**Abstract**

 Malicious code injection poses a serious security issue over the Internet or over the Web application. In malicious code injection attacks, hackers can take advantage of defectively coded Web application software to initiate malicious code into the organization's systems and network. The vulnerability persevere when a Web application do not properly sanitize the data entered by the user on a Web page. Attacker can steal confidential data of the user like password, pin number, and etc., these attacks resulting defeat of market value of the organization. This research work is model the malicious Web page prediction as a classification task and provides a convenient solution by using a powerful machine learning technique such as Support Vector Machine (SVM), Extreme Learning Machine (ELM). The main aim of this research work is to predict the type of the malicious attack like Redirect, Script injection and XSS using the machine learning approaches; in this case, the prediction time is taken into consideration. The supervised learning algorithms such as SVM and ELM are employed for implementing the prediction model.