Abstract

The Internet, which can be defined as a huge network of networks - both wired and wireless, uses the Internet Protocol Suite (TCP/IP) to make information available beyond geographical boundaries. Computing devices all through the world connect to the World Wide Web via the Client Server architecture. In this architecture, the client requests some information from a web server through a web browser. The web server connects to a database server in turn to fetch data. The connection between the web server and the database is the one that needs to be well secured. This is where the role of secure authentication techniques comes into picture. Nowadays, Cyber-crimes are becoming rampant. These include illegal access of data, illegal interception of data, eavesdropping of unauthorized data over an information technology infrastructure, etc. Popular Web attacks include Spam, Phishing Attacks, Information warfare, Nigerian Scams, and Denial-of-Service attacks. At some or the other stage, most of these are
ramifications of web attacks and SQL attacks – practical implementation of an advanced analysis and prevention technique of which is explained in this paper. It uses a multi-tier approach which makes web applications retain their simplicity for the user and complexity for the attacker.

References

- PHP, AJAX, MySQL and JavaScript Tutorials, http://www.w3schools.com/

Index Terms

Computer Science  Emerging Trends in Technology
Keywords
Denial-of-service Attacks  Xss  Brute Force  Dormant Phase  Alert Phase And Inquisitive Phase