Goals of the Secure Design Process

- Identify the threats in sufficient enough detail for **developers** to understand and code accordingly to mitigate the associated risk
- Design the **architecture** in such a way that it mitigates as many threats as possible
- Enforce **secure design principles** that force developers to consider security while coding

Secure Design Principles

- Secure Design Principles are the **practices or guidelines** that should be enforced on the developers during the development phase
- They help in deriving **secure architectural decisions**

- They help to eliminate design and architecture **flaws** and mitigate common security vulnerabilities within the application

Notes:

Secure Design Principles (Cont'd)

A list of secure design principles to prevent common security vulnerabilities:

- Security through obscurity
- Secure the weakest link
- Use least privilege principle
- Secure by default
- Fail securely
- Apply defense in depth
- Do not trust user input
- Reduce attack surface
- Enable auditing and logging
- Keep security simple
- Maintain a separation of duties
- Correctly fix security issues
- Apply security in the design phase

- Protect sensitive data
- Exception handling
- Secure memory management
- Protect memory or storage secrets
- Fundamentals of control granularity
- Fault tolerance
- Fault detection
- Fault removal
- Fault avoidance
- Loose coupling
- High cohesion
- Change management and version control

Design Secure Application Architecture

1. A typical web application architecture comprises three tiers: **web**, **application**, and **database**
2. Security at one tier is not enough; an **attacker** can breach the security of another tier to compromise the application
3. Design web application architecture with a **defense-in-depth** principle, such as providing security at each tier of the web application
4. Multi-tiered security includes proper input validation, **database layer abstraction**, server configuration, proxies, web application firewalls, data encryption, OS hardening, and other items

Notes: