COMPUTER SCIENCE E-1

Understanding Computers & the Internet

PROBLEM SET 6

Due Monday, April 8 at 5:30pm

14 questions, out of 41 points

Academic Honesty

All work that you do toward fulfillment of this course's expectations must be your own unless collaboration is explicitly allowed by the staff. Viewing, requesting, or copying another individual's work or lifting material from a book, magazine, website, or other source—even in part—and presenting it as your own constitutes academic dishonesty, as does showing or giving your work, even in part, to another student.

Similarly is dual submission academic dishonesty: you may not submit the same or similar work to this course that you have submitted or will submit to another. Nor may you provide or make available solutions to homework or exams to individuals who take or may take this course in the future. Moreover, submission of any work that you intend to use outside of the course (e.g., for a job) must be approved by the staff.

If in doubt as to the appropriateness of some act, contact the staff. All forms of academic dishonesty are dealt with harshly.

Submission Instructions

To submit this problem set, head to E-1 Submit (http://cse1.net/submit), where you can upload a PDF, Word Document, or text file. PDF files are preferred.

Jam Session

1. **(4 points)** As an avid Twitter user, it would be devastating for me to have to log in every time I wanted to share another 140 characters of wisdom with the world. How is it that Twitter is able to remember who I am as I go on my tweeting rampage? Be specific as to exactly where information is stored as well as what is exchanged between my web browser and a server.

2. **(3 points)** Why might a server want to expire its session cookies after some amount of time?

Securitas

3. **(2 points)** How is HTTPS different from HTTP? Why does the "S" in HTTPS make sites more secure?

4. **(3 points)** You and a friend are both using the same wireless network to browse the web. The network is encrypted using WPA2. Is it possible for you to see the network traffic generated by your friend? Why or why not?

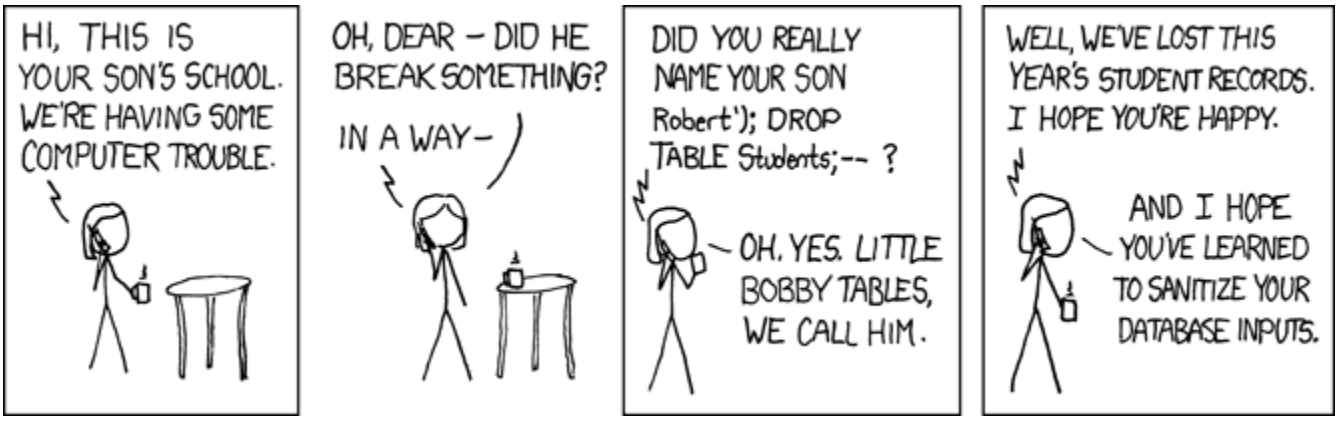
Attack of the Show

5. **(5 points)** You're running for class president at your high school, and your school has set up an online voting system. After logging in via your school's secure authentication system, students are taken to a form where they can select a candidate to vote for. You notice that after voting (for yourself of course), you were taken to the URL `http://school.edu/vote?for=you`. The next day, you find out that someone else has won the election by a landslide, but you suspect foul play is afoot. How could your opponent have taken advantage of the system? Propose a solution that would have thwarted your opponent's villainy.

6. **(3 points)** What's the difference between CSRF and XSS? How are XSS and session hijacking related?

7. **(3 points)** What is a SQL injection attack? What kind of damage might an attacker be able to incur via a SQL injection? How can we prevent SQL injections?

8. **(2 points)** What's so funny about the below?



Hail, Caesar!

9. **(2 points)** Give the ROT13 encryption of this message: "That's one small step for man; one giant leap for mankind." Assume that you can leave any punctuation as is , so you don't need to worry about encrypting those characters.

10. **(3 points)** The following message has been encrypted with ROT5 encryption. What does it say? "Mtzxyts, Ywfsvznqnyd Gfxj mjwj. Ymj Jflqj mfx qfsiji."

11. **(3 points)** How are the Caesar cipher and Vigenère cipher similar and different? Why is the Vigenère cipher more secure than the Caesar cipher?

12. **(3 points)** Using the Vigenère cipher and the key "ALICE", encrypt this message: "Sentence first—verdict afterwards." Just like last time, you can leave any punctuation as is.

13. **(3 points)** What's the difference between symmetric key cryptography and asymmetric key cryptography? Why might we want to combine the two approaches in some cases?

14. **(2 points)** Explain the roles of the public key and the private key in asymmetric key cryptography.