Abstract

For internet, web application exists and for web application syntax, semantics, coding and design exists, and for coding and designing, algorithm exists, and for algorithm, protecting techniques and rules exists, But as the internet technologies advanced, vulnerability also advanced. Various old procedures, algorithm functions, coding and designing syntax and
Safe Guard Anomalies against SQL Injection Attacks

... semantics are there, which are vulnerable to attack and if used could be easily traced or hacked by the attacker. Old practices which are vulnerable should be banned in organization, companies and govt. sectors and secure guidelines should be issued, which consists of security guidelines and should be strictly followed. In this paper we have proposed coding flaws at different platforms and their solutions.

Reference

- Monica S. Lam, Michael Martin, Benjamin Livshits, and John Whaley, “Securing Web Applications with Static and Dynamic Information Flow Tracking,” PEPM’08, January 7–8, 2008, San Francisco, California, USA.
- SQL Injection Attack Examples based on the Taxonomy of Orso et al.
- V.B. Livshits and M.S. Lam, ”Finding Security vulnerability in java applications with static analysis”, In proceedings of the 14th Usenix Security Symposium, Aug 2005.

**Index Terms**

Computer Science  
Security

**Key words**

SQL Injection  
Database Security

Authentication  
HTTP