Abstract

Cross Site Scripting (XSS) becomes most popular issues in *web* application security. The attacker be able to inject certain scripting code into a *web* application and it will activated by the time another user access this application. User browser will send the user's information into attacker's computer. This *web* application vulnerability may give risks to an user account for hijacking. This may harmful for user account privacy.

The precaution steps can be done by filtering all input and output data variable in *web* application. This final assignment gives one of solution which is a *web* PHP application module to prevent the XSS called xrex. Xrex itself was immplemented into PHP class. XSS can be detected and helped by *rules* in form of *regex* according XSS cheat sheet [12]. This module was tested to *web* application and gave the input as strings of XSS attack and other strings which was considered normal. As a result, the input showed 0 false negative and 7 false positive due to xrex can not be oversee and filter hyperlink and image which is refered by other hosts.

Keywords: *Web* Security, XSS, Cross Site Scripting, PHP, *Regex*