**Cross Site Scripting:**

Cross-site Scripting (also known as [XSS](http://www.acunetix.com/websitesecurity/xss) or CSS) is generally believed to be one of the most common application layer hacking techniques. “A web page contains both text and HTML markup that is generated by the server and interpreted by the client browser. Web sites that generate only static pages are able to have full control over how the browser interprets these pages. Web sites that generate dynamic pages do not have complete control over how their outputs are interpreted by the client. The heart of the issue is that if mistrusted content can be introduced into a dynamic page, neither the web site nor the client has enough information to recognize that this has happened and take protective actions.” (CERT Coordination Center).

Cross-site Scripting allows an attacker to embed malicious [JavaScript](http://www.acunetix.com/websitesecurity/javascript/), VBScript, ActiveX, HTML, or Flash into a vulnerable dynamic page to fool the user, executing the script on his machine in order to gather data. The use of XSS 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 systems. The data is usually formatted as a hyperlink containing malicious content and which is distributed over any possible means on the internet.

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 also needs to know some HTML, JavaScript and a dynamic language, to produce a URL which is not too suspicious-looking, in order to attack a XSS vulnerable website.

Any web page which passes parameters to a database can be vulnerable to this hacking technique. Usually these are present in Login forms, Forgot Password forms, etc…