Exercise walk-through

Protecting Applications ▪ 5.5

eXercise

You must be able to

- explain secure by design and secure by default
- explain how input sanitization removes dangerous control characters
- state that sanitization blocks SQL injection, XSS, and directory traversal

Method — Design principles

Secure by design builds security into every development phase. Secure by default ships products with security features already enabled - safe out of the box, since most users never change defaults.

Method — Input sanitization

Sanitization removes or rejects dangerous control characters (single quote, double quote, semicolon) before processing input, blocking SQL injection, XSS, and directory-traversal attacks in one stroke.

Practice 2.1 ▪ 2 marks

Explain what ‘secure by default’ means.

Solution 2.1

Method: Design principles

Worked steps

a product ships with its security features already enabled B1, so it is safe out of the box without the user changing settings B1.

Practice 2.2 ▪ 3 marks

Name three attacks that input sanitization defends against.

Solution 2.2

Method: Input sanitization

Worked steps

SQL injection B1; XSS B1; directory traversal B1.

Practice 2.3 ▪ 2 marks

Which characters does input sanitization typically remove or reject?

Solution 2.3

Method: Input sanitization

Worked steps

control characters B1 such as the single quote, double quote, and semicolon B1.

Exam-style 3.1 ▪ 1 mark

Which single defense blocks SQL injection, XSS, AND directory traversal?

A a stronger password

B input sanitization

C a bigger monitor

D a UPS

Solution 3.1

Method: Input sanitization

A a stronger password

B input sanitization ✓

C a bigger monitor

D a UPS

Worked steps

B. input sanitization stops all three input attacks.

Exam-style 3.2 ▪ 1 mark

‘Secure by design’ means security is

A added at the very end

B built into every phase of development

C the user’s job only

D unnecessary

Solution 3.2

Method: Design principles

A added at the very end

B built into every phase of development ✓

C the user's job only

D unnecessary

Worked steps

B. security is a design principle throughout development.

Exam-style 3.3 ▪ 1 mark

A web form passes user input straight into a database query.
(a) State the risk this creates.
(b) Explain how input sanitization removes the risk.

Solution 3.3

Method: Input sanitization

Worked steps

(a) SQL injection B1. (b) sanitization strips dangerous control characters from the input B1 so they cannot alter the database query B1.