# Latest Version: 18.0

## Question: 1

In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

A. Smurf
B. distributed denial of service
C. cross-site scripting
D. rootkit exploit

**Answer: C**

Explanation
Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message.
Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on.
For example the code below is written in hex: <a
href=javascript:alert&#
x28'XSS')>Click Here</a>
is equivalent to:
<a href=javascript:alert('XSS')>Click Here</a>
Note: In the format "&#xhhhh", hhhh is the code point in hexadecimal form.

## Question: 2

Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

A. user input validation in a web page or web application
B. Linux and Windows operating systems
C. database
D. web page images

**Answer: A**

Explanation
SQL injection usually occurs when you ask a user for input, like their username/userid, but the user gives ("injects") you an SQL statement that you will unknowingly run on your database. For example:
Look at the following example, which creates a SELECT statement by adding a variable (txtUserId) to a

Select string. The variable is fetched from user input (getRequestString):
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
If user enter something like this: "100 OR 1=1" then the SQL statement will look like this:
SELECT * FROM Users WHERE UserId = 100 OR 1=1;
The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE. A hacker might get access to all the user names and passwords in this database.

## Question: 3

Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two)

A. Check integer, float, or Boolean string parameters to ensure accurate values.
B. Use prepared statements and parameterized queries.
C. Secure the connection between the web and the app tier.
D. Write SQL code instead of using object-relational mapping libraries.
E. Block SQL code execution in the web application database login.

**Answer: A, B**

## Question: 4

Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)

A. Patch for cross-site scripting.
B. Perform backups to the private cloud.
C. Protect against input validation and character escapes in the endpoint.
D. Install a spam and virus email filter.
E. Protect systems with an up-to-date antimalware program

**Answer: D, E**

Explanation
Phishing attacks are the practice of sending fraudulent communications that appear to come from a Reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information,
or to install malware on the victim's machine.

## Question: 5

Which two mechanisms are used to control phishing attacks? (Choose two)

A. Enable browser alerts for fraudulent websites.
B. Define security group memberships.
C. Revoke expired CRL of the websites.
D. Use antispyware software.
E. Implement email filtering techniques.

**Answer: A, E**