**OWASP (Open Web Application Security Project)**



**Broken Access Control**

Access control is act or policy for limiting user to do what they are allowed to do. (Providing keys for specific door)

Broken Access control is when legitimate user or attackers can subvert access control protection and access information they aren’t supposed to.

* Bypassing control checks
* Elevating their privileges beyond what they’re supposed to have
* Forcing access to restricted pages

**Cryptographic Failures**

Personal and sensitive data must be protected both in transit and at rest.

When cryptographic methods fail or aren’t properly implemented personal data maybe exposed this is known as cryptographic failure.

* Data being transmitted in clear text.
* Using old, weak or broken cryptographic methods
* Using default algorithms or protocols

**Injections**

Insert code into the system that makes the app run in unexpected manner. Giving the attacker greater level of access.

* It doesn’t filter or sanitize user supplied data
* It hasn’t gone through application security testing

**Insecure Design**

Focuses on risk related to design and architectural flaws. (Designed a building but forgot to add a roof and adding security feature like door lock won’t help)

* Looking at how exposed the application is going to be
* Analyzing expectations for how the application will be used
* Compiling technical requirements

**Security Misconfiguration**

If an application has a security feature that aren't correctly implemented or configured. (If a door has a strong lock but we don’t lock that door)

* Default account and password enabled
* Latest security features are disabled or not enabled correctly
* Having unnecessary feature or components

**Vulnerable & Outdated Components**

Many app consist of premade, third party or outdated components which introduce vulnerability to system.

* Use unsupported or out-of-date software regularly
* If software developers don’t test library compatibility
* If you don’t scan for vulnerabilities

**Identification & authentication failures**

When the application identification, authentication or session management features are not implemented correctly or sufficiently protected. (a door lock accepting from duplicate key)

* Permits brute-force or automated attacks
* Uses plaintext
* Encrypted or weakly hashed password data stores
* Permits weak passwords

**Software & Data Integrity**

Integrity means the completeness and accuracy of the data and the software.

* Use software from untrusted sources
* Fail to check components for known vulnerabilities
* Use application with insecure auto update functions

**Security Logging & Monitoring Failures**

*Insufficient logging and monitoring*

Intelligent monitor system that log events and potential security threats that way administrators can analysis attacks and defend against them.

* Not logging Failed login events.
* The application begins unable to detect or alert for active attacks in real time
* Logs being only stored locally

**Server-Side request forgery**

Application fetched remote resources without validating the URL user has given. This way an attacker can make an application reach out an unexpected and unsafe destination.