AP CYBERSECURITY • EXERCISE SHEET

# 5.5 Protecting Applications

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

**KEY WORDS** input sanitization 输入清理 • secure by design 安全设计 • secure by default 默认安全 • sql injection SQL 注入 • directory traversal 目录遍历

## Objective

Build the skills to answer exam questions on **secure by design** 安全设计 and **input sanitization** 输入清理.

**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

## 1 Worked examples

Study these first. Each one shows the method for a task used later.

### ■ 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.

### ■ 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.

## 2 Practice

**2.1** Explain what 'secure by default' means. [2]



**2.2** Name three attacks that input sanitization defends against. [3]

**2.3** Which characters does input sanitization typically remove or reject? [2]

## 3 Exam-style questions

**3.1** Which single defense blocks SQL injection, XSS, AND directory traversal? [1]

- **A** a stronger password
- **B** input sanitization
- **C** a bigger monitor
- **D** a UPS

**3.2** 'Secure by design' means security is [1]

- **A** added at the very end
- **B** built into every phase of development
- **C** the user's job only
- **D** unnecessary

**3.3** A web form passes user input straight into a database query.

(a) State the risk this creates. [1]

(b) Explain how input sanitization removes the risk. [2]

## Solutions

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

**2.2** SQL injection; XSS; directory traversal.

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

**3.1 B**. input sanitization stops all three input attacks.

**3.2 B**. security is a design principle throughout development.

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