Sensitive Data Exposure Vulnerabilities

Sensitive Data Exposure

- Sensitive data exposure vulnerabilities refer to security flaws in a system that lead to the unintended exposure of confidential or sensitive information.

- These vulnerabilities can have serious consequences, including data breaches, privacy violations, and financial losses.

Sensitive Data Exposure Examples

- Weak Password Storage: Storing passwords in plaintext or using weak hashing algorithms without salting, making it easier for attackers to retrieve user passwords from a compromised database.
- Information Disclosure in Error Messages: Revealing sensitive data, such as system paths, database details, or user credentials, in error messages or logs that could aid attackers in exploiting the system.
- Directory Traversal: Allowing users to manipulate file paths in requests to access files and directories outside their intended scope, potentially exposing sensitive files.
- Unencrypted Backups: Storing backups of sensitive data without encryption or proper access controls, making them vulnerable if they are stolen.

Demo: Sensitive Data Exposure Vulnerabilities