Exercise walk-through

3.5
Connecting JavaScript with SQL

GAC Computing

You must be able to

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

1 The method

Method — 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

Practice 2.1 ▪ 1 mark

State the format commonly returned by an API to the browser.

Solution 2.1

Worked steps

- JSON. B1

Practice 2.2 ▪ 1 mark

State why a parameterised query is safer than joining a user value into SQL text.

Solution 2.2

Method: Keep values separate from SQL — p.4

Worked steps

- The value is sent separately from the SQL text. B1

Practice 2.3 ▪ 2 marks

Explain the server's role between a browser request and database query.

Solution 2.3

Method: Keep values separate from SQL — p.4

Worked steps

- It validates the request and controls the database query. B1
- It returns an appropriate response to the browser. A1

3 Exam-style

Exam-style 3.1 ▪ 4 marks

Explain how a parameterised query protects a search endpoint from SQL injection.

Solution 3.1

Method: Keep values separate from SQL — p.4

Worked steps

- The SQL structure is fixed by the server. B1
- User input is supplied as a separate parameter. A1
- It cannot become part of the SQL command. A1
- The endpoint can safely search for the requested value. B1

Exam-style 3.2 ▪ 4 marks

Describe the main steps when a browser requests a student's course list.

Solution 3.2

Method: Keep values separate from SQL — p.4

Worked steps

- The browser sends a request to a server route. **B1**
- The server authenticates and validates the request. **A1**
- It runs a parameterised database query. **A1**
- It returns the permitted course rows as JSON. **B1**