**Vulnerability**

* **Vulnerability**  is a process of evaluating security risks in software systems to reduce the probability of threats.
* The purpose of vulnerability testing is reducing the possibility for intruders/hackers to get unauthorized access of systems.

## Manipulating the URL

By manipulating parts of the URL, a hacker can gain access to web pages found on servers that they wouldn’t normally have access to.

Most users will visit a website and then use the links provided by the website. This will get them to where they need to go without much problem.

**SQL Injection**

SQL injection is a code injection technique that might destroy your database.

SQL injection is one of the most common web hacking techniques.

SQL injection is the placement of malicious code in SQL statements, via web page input.

**SQL in Web Pages**

SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will **unknowingly** run on your database.

**Cross-site scripting**

* **Cross-site scripting** attacks, also called XSS attacks, are a type of injection attack that injects malicious code into otherwise safe websites.
* The main purpose of this attack is to steal the other user’s identity data – cookies, session tokens, and other information. In most cases, this attack is being used to steal the other person‘s cookies. As we know, cookies help us to log in automatically. Therefore with stolen cookies, we can log in with the other identities. And this is one of the reasons, why this attack is considered one of the riskiest attacks.
* An XSS attack is being performed on the client-side. It can be performed with different client-side programming languages. However, most often this attack is performed with JavaScript and HTML.