**KEY TERMS:**

**1.Vulnerability:**

A bug in code or a flaw in software design that can be exploited to cause harm.

Exploitation may occur via an authenticated or unauthenticated attacker. A gap in security procedures or a weakness in internal controls that when exploited results in a security breach.

**2.URL manipulation:**

URL manipulation, also called URL rewriting, is the process of altering (often automatically by means of a program written for that purpose) the parameters in a URL (Uniform Resource Locator).

URL manipulation can be employed as a convenience by a Web server administrator, or for nefarious purposes by a hacker.

**3.SQL injection:**

SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

In general the way web applications construct SQL statements involving SQL syntax written by the programmers is mixed with user-supplied data.

**4.XSS:(Cross-site Scripting)**

Cross-site Scripting (XSS) happens whenever an application takes untrusted data and sends it to the client (browser) without validation.

This allows attackers to execute malicious scripts in the victim's browser which can result in user sessions hijack, defacing web sites or redirect the user to malicious sites.

**5.Cross-Site Request Forgery (CSRF):**

**Cross-Site Request Forgery** (CSRF) is an attack that forces an end user to execute unintended actions on a web application in which they are currently authenticated.

**6.Security Misconfiguration:**

Security misconfigurations are **security controls that are inaccurately configured or left insecure, putting your systems and data at risk**.

Basically, any poorly documented configuration changes, default settings, or a technical issue across any component in your endpoints could lead to a misconfiguration.