Asian Journal of Engineering and Technology Innovation

ISSN : 2347-7385

REVIEW ARTICLE

Defeating SQL injection using Data cleansing algorithm

Digambar Patil, Abhishek Bhardwaj, Laxman Teli, Dattatray Lugade, , Vijay Girange
Computer Engineering Indira College of Engineering and Management, Parandwadi, Pune.

Received on: 20-02-2014
Accepted on: 10-03-2015
Published on: 15-03-2015

Digambar Patil,
Abhishek Bhardwaj,
Laxman Teli,
Dattatray Lugade, ,
Vijay Girange
Computer Engineering, Indira College of Engineering and ManagementParandwadi, Pune
laxmant.13893@gmail.com

ABSTRACT
Security is one of the major concerns in communication networks and other online services. Injection attacks and XSS attacks are the two most common attacks on System. This proposed methodology is based on Proxy Agent, that will try to classify the request as a scripted request, or query based request, and then, will detect the type of attack occurred, if any. This method will detect both SQL injection attack as well as the Cross -Site Script attack. SQLIA is technique by which attackers gain access over back -end databases by inserting the malicious codes through front-end.SQL injection attacks (SQLIAs) in recent days have emerged as a major threat to database security.

Keywords: Code-Injection, HTTP protocol, SQL-Injection, Cross-Site Scripting, SQL query, Proxy agent.

QR Code for Mobile users

Conflict of Interest: None Declared

Cite this article as:
Digambar Patil, Abhishek Bhardwaj, Laxman Teli, Dattatray Lugade, , Vijay Girange, Defeating SQL injection using Data cleansing algorithm. Asian Journal of Engineering and Technology Innovation 03 (06); 2015; 07-09.

INTRODUCTION

DEFINITION:

SQL Intrusion Protection against Injection Attacks using a reverse proxy server and preventing it using data cleansing algorithm. SQL sing data cleansing algorithm

SCOPE:

SQL Injection attacks provide a great threat to the applications dependent on database. Attack will occur due to poor system design, mistakes in configuration, or poorly written source code of the system web application. A threat may be lead to harm the database, and other components of same, which are needed to be protected from all types of threat. Reverse proxy will help the user request to direct request to the proxy server and then cleaning the request by modified data cleansing algorithm and the re-directing the request to the main server if not found malicious.

RELATED WORK DONE:

LwinKhinShar and HeeBengKuan Tan[1], has proposed the strategy for fighting SQL injection attack, which now has come as widespread security risk, calls to integrate together defensive coding practices & vulnerability detection at runtime.

Atul S. Choudhary[2], proposed Security is one of the major concerns in communication networks and other online Internet services, which

have become pervasive in domains like business organizations, government bodies.Internet Network security involves activities that all enterprises, organizations, and institutions undertake to keep safe the value and usability of their owned assets and to maintain the integrity between the operations.

S. Fouzul Hidhayaand & Angelina Geetha[3], proposed the term SQL injection has been believed to be first used in "SQL Injection FAQ" published by Chip Andrews . He, explains facts about the SQL injection attacks done till now. The black-box test method implemented in WAVES, used a web crawler to identify points in web application that can be used to inject SQLIAs

Mahima shriwastava [4] , proposes the database community has produced a large amount of research on integrity constraints and other safety measures to maintain and ensure the quality of information stored in relational databases, real-world databases often still contain a non-trivial number of errors.

PROPOSED SYSTEM:

A Code Injection Detection Tool (CIDT) is proposed in this paper which will deal with the Code Injection attacks, caused in Web Applications. The system proposed will consists of two modules; the Script detector and Query detector.All HTTP requests coming through the client side instead of going to the web server will transfer to CIDT within which the request is feed to both modules one by one and when any malicious content is found in the request by either of module, the request will be considered as not valid and its execution will be blocked on the server. Injection Detection Tool will function like a proxy between user request and web server. The HTTP request having a session id will be forwarded to the proxy agent (CIDT), which will authenticate the request by sending it to the Query detector and Script Detector. First, Script detector validates the request and if any invalid character is found in the input query it is rejected and not forwarded to next immediate module in the system.Only request which are reported as valid by Query detector are forwarded to the next module. Script detector filters the request for invalid tags and encodes it before forwarding to application server. Functioning of both the modules is independent in a sense that the valid request goes to both the modules before getting executed on the web server.

RESEARCH DIRECTIVES:

Proposed algorithms:

1. Query detector: In this algorithm proposed by the user input will be taken here username and password and checked for any misbehaved query in the input. In general this will not direct the request to the script detector if detection true.
2. Script Detector: It will take the input from query detector and scan it for URLs scripts.Flow wise check of all the tokens in the list will be carried out. Regular expressions will be used in this type of checking. If tags are matched correctly then check for the attributes will be performed. Encoding unknown tags will be done after this.
3. Modified Data Cleansing Algorithm (DC algorithm): The modified data cleansing algorithm will attempt to clean the request if not possible it will just not allow and block the user request

CONCLUSION:

Different injection attacks are studied.The system is proposed to check maximum vulnerability thus there exists a chance of attack as the advanced sql injection attacks are developed.The detection and prevention of the attacks will be done with the help of the filter designed.

REFERENCES

1. LwinKhinShar and HeeBengKuanTan,"Defeating SQL injection",Nanyang Technological University, Singapore,IEEE March 2013.
2. Atul S. Choudhary Vishwakarma Institute of Technology, " CIDT: Detection of Malicious Code Injection Attacks on Web Application",IJCA August 2012.
3. S. Fouzul Hidhaya and Angelina Geetha, "Intrusion Protection against SQL Injection Attacks Using a Reverse Proxy",CS & IT 2012.
4. Mahima Srivastava*" Algorithm to Prevent Back End Database against SQL Injection Attacks"*Dept. Of CSE RKGITW Ghaziabad, India 2014.
5. Lwin Khin Shar and Hee Beng Kuan Tan "Mining Input Sanitization Patterns for Predicting SQL Injection and Cross Site Scripting Vulnerabilities",School of Electrical and Electronic Engineering ,Nanyang Technological University Singapore, ,IEEE March 2012.