

Injections\_Quiz

Started on

Thursday, 13 March 2025, 3:25 PM

State

Finished

Completed on

Thursday, 13 March 2025, 3:29 PM

Time taken

3 mins 20 secs

Marks

15.00/15.00

Grade

100.00 out of 100.00

Question 1

Complete

Mark 1.00 out of 1.00

Flag question

Which of the following best describes Stored XSS?

☐ a. A script is embedded in a URL and executed when the victim clicks the link

☐ b. XSS that only works on outdated browsers

☒ c. The malicious script is stored in the database and executed when loaded by a user

☐ d. A script is executed immediately when injected

Question 2

Complete

Mark 1.00 out of 1.00

Flag question

What is the most common way to fix XSS vulnerabilities?

☐ a. Allowing only admin users to enter scripts

☒ b. Using DOMPurify to sanitize user input

☐ c. Storing scripts in the database

☐ d. Using JavaScript's eval() function

Question 3

Complete

Mark 1.00 out of 1.00

Flag question

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

☐ a. Allow script execution inside innerHTML

☒ b. Sanitize user input using DOMPurify or server-side escaping

☐ c. Use inline JavaScript to filter malicious code

☐ d. Use dangerouslySetInnerHTML without sanitization

Question 4

Complete

Mark 1.00 out of 1.00

Flag question

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

☐ a. Increases query execution speed

☐ b. Adds an additional condition to the query

☐ c. Encrypts user input

☒ d. Comments out the rest of the SQL query

Question 5

Complete

Mark 1.00 out of 1.00

Flag question

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

☐ a. `<script>alert("XSS")</script>`

☐ b. `<img src=x onerror=alert("XSS")>`

☒ c. All of the above

☐ d. `<iframe src=javascript:alert("XSS")>`

Question 6

Complete

Mark 1.00 out of 1.00

Flag question

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

☐ a. `SELECT * FROM users WHERE username = ? AND password = ?;`

☐ 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 = "" + user_input + "" AND password = "" + pass_input + "";`

Question 7

Complete

Mark 1.00 out of 1.00

Flag question

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

☒ a. By using DOMPurify to sanitize both input and output

☐ b. By encoding all data before storing it

☐ c. By only allowing administrators to post comments

☐ d. By blocking all comments containing `<script>`

Question 8

Complete

Mark 1.00 out of 1.00

Flag question

What is the main difference between SQL Injection and XSS?

☐ a. Both are prevented using the same techniques

☒ b. SQL Injection targets databases, while XSS targets browsers

☐ c. XSS can modify SQL databases

☐ d. SQL Injection is always more dangerous than XSS

**Question 9**

Complete

Mark 1.00 out of 1.00

Flag question

What additional security measures can prevent XSS attacks?

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

**Question 10**

Complete

Mark 1.00 out of 1.00

Flag question

What does the dangerouslySetInnerHTML property in React do?

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

**Question 11**

Complete

Mark 1.00 out of 1.00

Flag question

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

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

**Question 12**

Complete

Mark 1.00 out of 1.00

Flag question

What is SQL Injection?

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

**Question 13**

Complete

Mark 1.00 out of 1.00

Flag question

Why does this React component not execute XSS payloads?

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

**Question 14**

Complete

Mark 1.00 out of 1.00

Flag question

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

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

**Question 15**

Complete

Mark 1.00 out of 1.00

Flag question

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

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