Abstract

Utilization of websites to help the community both in terms of exchanging information or conducting transactions is common. However, the use of PHP programming language in website development is still very vulnerable to security attacks, for example attacks such as XSS and SQL Injection. This research builds the detection of php scripts using the Forward Taint data analysis method. Research has been carried out to test this attack. However, the accuracy that has been inferred is still very low. This is getting higher because of the false positive generated. So in solving this problem, the forward taint data analysis method performs double checks that will reduce the positive false value generated. Accuracy resulting from this research reached 90%. These results outperform other existing methods.

Keywords: PHP Vulnerability, SQL Injection, XSS, Forward Taint analysis, Regular Expression