Abstract

Nowadays, web applications are common around the world. Every major company/organization has a web application presence. Many 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 passwords, credit card numbers, financial data, medical data, email details. Typically, the web user/client supplies this information, such as a username and password, and the web server receives user requests and interacts with the back-end database to return relevant data to the front-end.

Web applications penetration testing and security has become progressively more important these days. A lot of malicious attacks are being deployed on the web applications. Due to the dramatic increase in web applications usage, web applications get vulnerable to a variety of threats. Most of these malicious attacks are targeted towards the web application layer, and a webfirewall alone cannot prevent these kinds of attacks. The reason behind the success of these attacks is the ignorance of application developers while coding the web applications and the
SQLi and XSS Attack Introduction and Prevention Technique

predefined vulnerabilities in the existing technologies. Web application attacks are the latest trend and hackers are trying to hack/exploit the web application using different techniques. Various types of solutions are available as open source and in market. But the selection of suitable solution for the security of the organizational systems is a major issue. Some Attack Prevention Technique protect web applications from attacks they sit in front of web applications monitors activity, and block malicious traffic.

References

http://www.owasp.org/index.php/Xss_(Cross_site_scripting)_prevention_cheat_Sheet

Index Terms

Computer Science Security

Keywords

SQL injection attack, SQL query, XSS (cross site scripting), Web application, Payload, filters.