1

Questions

1. Why might an attacker use time-based techniques in SQL injections for database security testing?

A. It generally speeds up transaction processing within databases.
B. It can indicate the presence of vulnerabilities for attackers to exploit.
C. It ensures that SQL code executes without errors.
D. It assists in legal auditing processes of database systems.

2. What is a crucial technique to prevent SQL injection attacks?

A. Enabling indexed search across databases.
B. Forcing strict query plan execution strategies.
C. Implementing parameterized queries to prevent SQL injection.
D. Coding with high-performance execution routines.

3. How can databases defend against time-based SQL injection attacks?

A. Implementing zero trust architecture in network access.
B. Through regular backups to maintain data integrity.
C. By encrypting data stored in databases to protect visibility.
D. By ensuring all user inputs are validated against predefined criteria.