Started on	Thursday, 13 March 2025, 3:25 PM
State	Finished
Completed on	Thursday, 13 March 2025, 3:38 PM
Time taken	12 mins 48 secs
Marks	14.00/15.00
Grade	**93.33** out of 100.00

Question 1

Complete

Mark 1.00 out of 1.00

What does `--` in an SQL Injection attack do?

- a. Increases query execution speed
- b. Comments out the rest of the SQL query
- c. Adds an additional condition to the query
- d. Encrypts user input

Question 2

Complete

Mark 1.00 out of 1.00

Why does this React component not execute XSS payloads?

- a. React automatically escapes input to prevent script execution
- b. The browser blocks all inline scripts by default
- c. dangerouslySetInnerHTML is required to execute scripts
- d. The comment data is stored in a secure database

Question 3

Complete

Mark 1.00 out of 1.00

How can a developer protect against XSS attacks in a MERN stack app?

- a. Use dangerouslySetInnerHTML without sanitization
- b. Use inline JavaScript to filter malicious code
- c. Sanitize user input using DOMPurify or server-side escaping
- d. Allow script execution inside innerHTML

Question 4

Complete

Mark 1.00 out of 1.00

What is the most common way to fix XSS vulnerabilities?

- a. Storing scripts in the database
- b. Using JavaScript's eval() function
- c. Allowing only admin users to enter scripts
- d. Using DOMPurify to sanitize user input

Question 5

Complete

Mark 1.00 out of 1.00

Which of the following XSS payloads is most likely to bypass filtering?

- a. <iframe src=javascript:alert('XSS')>
- b. All of the above
- c. <img src=x onerror=alert('XSS')>
- d. <script>alert('XSS')</script>

Question 6

Complete

Mark 1.00 out of 1.00

Which payload can be used to bypass authentication in an SQL injection attack?

- a. '; SELECT * FROM passwords;
- b. ' OR username='admin' AND password='admin';
- c. ' OR 1=1 --
- d. ' AND DROP TABLE users;

Question 7

Complete

Mark 1.00 out of 1.00

Which of the following SQL queries is vulnerable to SQL Injection?

- a. SELECT * FROM users WHERE username = '" + user_input + "' AND password = '" + pass_input + "';
- b. SELECT * FROM users WHERE username = 'admin' AND password = 'admin';
- c. PREPARE stmt FROM 'SELECT * FROM users WHERE username = ? AND password = ?';
- d. SELECT * FROM users WHERE username = ? AND password = ?;

Question 8

Complete

Mark 1.00 out of 1.00

What is the main difference between SQL Injection and XSS?

- a. SQL Injection targets databases, while XSS targets browsers
- b. SQL Injection is always more dangerous than XSS
- c. Both are prevented using the same techniques
- d. XSS can modify SQL databases

Question 9

Complete

Mark 1.00 out of 1.00

How does the fixed version of the XSS Demo prevent XSS?

- a. By blocking all comments containing <script>
- b. By only allowing administrators to post comments
- c. By encoding all data before storing it
- d. By using DOMPurify to sanitize both input and output

Question 10

Complete

Mark 1.00 out of 1.00

What is SQL Injection?

- a. A way to encrypt SQL queries
- b. A tool to optimize database performance
- c. A method to securely access a database
- d. A technique used to bypass authentication and manipulate database queries

Question 11

Complete

Mark 1.00 out of 1.00

What is the best way to protect a Node.js MySQL database from SQL Injection?

- a. Validate user input with client-side JavaScript only
- b. Store passwords in plain text for easy authentication
- c. Use eval() to sanitize user input
- d. Use prepared statements and parameterized queries

Question 12

Complete

Mark 0.00 out of 1.00

Which of the following is NOT a way to prevent SQL Injection?

- a. Using ORMs like Sequelize or Mongoose
- b. Using Prepared Statements
- c. Escaping user input before using it in a query
- d. Using DOMPurify for sanitization

Question 13

Complete

Mark 1.00 out of 1.00

What additional security measures can prevent XSS attacks?

- a. Content Security Policy (CSP)
- b. Sanitizing user input before storing it
- c. Escaping special characters (<, >)
- d. All of the above

Question 14

Complete

Mark 1.00 out of 1.00

Which of the following best describes Stored XSS?

- a. XSS that only works on outdated browsers
- b. A script is executed immediately when injected
- c. A script is embedded in a URL and executed when the victim clicks the link
- d. The malicious script is stored in the database and executed when loaded by a user

Question 15

Complete

Mark 1.00 out of 1.00

What does the dangerouslySetInnerHTML property in React do?

- a. Blocks XSS automatically
- b. Encrypts JavaScript code
- c. Prevents all forms of user input
- d. Allows raw HTML to be inserted into the page