ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

A Review: Prevent SQL Injection Attacks Using IPS

Harpreet Kaur[1], Mrs. Sarika Dhingra[2]

Student, CSE, JCDMCOE, Sirsa, India [1]

Asst Professor, CSE, JCDMCOE, Sirsa, India [2]

Abstract: Database is the key component for store the information in organizations. The information of organization should be secured from the intruders so that the information should be confidential and available at the right time and no wrong operation should be executed. Database information is the crucial part as it needs more security because this contains the password, user information, even it can be in encrypted form but intruder can alter the information or delete it. This paper has been considered the scenario of company where the multiple users can perform different operations and there is need to traverse the operations of the user. Several mechanisms needed to protect data, such as authentication, user privileges, encryption, and auditing, have been implemented in commercial DBMS. But still there are some ways through which systems may be affected by malicious transactions. This paper has been proposed the IPS technique to prevent the intruder's attack.

Keywords: Intruder, IPS, SQL-Injection, Database, Security.

I. INTRODUCTION

The web is a highly programmable environment that allows mass customization through the immediate deployment of a large and diverse range of applications, to millions of global users. Two important components of a modern website are flexible web browsers and web applications; both available to all and sundry at no expense. Web browsers are software applications that allow users to retrieve data and interact with content located on web pages within a website. The Internet is a huge interconnected network, the largest in the world. A great deal has been made about the accessibility of the Internet as well as how it will supposedly change all of our lives. Computer files are replacing paper files as electronic records in institutions such as hospitals, insurance providers, and banks are quickly replacing their carbon-based counterparts. As they are getting used to the idea of using it, people are going shopping and banking over the Internet.[3] People are demanding more and more access to the Internet – always wanting the information faster, more constantly available, and increasingly diverse in content. Insurance providers are starting to encourage employers, physicians, and insurance brokers to submit medical claims information electronically in order to cut down on costs and improve turnaround time. So for this, the SQL technique has been introduced for managing and retrieving information. SQL (pronounced "S-Q-L") is the high-level language used in numerous relational database management systems. It was originally developed in the early 1970's by Edgar F. Codd at IBM and soon became the most-widely used language for all relational databases. SQL is a declarative computer language which has elements which include clauses, expressions, predicates, queries, and statements [2].

As stated, websites depend on databases to deliver the required information to visitors. If web applications are not secure, i.e., vulnerable to, at least one of the various forms of hacking techniques, then your entire database of sensitive information is at serious risk.

Some hackers, for example, may maliciously inject code within vulnerable web applications to trick users and redirect them towards phishing sites. This technique is called Cross-Site Scripting and may be used even though the web servers and database engine contain no vulnerability themselves. Recent research shows that 75% of cyber attacks are done at web application level.

Database security is the system, processes, and procedures that protect a database from unintended activity. Unintended activity can be categorized as authenticated misuse, malicious attacks or inadvertent mistakes made by authorized individuals or processes. [4].

One of the techniques available to the would-be information thieves is SQLInjection (SQL-I). SQL-I attacks involve a variety of methods, but the intention of an attacker using it is to submit specially-chosen patterns when asked for the user's username and password on an internet form

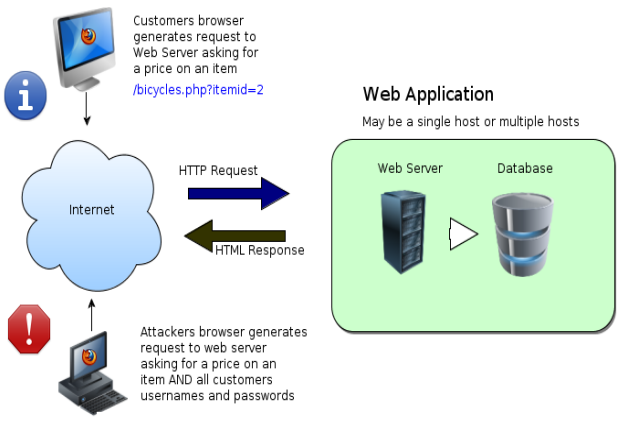

Fig 1 Web Server Attack

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

Privilege elevation exploits can be defeated with a combination of query-level access control and traditional intrusion prevention systems (IPS). Query-level access control can detect a user who suddenly uses an unusual SQL operation, while an IPS can identify a specific documented threat within the operation.

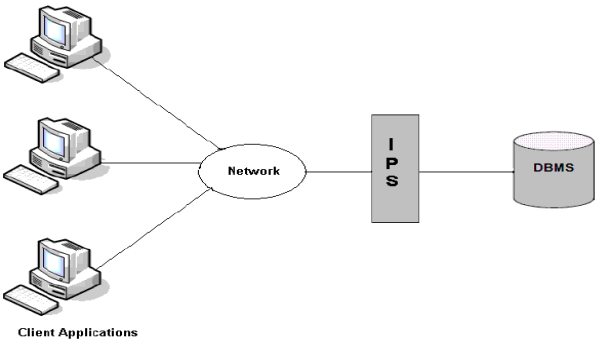

Fig 2 Database Management System with Intrusion Prevention System

II. LITERATURE REVIEW

Author has been proposed the attacks using SQL. SQL Injection poses a serious security issue over the Internet or over web application. In SQL injection attacks, hackers can take advantage of poorly coded Web application software to introduce malicious code into the organization's systems and network. The vulnerability exists when a Web application do not properly filter or validate the entered data by a user on a Web page. Large Web applications have hundreds of places where users can input data, each of which can provide a SQL injection opportunity. Attacker can steal confidential data of the organization with these attacks resulting loss of market value of the organization. This paper presents an effective survey of SQL Injection attack, detection and prevention techniques [1].

The penetration test is a crucial way to enhance the security of web applications. Improving accuracy is the core issue of the penetration test research. The test case is an important factor affecting the penetration test accuracy. In this paper, they discuss how to generate more effective penetration test case inputs to detect the SQL injection vulnerability hidden behind the inadequate blacklist filter defense mechanism in web applications. They propose a model based penetration test method for the SQLinjection vulnerability, in which the penetration test case generation is divided into two steps: i) Building model for the penetration test case, and ii) Instantiating the model of penetration test case. Our method can generate test case covering more types and patterns of SQL injection attack input to thoroughly test the blacklist filter mechanism of web applications. Experiments show the penetration test case generated by our method can effectively find the SQL injection vulnerabilities hidden behind the inadequate blacklist filter defense mechanism thus reduce the false negative and improve test accuracy [2].

With changing times, our dependence on the web applications for the fulfilment of our daily needs (like online shopping, banking, share trading, ticket booking, payment of bills etc.) has increased. Because of this, our confidential data is present in the databases of various applications on Web. The security of this myriad amount of data is a matter of major concern. In recent times, SQL Injection attacks have emerged as a major threat to database security. In this paper they define SQL Injections, illustrate how SQL Injections are performed. In addition they have also surveyed the various SQL Injection detection and Prevention tools and well-known attack methods. Finally, they have provided our solution to the problem and have assessed its performance [3].

Security in today's world is one of the important challenges that people are facing all over the world in every aspect of their lives. Similarly security in electronic world has a great significance. In this paper, they survey the security of database. This is an area of substantial interest in database because they know that, the use of database is becoming very important in today's enterprise and databases contains information that is major enterprise asset. This survey was conducted to identify the issues and threats in database security, requirements of database security, and how encryption is used at different levels to provide the security [4].

Intrusion detection and prevention systems (IDPS) are security systems that are used to detect and prevent security threats to computer systems and computer networks. These systems are configured to detect and respond to security threats automatically there by reducing the risk to monitored computers and networks. Intrusion detection and prevention systems use different methodologies such as signature based, anomaly based, stateful protocol analysis, and a hybrid system that combines some or all of the other systems to detect and respond to security threats. The growth of systems that use a combination of methods creates some confusion when trying to choose a methodology and system to deploy. This paper seeks to offer a clear explanation of each methodology and then offer a way to compare these methodologies [5].

The traditional solution to database security has a drawback that it cannot deal with malicious attacks by persons with legal identity, and that, it is in general not cost-effective to users who have different security requirements for it only offers fixed security level. By adopting multi-layer security model, namely "user +OS +DBMS +transaction-level intrusion tolerance", it integrates redundancy and variety technology; by adopting integral security strategy and server-oriented intrusion tolerance technology, it realizes the survivability and availability of database, and the confidentiality and integrity of sensitive data. In this way, it can effectively resist malicious attacks by persons with legal identity and reduce the cost of security [6].

III. OBJECTIVES

The main Aim of this research is to understand the security threats and identify the appropriate security techniques used to detect and prevent database from malicious attack. Intrusion prevention system comes in between the network and DBMS as shown. Thus it checks all the transactions before they are committed and prevents the malicious ones from getting committed.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

1. This model will even help us to avoid damage from those malicious transactions which cannot be rolled back.
2. This model shown acts before the database and prevents the transactions from getting committed in database.
3.Instant detect and prevent database from malicious transactions using algorithm for instant detection and prevention.
4. Implementation of this research will be demonstrated by Developing the Web Application in ASP.Net 4.0 with Backend SQL Server 2008.

IV. PROPOSED METHODOLOGY

These are the steps which need to follow for database security and this will protect the database from the crucial SQL queries. The weight age concept has been considered with the queries for identify the crucial queries.
1. Work on above mentioned Phases
2.Design an Algorithm for INSTANT detection and Prevention.
3. Implement the algorithm with help of programming.
4. Perform Experimental Evaluation.
5. Introduce any hashing technique to improve data security.
6. Perform different Malicious Transactions to verify success rate of method.
7. Experimental results and analysis of the application.

V. CONCLUSION AND FUTURE WORK

In this paper, we have been proposed the security technique such as IPS and methods which can be used for secure transmission of the information over the inter-network and intra-network which will protect from the SQL-I Attack. The proposed is not implemented yet.
The implementation part will be covered in the next paper, which will demonstrate the real working of proposed algorithm.

REFERNCES

[1]Kumar, P. ; Pateriya, R.K.(2012), "A survey on SQL injection attacks, detection and prevention techniques", Computing Communication & Networking Technologies (ICCCNT),Third International Conference, Page(s): 1 – 5
[2]Tian Wei et. al. (2012), "Attack Model Based Penetration Test for SQL Injection Vulnerability", Computer Software and Applications Conference Workshops (COMPSACW), 2012 IEEE, Page(s): 589 – 594
[3] Neha Singh (2012), " Sql Injections – A Hazard To Web Applications", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 6, June 2012.
[4] Iqra Basharat(2012), "Database Security and Encryption: A Survey Study", International Journal of Computer Applications,Volume 47– No.12, June 2012
[5]Mudzingwa, D. (2012), "A study of methodologies used in intrusion detection and prevention systems (IDPS)", Proceedings of IEEE, Page(s):1 - 6
[6]Jianhua Lu et. al. (2012), "A Design of Solution to Database Security Based on Multi-Layer Intrusion Tolerance", Industrial Control and Electronics Engineering (ICICEE), Page(s): 1571 – 1574.