwxrwxrwx`	0777	read, write, & execute

(this page intentionally left blank)