**Vulnerability**

**URL Manipulation**

URL manipulation is the process of manipulating the website URL query strings & capture of the important information by hackers. This happens when the application uses the HTTP GET method to pass information between the client and the server. The information is passed in parameters in the query string. The tester can modify a parameter value in the query string to check if the server accepts it.

**SQL Injection**

SQL injection is the most common application layer attack technique used by hackers, in which malicious SQL statements are inserted into an entry field for execution. SQL injection attacks are very critical as an attacker can get critical information from the server database. It is a type of attack which takes the advantage of loopholes present in the implementation of web applications that allows a hacker to hack the system. To check the SQL injection we have to take care of input fields like text boxes, comments, etc. To prevent injections, special characters should be either properly handled or skipped from the input.

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 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.

**XSS**

Cross-site scripting is a [computer security vulnerability](https://en.wikipedia.org/wiki/Vulnerability_%28computer_science%29)found in web applications. XSS enables attackers to [inject client-side script](https://en.wikipedia.org/wiki/Client-side_script) into [Web pages](https://en.wikipedia.org/wiki/Web_page) viewed by other users and trick a user into clicking on that URL. Once executed by the other user’s browser, this code could then perform actions such as completely changing the behavior of the website, stealing personal data, or performing actions on behalf of the user.

Cross-site scripting attacks, also called XSS attacks, are a type of injection attack that injects malicious code into otherwise safe websites. An attacker will use a flaw in a target web application to send some kind of malicious code, most commonly client-side JavaScript, to an end user

XSS occurs when an attacker tricks a web application into sending data in a form that a user’s browser can execute. Most commonly, this is a combination of HTML and XSS provided by the attacker, but XSS can also be used to deliver malicious downloads, plugins, or media content.

**Key Concepts of XSS**

* XSS is a web-based attack performed on vulnerable web applications.
* In XSS attacks, the victim is the user and not the application.
* In XSS attacks, malicious content is delivered to users using JavaScript

TC for secrurity testing

