Abstract

With the recent rapid increase in web based applications that employ back-end database services, results show that SQL Injection and Remote File Inclusion are the two frequently used exploits rather than using other complicated techniques. With the rise in use of web applications, SQL injection based attacks are gradually increasing and is now one of the most common attacks in the internet. It allows an attacker to gain control over the database of an application, thereby able to read and alter confidential data. This paper illustrates few different forms of SQL injection and based on observation, it is seen that SQL Injection is interpreted differently on different databases. Finally, an effective solution is proposed for the prevention of these kinds of injection attacks, in such a way that it is independent of the underlying platform and database. Two levels of user authentication has been proposed in this method, SQL based authentication and an XML based authentication, and has been found to be very effective in preventing such attacks.
Preventing SQL Injection Attacks

- NTAGW ABIRA Lambert, KANG Song Lin, "Use of Query Tokenization to detect and prevent SQL Injection Attacks", 978-1-4244-5540-9/10/2010 IEEE.
- Prof (Dr.) Shushila, Madan Supriya Madan, "Shielding Against SQL Injection Attacks Using ADMIRE Model", 2009 First International Conference on Computational Intelligence, Communication Systems and Networks, 978-0-7695-3743-6/09 2009 IEEE.

Index Terms

Computer Science
Security

Keywords

Web architecture  SQLIA  HTTP  XML