Abstract

Cross Site programming (XSS) is the script attack in web pages, and it is accounted as one of the most dangerous problems of web applications. The researchers of security have investigated on different problems and they have found that the XSS vulnerability exists in many of known websites. The vulnerability is applied when an attacker reaches to an authorized user’s web explorer optionally and he/she might do cookie theft, develop destructive software, thieve the session and change the path of destruction. The validation of the user’s input is the first obstacle to protect the web applications against this vulnerability. The main aim of improving the security of web applications is improvement in the quality of user’s input validation. Unfortunately, the web application developers usually forget the user’s input validation and/or implement a weak validation. In this paper, it is attempted to present a pattern to validate the user’s input correctly in the web applications, and the obtained results are compared with the tools of scanning the existing vulnerability.

Index Terms

Computer Science  Networks
Keywords

web vulnerabilities, input validation, XSS malware