

3.5 Full-stack data flow and security

Name: _____ Class: _____ Date: _____ **Total: 12 marks**

KEY WORDS JSON JSON • parameterised query 参数化查询 • SQL injection SQL 注入
• database 数据库

Objective

Explain secure data flow from browser to server, database, and JSON response.

You must be able to:

- trace request-response data flow
- explain parameterised queries
- identify a SQL-injection risk

1 Worked examples

■ Keep values separate from SQL

The browser requests data. The server validates the request, uses a **parameterised query** 参数化查询, and returns rows as JSON.

Parameters keep a value separate from SQL text. Never build SQL by joining a user's input into a query string, because that can allow **injection** 注入.

2 Practice

2.1 State the format commonly returned by an API to the browser. [1]

2.2 State why a parameterised query is safer than joining a user value into SQL text. [1]

2.3 Explain the server's role between a browser request and database query. [2]

3 Exam-style questions

3.1 Explain how a parameterised query protects a search endpoint from SQL injection. [4]

3.2 Describe the main steps when a browser requests a student's course list. [4]

Solutions

2.1

- JSON.

2.2

- The value is sent separately from the SQL text.

2.3

- It validates the request and controls the database query.
- It returns an appropriate response to the browser.

3.1

- The SQL structure is fixed by the server.
- User input is supplied as a separate parameter.
- It cannot become part of the SQL command.
- The endpoint can safely search for the requested value.

3.2

- The browser sends a request to a server route.
- The server authenticates and validates the request.
- It runs a parameterised database query.
- It returns the permitted course rows as JSON.