Abstract

SQL injection attack (SQLIA) is a serious threat to web applications. A successful SQLIAs can have serious consequences to the victimized organization that include financial lose, reputation lose, compliance and regulatory breach. Therefore, developing approaches for mitigating SQLIA is paramount important. To this end, we propose an approach based on negative tainting along with SQL keyword analysis for detecting and preventing SQLIA. We have tested our proposed approach on all types of SQLIAs techniques by generating SQL queries containing legitimate SQL commands and SQLIA. We present an analysis and evaluation of the proposed approach to demonstrate its effectiveness in detecting and protecting SQLIA attack.

References

2. P. Bisht, P. Madhusudan, and V. Venkatakrishnan, "CANDID: Dynamic candidate


Index Terms

Computer Science Security

Keywords

Cybercrime, SQL Injection, SQLIA, Vulnerabilities, Web Application Security