**Week 23**

# AP Cybersecurity

Homework bundle for this week

本周作业合集

exercises.lol

## Contents 目录


**Topic 5 quiz** . . . . . 2

**Exercise sheet 5.1** . . . . . 5

**Past-paper questions 5.1** . . . . . 8

**Exercise sheet 5.2** . . . . . 9

**Past-paper questions 5.2** . . . . . 12

**Exercise sheet 5.3** . . . . . 13

**Exercise sheet 5.4** . . . . . 16

**Exercise sheet 5.5** . . . . . 19

**Past-paper questions 5.5** . . . . . 22

**Exercise sheet 5.6** . . . . . 23

**Past-paper questions 5.6** . . . . . 27

# 5. Securing Applications and Data

**Starter Quiz · 课前小测**

AP Cybersecurity Name: _____ Score: _____

1. Typing ' OR '1'='1 into a login field is a...
   - ☐ buffer overflow
   - ☐ SQL injection
   - ☐ XSS attack
   - ☐ directory traversal
2. "Allow access only during business hours" describes which model?
   - ☐ RBAC
   - ☐ RuBAC
   - ☐ DAC
   - ☐ MAC
3. Symmetric encryption uses...
   - ☐ two different keys
   - ☐ the same key to encrypt and decrypt
   - ☐ no key
   - ☐ a public key only
4. To send Bob an encrypted message, you use...
   - ☐ Bob's public key
   - ☐ Bob's private key
   - ☐ your private key
   - ☐ no key
5. "Secure by default" means a product ships with...
   - ☐ all security features off
   - ☐ security features already enabled
   - ☐ no security at all
   - ☐ a free gift
6. What single number sets owner read+write, group read, others none? (chmod ____)

   _____

7. Data validation checks that user input meets expected rules before processing.

   ☐ True ☐ False

8. The principle of least privilege gives each entity exactly the access it needs, no more.

   ☐ True ☐ False

9. A larger keyspace makes an encryption key harder to guess.

   ☐ True ☐ False

10. The private key must be kept secret and never shared.

    ☐ True ☐ False

AP Cybersecurity

1. **SQL injection**

   SQL control characters in input = **SQL injection**.

2. **RuBAC**

   A **condition** (time) = **RuBAC**.

3. **the same key to encrypt and decrypt**

   **Symmetric** = one shared key.

4. **Bob's public key**

   Encrypt with the **recipient's public key**.

5. **security features already enabled**

   **Secure by default** = safe out of the box.

6. **640**

   6 (4+2), 4, 0 → **640**.

7. **True**

   **Data validation** is the core defense.

8. **True**

   **Least privilege** limits access to what is needed.

9. **True**

   More possible keys = more guessing time.

10. **True**

    Security rests on the **private key** staying secret.

AP CYBERSECURITY • EXERCISE SHEET

# 5.1 Application and Data Vulnerabilities and Attacks

Name: _____ Class: _____ Date: _____ **Total: 10 marks**

**KEY WORDS** directory traversal 目录遍历 • sql injection 数据库注入 • buffer 缓冲区 • buffer overflow 缓冲区溢出 • data validation 数据验证

## Objective

Build the skills to answer exam questions on application attacks such as **SQL injection** 数据库注入 and **directory traversal** 目录遍历.

**You must be able to:**

- identify an application attack from log evidence
- explain how unchecked user input enables injection attacks
- name **data validation** 数据验证 as the core defense

## 1 Worked examples

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

### ■ Reading the evidence

SQL injection shows OR 1=1 and – in a query. XSS shows a <script> tag. Directory traversal shows ../ in a URL. A buffer overflow shows an unusually long input string.

### ■ The common cause

Every one of these attacks exploits unchecked user input. Data validation - checking input meets expected rules before processing - is the core defense.

## 2 Practice

**2.1** A login field receives the input ' OR '1'='1. Name the attack. [1]

**2.2** Explain how a **directory traversal** attack works. [2]

**2.3** A web application does not check what users type into its input fields.

(a) State the general name for the resulting class of attack. [1]

(b) Name the defense that would prevent it. [1]

## 3 Exam-style questions

**3.1** A URL request for ../../../etc/passwd is a [1]

- **A** SQL injection
- **B** XSS attack
- **C** directory traversal attack
- **D** smurf attack

**3.2** Sending far more data than a memory buffer can hold is a [1]

- **A** buffer overflow
- **B** cross-site scripting
- **C** SQL injection
- **D** directory traversal

**3.3** A bank's log shows an input string containing ' OR '1'='1' – in its loan form.

(a) Name the attack. [1]

(b) Explain what the attacker is trying to do. [2]

## Solutions

**2.1** SQL injection.

**2.2** the attacker puts ../ sequences in a URL to climb out of the intended folder and reach sensitive files.

**2.3** (a) injection attacks. (b) data validation / input sanitization.

**3.1 C**. ../ climbing folders is directory traversal.

**3.2 A**. overflowing a buffer into nearby memory is a buffer overflow.

**3.3** (a) SQL injection. (b) inject control characters into the database query to make it return or change data it should not.

18. Which of the following types of attacks occurred when the adversary submitted a string that included `' OR '1'='1';--`?
    (A) SQL injection attack
    (B) Buffer overflow attack
    (C) Cross site scripting attack
    (D) Directory traversal attack

19. Which of the following security controls would most likely prevent an attack like this in the future?
    (A) Encryption
    (B) Stateful firewall
    (C) Input sanitization
    (D) Access control list

20. Which of the following best explains how the adversary attempted to manipulate the bank's customer database through the online loan application form?
    (A) When user input is fed into a server's file system, HTTP requests can access sensitive data.
    (B) When user input contains executable scripts, those scripts can run in the user's browser and access sensitive data.
    (C) When user input exceeds the size of the designated memory, it can allow the adversary to access, modify, and delete files.
    (D) When user input from a web form is fed directly into a database query, an adversary can inject control characters that can allow an adversary to view or modify the contents of a database.

AP CYBERSECURITY • EXERCISE SHEET

# 5.2 Protecting Applications and Data: Managerial Controls and Access Controls

Name: _____ Class: _____ Date: _____ **Total: 9 marks**

**KEY WORDS** access control models 访问控制模型 • principle of least privilege 最小权限原则

## Objective

Build the skills to answer exam questions on **access control models** 访问控制模型 and **Linux permissions** Linux 权限.

**You must be able to:**

- choose the right access model (RBAC, RuBAC, DAC, MAC) from a scenario
- read and write Linux permissions using read 4 / write 2 / execute 1
- apply the **principle of least privilege** 最小权限原则

## 1 Worked examples

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

### ■ Choosing the model

RBAC follows your role; RuBAC follows a condition (like time); DAC lets the owner decide; MAC uses central levels. Match the scenario's decider to the model.

### ■ Linux permissions

Each group's number adds read (4) + write (2) + execute (1). chmod 640 = owner read+write (6), group read (4), others none (0).

## 2 Practice

**2.1** "Access allowed only during business hours" - name the access-control model. [1]

**2.2** Write the chmod number that gives the owner read+write, the group read, and others nothing. [2]

**2.3** A file needs: owner read+write+execute, group read+execute, others none.

(a) Write the chmod number. [1]

(b) State what the ’7’ means. [1]

## 3 Exam-style questions

**3.1** “Every user with the role ‘nurse’ can open patient charts” describes [1]

- **A** RuBAC
- **B** RBAC
- **C** DAC
- **D** MAC

**3.2** The permission string -rw-r—— corresponds to which chmod number? [1]

- **A** chmod 444
- **B** chmod 640
- **C** chmod 740
- **D** chmod 777

**3.3** An administrator applies the principle of least privilege.

(a) State what least privilege means. [1]

(b) Explain one security benefit. [1]

## Solutions

**2.1** RuBAC / rule-based access control.

**2.2** 640: owner 6 = 4+2, group 4, others 0.

**2.3** (a) 750. (b) 7 = 4+2+1 = read + write + execute.

**3.1 B**. access follows the role, so RBAC.

**3.2 B**. owner rw = 6, group r = 4, others none = 0 → 640.

**3.3** (a) each entity gets exactly the access it needs and no more. (b) if an account is compromised, the damage is limited to that minimal access.

2. A school district wants to ensure that only the school principal (**`kmurray`**) can edit faculty evaluation reports and to limit permissions for everyone else. The district's system administrator wants to set the following permission for the file **`Oak_Park_HS`**, which contains the faculty evaluations.

```
-rw-r----- kmurray staff 2048 Sep 18 10:45 Oak_Park_HS
```

Which of the following commands can be used to set the permissions shown?

(A) `chmod 444 Oak_Park_HS`

(B) `chmod 640 Oak_Park_HS`

(C) `chmod 740 Oak_Park_HS`

(D) `chmod 777 Oak_Park_HS`

3. Consider the following email.

**From: Management**
**To: Security Manager**

---

**Subject: New Access Rules for Transaction System**

Thank you for implementing access restrictions on our internal applications.

We are now interested in applying additional security rules that automatically limit user access based on specific conditions. For example, access to the transaction system should only be allowed during business hours and from devices connected to the corporate network.

Thanks!

Which of the following access control models best meets the request in the email?

(A) DAC

(B) MAC

(C) RBAC

(D) RuBAC

AP CYBERSECURITY • EXERCISE SHEET

# 5.3 Protecting Stored Data with Cryptography

Name: _____ Class: _____ Date: _____ **Total: 9 marks**

**KEY WORDS** symmetric encryption 对称加密 • keyspace 密钥空间 • aes 高级加密标准 • ciphertext 密文 • block cipher 分组密码

## Objective

Build the skills to answer exam questions on **symmetric encryption** 对称加密, keys, and **keyspace** 密钥空间.

**You must be able to:**

- define plaintext, ciphertext, key, and keyspace
- explain that symmetric encryption uses one shared key (e.g. **AES** 高级加密标准)
- relate key length to keyspace size ($2^n$)

## 1 Worked examples

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

### ■ The vocabulary

Encryption combines plaintext with a key to make ciphertext; decryption reverses it. The keyspace is the number of possible keys; an n-bit key has $2^n$ of them.

### ■ Symmetric encryption

Symmetric encryption uses the same key to encrypt and decrypt. AES is the standard block cipher. The challenge is sharing the single secret key safely.

## 2 Practice

**2.1** Define **ciphertext**. [1]

**2.2** Explain what 'symmetric' means in symmetric encryption. [2]

**2.3** How many possible keys does a 4-bit key have? [1]

## 3 Exam-style questions

**3.1** The standard modern symmetric block cipher is [1]

- **A** RSA
- **B** AES
- **C** HTTP
- **D** MAC

**3.2** A larger keyspace makes an encryption key [1]

- **A** easier to guess
- **B** harder to guess
- **C** shorter
- **D** unnecessary

**3.3** A company encrypts stored files with a symmetric algorithm.

(a) State the main practical challenge of symmetric encryption. [1]

(b) Explain why longer keys are more secure but slower. [2]

## Solutions

**2.1** the scrambled output of an encryption algorithm.

**2.2** the same key is used to encrypt and to decrypt; both parties must share that secret key.

**2.3** $2^4 = 16$.

**3.1 B**. AES is the symmetric standard.

**3.2 B**. more possible keys means more guessing time.

**3.3** (a) sharing the single secret key safely. (b) a longer key has a larger keyspace so it is harder to guess, but it takes more time to encrypt and decrypt.

AP CYBERSECURITY • EXERCISE SHEET

# 5.4 Asymmetric Cryptography

Name: _____ Class: _____ Date: _____ **Total: 9 marks**

**KEY WORDS** private key 私钥 • public key 公钥 • asymmetric encryption 非对称加密 • key pair 密钥对 • key 密钥

## Objective

Build the skills to answer exam questions on **asymmetric encryption** 非对称加密 and public/private key pairs.

**You must be able to:**

- explain the roles of a **public key** 公钥 and a **private key** 私钥
- say which key encrypts and which decrypts when sending a secret
- state that asymmetric encryption solves the key-sharing problem

## 1 Worked examples

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

### ■ The key pair

A key pair has a public key (shared with everyone) and a private key (kept secret). They are mathematical inverses: what one locks, only the other unlocks.

### ■ Sending a secret

To send Bob a secret, encrypt with Bob's public key. Only Bob's private key can decrypt it - so no shared secret ever had to be exchanged in advance.

## 2 Practice

**2.1** State which key you use to encrypt a message you are sending to someone. [1]

**2.2** Explain why the private key must be kept secret. [2]

**2.3** State the main advantage of asymmetric over symmetric encryption. [1]

## 3 Exam-style questions

**3.1** To send Bob an encrypted message, you use [1]

- **A** Bob's public key
- **B** Bob's private key
- **C** your private key
- **D** no key

**3.2** Which is an asymmetric encryption algorithm? [1]

- **A** AES
- **B** RSA
- **C** WPA3
- **D** SHA-256

**3.3** Alice wants to send Bob a confidential file over the internet.

(a) State which key Alice uses to encrypt it. [1]

(b) Explain why only Bob can read the file. [2]

## Solutions

**2.1** the recipient's public key.

**2.2** the private key is the only key that can decrypt messages sent to its owner; if it leaks, an adversary can read those messages.

**2.3** it solves the key-sharing problem - no shared secret must be exchanged first.

**3.1 A**. encrypt with the recipient's public key.

**3.2 B**. RSA is asymmetric; AES is symmetric.

**3.3** (a) Bob's public key. (b) only Bob's matching private key can decrypt it, and Bob keeps that private key secret.

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.

18. Which of the following types of attacks occurred when the adversary submitted a string that included `' OR '1'='1';--`?
    (A) SQL injection attack
    (B) Buffer overflow attack
    (C) Cross site scripting attack
    (D) Directory traversal attack

19. Which of the following security controls would most likely prevent an attack like this in the future?
    (A) Encryption
    (B) Stateful firewall
    (C) Input sanitization
    (D) Access control list

AP CYBERSECURITY • EXERCISE SHEET

# 5.6 Detecting Attacks on Data and Applications

Name: _____ Class: _____ Date: _____ **Total: 11 marks**

**KEY WORDS** honeypot 蜜罐 • accounting 审计记录 • sql injection SQL 注入 • directory traversal 目录遍历 • cross-site scripting (xss) 跨站脚本

## Objective

Build the skills to answer exam questions on detecting data attacks with **honeypots** 蜜罐 and log analysis.

**You must be able to:**

- describe accounting, honeypots, and hash checks as detective controls
- read application logs to identify SQL injection, XSS, and traversal
- weigh cost against sensitivity when choosing detection

## 1 Worked examples

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

### ■ The honeypot

A honeypot is a fake valuable file. Because no one has a legitimate reason to open it, any access is an unambiguous alarm - but it only catches an attacker who tries to open it.

### ■ Reading log signatures

SQL injection shows OR 1=1 and –. XSS shows <script> tags. Directory traversal shows ../. A buffer overflow shows very long input strings.

## 2 Practice

**2.1** Explain how a **honeypot** detects an attacker. [2]

**2.2** How can a cryptographic hash reveal that a file was altered? [2]

**2.3** Match each log signature to its attack.

(a) OR 1=1 and – [1]

(b) a <script> tag [1]

(c) ../ in a request path [1]

## 3 Exam-style questions

**3.1** A fake valuable file whose access signals an attack is a [1]

- **A** firewall
- **B** honeypot
- **C** baseline
- **D** patch

**3.2** Seeing <script> tags in user input in the logs indicates [1]

- **A** SQL injection
- **B** cross-site scripting (XSS)
- **C** directory traversal
- **D** a smurf attack

**3.3** A company wants cheap detection for tampering with sensitive files.

(a) Name one low-cost detective control. [1]

(b) Explain one limitation of a honeypot. [1]

## Solutions

**2.1** it is a fake valuable file no one should open, so any access is a clear sign of malicious activity.

**2.2** re-hash the file and compare to the recorded hash; if the hash changed, the file changed.

**2.3** (a) SQL injection. (b) XSS. (c) directory traversal.

**3.1 B**. a honeypot has no legitimate reason to be opened.

**3.2 B**. an injected <script> tag is the XSS signature.

**3.3** (a) a honeypot or a cryptographic hash check. (b) a honeypot only catches an attacker who actually tries to open it.

9. How does the email's claim that "Over 92% of employees have already completed the verification" attempt to pressure the recipient into responding to the email?
   (A) By framing the request as routine HR communication that seems safe, showing the use of familiarity
   (B) By implying that the opportunity to comply is limited and may soon be lost, showing the use of scarcity
   (C) By presenting the request as coming from those in power and intimidating the recipient, showing the use of authority
   (D) By applying social pressure and making the recipient believe most coworkers have already acted, showing the use of consensus

10. Which of the following is the most likely impact if the recipient responds to this email with the requested information?
   (A) An adversary could use the recipient's personal details to impersonate them.
   (B) An adversary could use the recipient's device as a foothold and move laterally on the network compromising other devices.
   (C) An adversary could infect the recipient's device with malicious code hidden in the reply email.
   (D) An adversary could disrupt the entire payroll system by disabling access for all employees.

11. A natural gas company's help desk receives reports from employees that the company's website is intermittently crashing when they try to log in. The cybersecurity analyst reviews the server's access logs and finds the following entries.

```
[22/Oct/2025:10:11:02] "GET /index.html HTTP/1.1" 200 4521
[22/Oct/2025:10:11:07] "GET /about.html HTTP/1.1" 200 3890
[22/Oct/2025:10:11:10] "GET ../../../../etc/passwd HTTP/1.1" 403 721
[22/Oct/2025:10:11:12] "GET ../../../../etc/shadow HTTP/1.1" 403 654
```

   Which of the following application attacks is indicated in the log file?
   (A) Buffer overflow attack
   (B) Cross site scripting attack
   (C) Directory traversal attack
   (D) SQL injection attack

18. Which of the following types of attacks occurred when the adversary submitted a string that included `' OR '1'='1';--`?
   (A) SQL injection attack
   (B) Buffer overflow attack
   (C) Cross site scripting attack
   (D) Directory traversal attack