Abstract

Nowadays, web applications are common around the world. Every major company/organization have a web application presence. Most of these organizations use web applications to provide various services to clients. Some of these web applications employ database driven content. The back-end database often contains confidential and sensitive information such as password, credit card number, financial data, medical data, email details. Typically the web user/client supplies information, such as a username and password and web server receive user request and interact with the back-end database and returned relevant data to the Front-end.

Web Applications penetration testing and security has become progressively most important these days. A lot numbers of malicious attacks are being deployed on the web application. Due to dramatic increase in Web applications usage, Web application get vulnerable to variety of threats. Most of these malicious attacks are targeted towards the web application layer and waf firewall alone cannot prevent these kinds of attacks. The reason behind success of these attacks is the ignorance of application developers while coding the web applications and the
SQL injection attack, SQL query, XSS (cross site scripting), Web application, Payload, filters.