COM-402 exercises 2024, session 4: Data Security

Exercise 4.1

Your application uses an SQL database which stores the names, grades and year of graduation of students.

- What mechanism can you apply to allow user Alice to only read data of students that graduate in 2026?

Exercise 4.2

Consider an application that contains medical data. For more security, it uses two different tables: one with the personal data of patients and the other one with their medical conditions. Three database users are defined:

1. a user that can only read and write the personal data table
2. a user that can read the personal data and the medical data
3. a user that can read and write the medical data

The first user is used when patients update there personal data. The second user is used when the patients want to see their medical information. Finally, the third user is used when a doctor logs in to update the medical data.

- Which part of the application would have to be vulnerable to SQL injections, to allow a patient to read the medical information of another patient?
- What is a typical way of preventing an SQL injection?

Exercise 4.3

- Why is transparent data encryption (the DB encrypts before writing to files) better than an encrypted file system (the OS encrypts the content of the files)?

Exercise 4.4

- Give two reasons why it is important to salt password hashes.

Exercise 4.5

You just built a very nice rainbow table that can crack 99% of 8 letter passwords. Compared to a brute-force attack, it uses 1,000 times less hash operations to find a password.

You are given a list of ten thousand hashes that need to be cracked.

- Is it going to be faster to crack the passwords with the rainbow table or with a classical brute-force attack?

Exercise 4.6

- Why calculating a Windows password hash (based on MD4) is about 200,000 times faster than calculating a Linux password hash based on SHA512?

Exercise 4.7

- Why is a graphics card that can calculate 10,000 hashes in parallel, not efficient for cracking password hashes like Argon or Scrypt?