Tutorial 1 – Security Problems

Question 1 -

A university uses a database system to manage student records. Identify two possible vulnerabilities and suggest corresponding best practices to secure them.

Answer: Databases are prone to SQL injection and Data Tampering my incorrect access control.

Question 2

Explain how poor application design can compromise database security and suggest two ways to improve it.

Answer: poor application design such as unvalidated input boxes can lead to vulnerability such as SQL injection. These can be avoided by implementing sanitation to code and do regular code review to check for unvalidated input boxes.

Question 3

You are working in an organization where users often forget to log out of their database sessions on shared terminals.  
a) Identify the security threat in this scenario.  
b) Propose two solutions to mitigate the threat.

Answer: This can allow an attacker to use the current session and get data out of the database. We should implement timeout sessions for certain accounts.

Question 4

A small company is using default passwords and configurations on their database and web applications.  
a) Identify the type of vulnerability this presents.  
b) Suggest two best practices to eliminate this risk.

Answer: Having a default password is very prone to dictionary and brute force attacks making it easy for attackers to retrieve data and cause data leaks.

Question 5

An attacker gains access to a database server by exploiting a vulnerability in an outdated operating system.  
a) What type of security weakness was exploited?  
b) Recommend two actions to prevent such incidents.

Answer: Security patches is very important as it patches new vulnerability that the system might have that are prone to current attackers, hence we should run scheduled updates to make sure that those vulnerabilities are consistently patched.

Question 6  
A developer accidentally gives full access privileges to a low-level employee in a customer database system.  
a) What security issue is this an example of?  
b) How can it be prevented in the future?

Answer: a) Poor Access control

b) By having a strict access control list , and relevant SOP in place for what level of employee having what kind of access

Question 7  
During a power outage, a database server shuts down improperly, resulting in partial data loss.  
a) What risk does this situation illustrate?  
b) Provide two recommendations to avoid such loss in future.

Answer: a) The risk illustrated is avoidable risk by having proper mitigation tactics in place

b) Since the integrity of data is lost during the power outage, we can add UPS uninterrupted power supplies from the power source to the servers to give us enough time to shutdown or run the servers during the power outage. We can also use RAID architecture for our servers to prevent data lost during physical failure.

Question 8  
An internal employee tries to steal customer data using authorized access.  
a) What kind of threat does this represent?  
b) Suggest two mitigation strategies.

1. Answer: Implement monitoring and auditing tools to track access and changes to sensitive data.
2. Apply role-based access controls (RBAC) and conduct regular access reviews to ensure employees only have necessary permissions.