Abstract

This paper describes the security attacks and specially focuses on Cross Site Scripting attacks. It further also discusses types and several counter measures. The major problem faced by the web application is the parameter manipulation, through which the attackers are aiming to access the database. Generally web applications maintain same structure and value. In that,
required information is being accessed by the identical variables and keywords through web parameters. Parameter manipulation is the major issue in the web application used by the attacker to manipulate the parameter being sent by the browser and executed by the server. These vulnerabilities occur after the string gets returned to the user's web browser by a susceptible web application. Therefore, to prevent XSS vulnerabilities, it is obligatory to prepare preventative measures to protect the parsing processing in the web browser so that there is no influence even from the effect of the string prepared by the attacker.

Reference


Index Terms

Computer Science

Communications

Key words

Cross Site Scripting

web

cross site scripting

application

parameter manipulation

XSS vulnerabilities