**Cross Site Scripting: -**

It is also known as XSS or CSS. It is one of the famous application layer based attack.

Generally CSS references to the hacking technique which leverages the vulnerabilities present in the code of a web application to allow an attacker to send malicious content from end-user and with the help of that collect some type of data from the victim.

A web page contains both the text and HTML mark ups that is generated by web servers and interpreted by client browsers. Web sites which generates static pages are able to have full control over how the browsers interprets these pages but the web sites which generates dynamic pages do not have complete control over how their outputs are interpreted by the client. So problem arises when mistrusted content can be introduced into a dynamic page. In such a scenario neither web server nor the client has enough information to recognize that this has happened and take protective actions.

With the help of CSS an attacker can embed malicious JAVA script, VB script, ActiveX, HTML or Flash into a vulnerable dynamic page, execute these scripts on target’s machine in order to get the data. The use of CSS might compromise private information, manipulate or steal cookies, create requests that can be mistaken for those of a valid user, or execute malicious code on the end-user system.

As a hacking tool, the attacker can formulate and distribute a custom crafted CSS URL just by using a browser to test the dynamic website response. The attacker must have the basic knowledge of HTML, Java Script and a dynamic language to generate a URL which is not suspicious looking in order to attack the CSS vulnerable web site.

Any web page which passes parameters to the database can be vulnerable to this attack. The best example of this is login forms and forgot password forms.

Generally in CSS attack the hacker infects the legitimate web page with his malicious client side script. When a user visit this infected web page the script is downloaded to his browser and executed.

**Is your site vulnerable to XSS:-**

To check if a website is vulnerable to CSS/XSS, it must be checked against all possible set of input where a user is supposed to post or submit his/her data in a forum, thread, discussion or in form of a message.

The other way is to scan the whole website by any website vulnerability scanner. Some of the popular website vulnerability scanners are acunetix, sqlmap, nikto, w3af etc. If the scanner reports any XSS vulnerability then proper actions should be taken according to the report generated by the scanner.

**How it can be stopped:-**

Appropriate validation of the provided input should be done i.e. the input should be filtered and converted into an acceptable form. For that some functions can be written in JavaScript and the server side scripting language that scans the input and excludes the unwanted tags, syntaxes and characters.

An example in PHP is as follows:-

$input = strip\_tags($\_POST[‘input’]);

Where **strip\_tags** is an inbuilt function in PHP library.