Abstract

Web applications are most widely used technique for providing an access to online services. At the same time web applications are easiest way for vulnerable acts. When a security mechanism is failed then the user may download malicious code from a trusted web site. In this case, the malicious script is contracted to full access with all assets belonging to that legitimate web site. These types of attacks are called Cross-Site Scripting (XSS) attacks. Cross Site Scripting (XSS) attacks are the most common type of attack against web application, which allows hackers to inject the malicious script code for stealing the user’s confidential information. Recent studies show that malicious code detection has become the most frequent vulnerability. In web browsers, the malicious script codes are executed and used to transfer the sensitive data to the third party (or hackers) domain. Currently, most research areas are attempted to prevent XSS on both the client and server side. In this paper, we present a machine learning technique to classify the malicious web pages. This work focus some of the possible ways to detect the XSS script on client side based on the features extracted from the web document content and the URL to scan the web pages for check the malicious scripts.

References
Multiclass Classification of XSS Web Page Attack using Machine Learning Techniques

- Ryan Barnett Senior Security Researcher Trustwave's SpiderLabs rbarnett@trustwave.com. Revision 1(January 7, 2011) "XSS Street-Fight:The Only Rule Is There Are No Rules;"

Index Terms
Computer Science Artificial Intelligence

Keywords
Cross site scripting (XSS) SOL injection Script injection attack Cross site Request Forgery (CSRF) vulnerability
malicious code