Abstract

The increasing use of sophisticated JavaScript in web applications has led to the widespread exploitation of cross-site scripting (XSS) flaws. We present an "input filter & sanitization" detection-based approach for detecting cross-site attacks. This report presents a model of XSS filter which supplements the security at client/server side with the mechanism of two-way filter and delivers a platform independent explanation to cater security against enormous variants of XSS attack. To address the security issues, an open source PHP based website is evaluated to render threat against XSS-vectors injected in input fields, URL and source-code using commercial browsers. As a result of evaluation, the vulnerable sections of the website are declared as high/low recommendation for the proposed model. Considering the extracted facts, an experiment has been conducted on the website using the proposed model for detecting and sanitizing all the variants of XSS vectors.

Our work involves study of cross-site scripting attack ,its present technique and its detection methods. In that manner we have studied for XSS attacks and prepared a test bed(web application) to demonstrate the attack detection. For the detection purpose I taken input filter & sanitization detection-based method. So I have implemented the algorithms and Result observed. Finally I got very satisfactory results.