

Exercise walk-through

3.1

JavaScript for Web App's back-end

GAC Computing

You must be able to

- distinguish front end from back end
- describe a request and response
- decide which information and rules must stay on the server

1

The method

Method — Keep secrets off the page

The **front end** 前端 runs in the visitor's browser. The **back end** 后端 runs on a server controlled by the organisation. A browser sends a **request** 请求; the server returns a **response** 响应.

An API key, password, and database connection belong on the back end. Browser code is visible to every visitor. A rule such as “only enrolled students may download this file” must be enforced on the server.

2

Practice

Practice 2.1 ■ 1 mark

State where front-end code runs.

Solution 2.1

Method: Keep secrets off the page — p.4

Worked steps

- In the visitor's browser. **B1**

Practice 2.2 ■ 1 mark

State what a server returns after receiving a request.

Solution 2.2

Method: Keep secrets off the page — p.4

Worked steps

- A response. **B1**

Practice 2.3 ■ 2 marks

Explain why an API key must not be placed in browser JavaScript.

Solution 2.3

Method: Keep secrets off the page — p.4

Worked steps

- Browser code can be read by every visitor. **B1**
- The key could be copied and misused. **A1**

3

Exam-style

Exam-style 3.1 ■ 4 marks

A course site checks in JavaScript whether a user is enrolled before showing a PDF link. Explain why this is not enough to protect the PDF.

Solution 3.1

Worked steps

- A visitor can bypass or change browser-side JavaScript. **B1**
- They may find the PDF URL directly. **A1**
- The check is only a convenience, not enforced protection. **A1**
- The server must check enrolment before sending the file. **B1**

Exam-style 3.2 ■ 4 marks

Recommend a secure request-response process for downloading the PDF.

Solution 3.2

Method: Keep secrets off the page — p.4

Worked steps

- The browser requests the PDF from a back-end route. **B1**
- The server checks the user's authenticated enrolment. **A1**
- If permitted, it returns the PDF response; otherwise it rejects the request. **A1**
- The secret data and enforced rule remain on the server. **B1**