University of Toronto Engineering

UNIVERSITY OF TORONTO
FACULTY OF APPLIED SCIENCE & ENGINEERING

Module 12 – Code Injection

XSS, SQL, and buffer overflows

UNIVERSITY OF TORONTO
FACULTY OF APPLIED SCIENCE & ENGINEERING

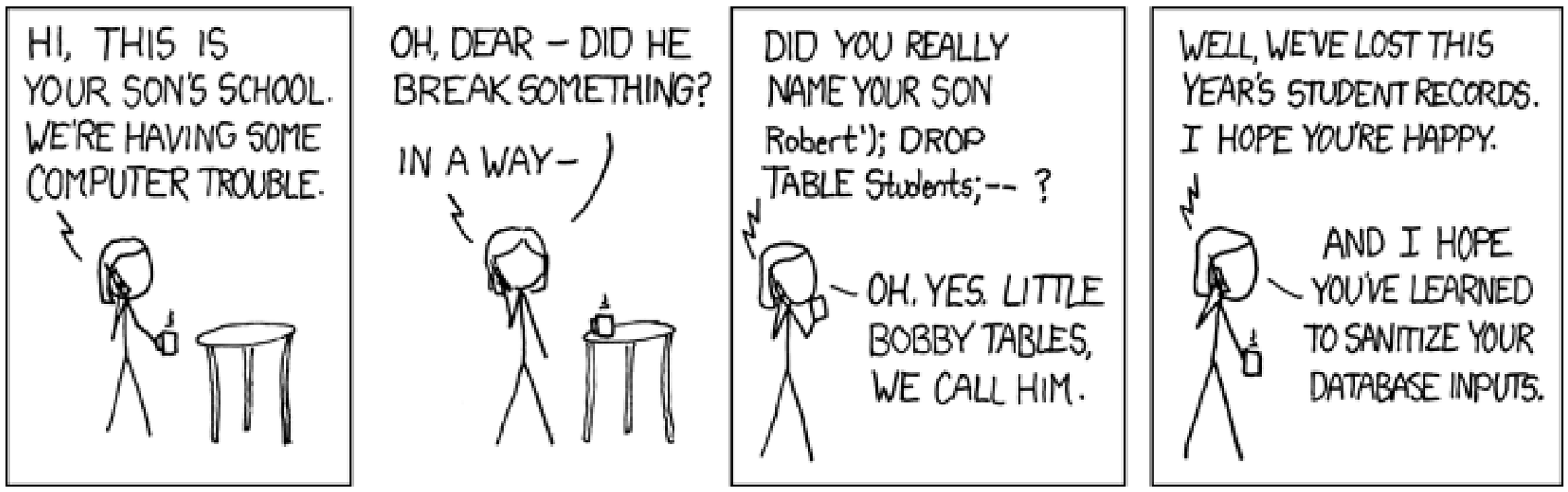
Module 12 – Code Injection

XSS stands for Cross-Site-Scripting

- Let's try it
- http://billy.scienceontheweb.net/gen/tryxss.php
- XSS is dangerous! It can change a form action page as we did in phishing, but it's the real site!
- How can we protect against it?
  - *Certificates don't work!*
  - *Being vigilant*
  - *Suspecting long URLs*
  - ***Sanitising input***
  - *Browsers*
    - *I had to give the HTTP header "X-XSS-Protection: 0" in that page*

Module 12 – Code Injection

- SQL injection is another common type, that inserts code into a database query
- We won't learn SQL today, but the gist is remarkably simple:



[32]

- Buffer overflows are another type of code injection…
  - *Open jibc again*
  - *We can set SP to be within the program code…*

Thanks!

Questions?

Email: b.graydon@ieee.org

UNIVERSITY OF TORONTO
FACULTY OF APPLIED SCIENCE & ENGINEERING