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


detection based on removing SQL query attribute values," Mathematical and Computer

40. W. G. J. Halfond and A. Orso, "Preventing SQL injection attacks using AMNESIA," 2006,
pp. 795-798.

41. Z. Su and G. Wassermann, "The essence of command injection attacks in web

42. S. Thomas and L. Williams, "Using Automated Fix Generation to Secure SQL
Statements," presented at the Proceedings of the Third International Workshop on Software

43. G. Wassermann and Z. Su, "An analysis framework for security in Web applications," in
Proceedings of the FSE Workshop on Specification and Verification of component-Based

44. G. Buehrer, B. W. Weide, and P. A. G. Sivilotti, "Using parse tree validation to prevent
SQL injection attacks," presented at the Proceedings of the 5th international workshop on
Software engineering and middleware, Lisbon, Portugal, 2005.

45. A. Nguyen-Tuong, S. Guarnieri, D. Greene, J. Shirley, and D. Evans, Automatically
hardening web applications using precise tainting: Springer, 2005.

46. F. Valeur, D. Mutz, and G. Vigna, "A learning-based approach to the detection of SQL
attacks," in Detection of Intrusions and Malware, and Vulnerability Assessment, ed: Springer,
2005, pp. 123-140.

Index Terms

Computer Science    Security

Keywords

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