Abstract

Cross-site scripting (XSS) is a code injection attack that allows an attacker to execute malicious script in another user's browser. Once the attacker gains control over the website vulnerable to XSS attack, it can perform actions like cookie-stealing, malware-spreading, session-hijacking and malicious redirection. Malicious JavaScripts are the most conventional ways of performing XSS attacks. Although several approaches have been proposed, XSS is still a live problem since it is very easy to implement, but difficult to detect. In this report, we propose an effective approach for XSS attack detection. Our method focuses on balancing the load between client and the server. Proposed method performs an initial checking in the client side for vulnerability, using divergence measure. If the suspicion level exceeds beyond a threshold value, then the request is discarded. Otherwise, it is forwarded to the proxy for further processing. In our approach we propose an attribute clustering method supported by rank aggregation technique to detect confounded JavaScripts. The approach is validated using real life data.
We also propose an XSS response system to mitigate XSS attack, which is based on SCIT architecture[7].

keywords: XSS, malicious script, proxy, divergence, attribute clustering,