**Abstract**

 Malicious code is a way of attempting to acquire sensitive information by sending malicious code to the trustworthy entity in an electronic communication. JavaScript is the most frequently used command language in the web page environment. If the hackers misuse the JavaScript code there is a possibility of stealing the authentication and confidential information about an organization and user. The attack is based on the malicious JavaScript code inserted into pages by intruders or hackers. Various attacks like redirect, script injection and XSS which usually include to transmitting private data to attacker or redirecting the victim to web content controlled by hacker. A cross-site scripting vulnerability allows the introduction of malicious content on a web site that is then served to users. Therefore filtering malicious JavaScript code is necessary for any web application. The aim of this work is to analyze different malicious code attacks phenomenon, various types of malicious code attacks. The experimental results obtained on XSS classification in web pages using Extreme Learning Machine techniques. ELM approach can be found in its high sparseness, it can also be seen that ELM accomplishes better and more balanced classification for individual categories as well in very less training time comparative to other classification algorithms. The data are collected from the real web pages and various features are extracted to classify the malicious web page using supervised learning algorithms and the results demonstrate that the proposed features lead to highly accurate classification of malicious page.