Multiple-Choice Questions:

1. Which of the following does <u>authentication</u> aim to accomplish?

   a. Restrict what operations/data the user can access

   b. Determine if the user is an attacker

   c. Flag the user if he/she misbehaves

   d. Determine who the user is

   e. None of the above

2. Which of the following does <u>authorization</u> aim to accomplish?

   a. Restrict what operations/data the user can access

   b. Determine if the user is an attacker

   c. Flag the user if he/she misbehaves

   d. Determine who the user is

   e. None of the above

3. Which of the following is an <u>authentication method</u>?

   a. Secret question

   b. Biometric

   c. Password

   d. SMS code

   e. All of the above

4. T or F? In <u>role-based access control</u>, each user is assigned one or more roles, and the roles determine which parts of the system the user is allowed to access.
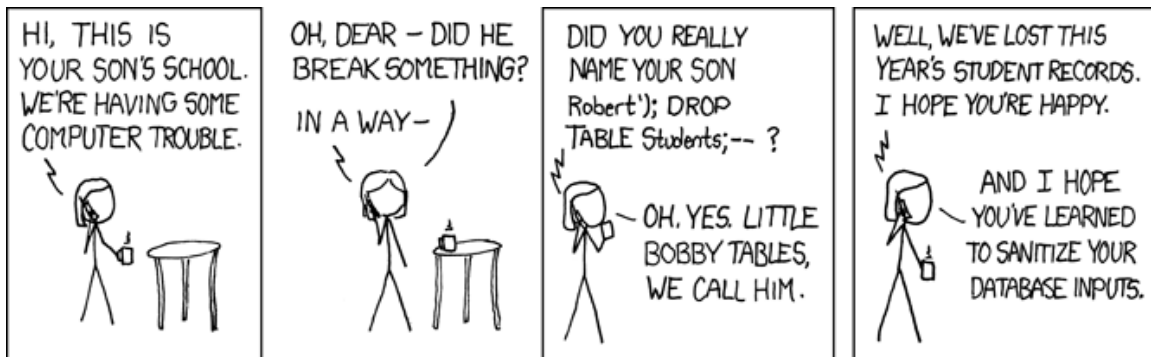
   a. True

   b. False

Solutions:

1. d

2. a

3. e

4. a

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 the 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

Solutions:

1. b

2. c

3. a

4. a

5. b

6. e

7. a

8. c

9. d