5 Application attacks and access control – Part 1

Name: _____ Class: _____ Date: _____

Vocabulary 词汇

Write each word three times. 把每个单词抄写三遍。

English	**中文**	**Write it 3 times** (English)		
SQL injection	数据库注入			
directory traversal	目录遍历			
Data validation	数据验证			
RBAC	基于角色的访问控制			
RuBAC	基于规则的访问控制			
DAC	自主访问控制			
MAC	强制访问控制			
least privilege	最小权限			

Recall

- You have typed into search boxes and login forms on websites.
- You know some files are private and some are shared.
- You understand that only certain people should edit certain things.

New ideas

Read these first. Each idea has a short worked example. Then do the Practice below.

1 Application attacks

Unchecked user input is the danger. **SQL injection** 数据库注入 puts commands into a form to read a database; **directory traversal** 目录遍历 uses `../` to reach other files. **Data validation** 数据验证 is the defence.

Worked example. Typing `' OR '1'='1` into a login makes the query always true - SQL injection.

2 Access control models

RBAC 基于角色的访问控制 follows your role; **RuBAC** 基于规则的访问控制 follows a condition (like time); **DAC** 自主访问控制 lets the owner decide; **MAC** 强制访问控制 uses central levels.

Worked example. "Only during business hours" is a condition, so it is RuBAC.

3 Linux permissions

Each file gives **read (4), write (2), execute (1)** to the owner, group, and others. `chmod 640` = owner read+write (6), group read (4), others none (0). Follow **least privilege** 最小权限.

Worked example. Owner rwx, group r-x, others none = 7,5,0 = chmod 750.

Watch out: Do not gloss over the direction of `../` - it climbs UP folders. Three of them reach the root of the file system.

Practice

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

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

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

2.4 Write the chmod number for owner read+write, group read, others none. [2]

2.5 State what the principle of least privilege means. [2]