**What is Broken Access Control?**

**Broken Access Control happens when a system fails to properly enforce rules about what authenticated users are allowed to do.**
**In short, it means users can act outside their intended permissions.**

**Access Control is about who can do what in a system.**

**Example:**

**1. Regular users should not access admin pages.**

**2. A user should not be able to edit another user's profile.**

**When these protections are missing or improperly set up, you get Broken Access Control vulnerabilities.**

**Common Example**

**Vertical Privilege Escalation : A normal user becomes an admin by accessing a hidden admin panel.**
**Horizontal Privilege Escalation : A user accesses another user's private data**
**Forced Browsing : Guessing or manipulating URLs to access restricted resources**
**Insecure ID References : Exposing database IDs directly without validation, letting users manipulate them**

**Impact :**

**Data theft (personal info, business secrets)**

**Unauthorized account takeover**

**Unauthorized system control**

**How to Prevent It**

**Always check authorization server-side (never trust user input!).**
**Use role-based access controls (RBAC) or attribute-based access controls (ABAC) properly.**
**Avoid exposing internal object IDs directly (use random tokens instead).**
**Implement strong logging and monitoring for unusual access patterns.**

**Deny access by default and allow only specific permissions explicitly.**