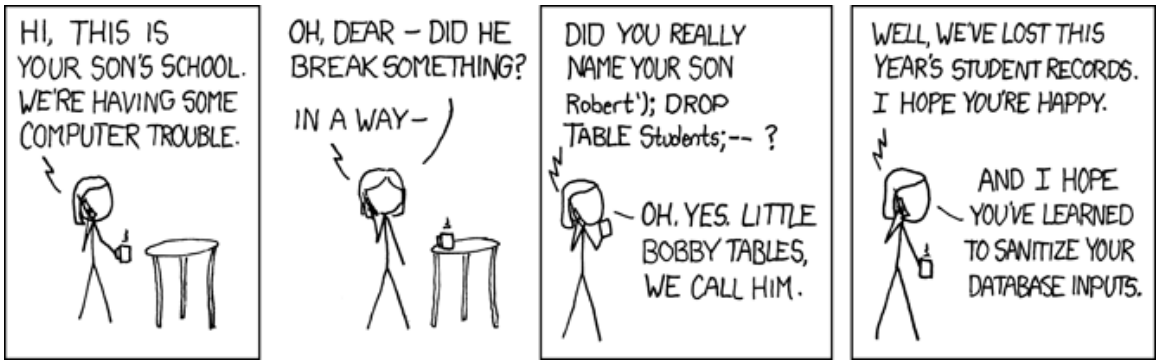
Multiple-Choice Questions:

1. What type of attack did the parents in this XKCD comic perform?



   a. Cross-site scripting
   b. SQL injection
   c. Child endangerment
   d. Reverse lookup
   e. Mask and shift

2. Which of the following is <u>not</u> a security exploit?

   a. Eavesdropping
   b. Cross-site scripting
   c. Authentication
   d. SQL Injection
   e. None of the above (i.e., they are all security exploits)

3. Where does packet sniffing happen?

   a. Over the network
   b. On GitHub
   c. In the database
   d. All of the above
   e. None of the above

4. How do you prevent SQL injection?
    a. Escape queries
    b. Interrupt requests
    c. Merge tables
    d. All of the above
    e. None of the above

5. In cross-site scripting where does the malicious script execute?
    a. On the web server
    b. In the user's browser
    c. On the attacker's system
    d. In the web app model code
    e. None of the above

6. Which of the following is <u>not</u> a CERT security practice?
    a. Adhere to the principle of least privilege
    b. Sanitize data sent to other software
    c. Use effective quality assurance techniques
    d. Validate input
    e. None of the above (i.e., all of them are CERT security practices)

7. T or F? Eavesdropping can be countered by using encryption.
    a. True
    b. False

8. How do you prevent packet-sniffing exploits?

    a. Escape packet text

    b. Scan for viruses

    c. Encrypt network communication with SSL

    d. Packet plugs

    e. None of the above

9. Imagine a social networking web app (like Twitter) that allows users to post short blurbs of text. Which type of exploit might be carried out by posting text that contains malicious code?

    a. Cross-site scripting

    b. SQL injection

    c. Packet sniffing

    d. a and b

    e. a, b, and c

10. Which of the following are most vulnerable to injection attacks?

    a. Session IDs

    b. Registry keys

    c. Network communications

    d. SQL queries based on user input

    e. None of the above are vulnerable to injection attacks

11. Which of the following is not a CERT security practice?

    a. Use blacklists to restrict access to services and resources

    b. Sanitize data sent to other software

    c. Use effective quality assurance techniques

    d. Validate input

    e. None of the above (i.e., all of them are CERT security practices)

Solutions:

1. b
2. c
3. a
4. a
5. b
6. e
7. a
8. c
9. d
10. d
11. a

Problem: Consider a web app that displays user posts, similar to Twitter and Facebook. The developers of the web app have accidentally left it vulnerable to cross-site scripting attacks. Explain how you would perform a cross-site scripting attack against the web app. Be thorough in your explanation.

Solution:

I would set up the attack by creating JavaScript that does something harmful. For example, it might redirect the current webpage to one that I made. My web page might try to trick the user into entering his/her username and password, which I would then steal.

To perform the attack, I would make a user post using the web app. My post would contain HTML code that causes my JavaScript to execute when loaded. Thus, any web app user who viewed my post would fall victim to my attack.