Abstract

In this world of networking where people around the globe are connected, Cross-site Scripting (XSS) has emerged to one of the most prevalent growing threat. XSS attacks are those in which attackers inject malicious codes, most often client-side scripts, into web applications from outside sources. Because of the number of possible injection location and techniques, many
applications are vulnerable to this attack method. Even though the main reason for the vulnerability primarily lies on the server side, the actual exploitation is within the victim’s web browser on the client side.

In this paper, we propose a passive detection system to identify successful XSS attacks. Based on a prototypical implementation, we examine our approach’s accuracy and verify its detection capabilities. We compiled a data-set of HTTP request/response from 20 popular web applications for this, in combination with both real word and manually crafted XSS exploits; our detection approach results in a total of zero false negatives for all tests, while maintaining an excellent false positive rate for more than 80 percent of the examined web applications.

Reference

- Cross site scripting techniques and mitigation by CESG revision 1.0, October 2007.
- SC magazine on the article Redditt Succumbs then cleans up from XSS Attack by Dan Kaplan dated September 28,2009.
- False Positive defined at Virus list.com .
- How serious are XSS threats http://doteduguru.com/id3067.

Index Terms

Computer Science Security

Key words

XSS attack Enhanced XSS Guard algorithm
E-Guard
Server-side detection
Client-side detection