ISSN 2395-1621

Online Kiosk for Lost and Found Valuable

[#1]Mahendra Dambe, [#2]Rishab Advani, [#3]Omkar Jambkar, [#4]Rishabh Gupta

[2]rdhadwani@gmail.com

Pimpri Chinchwad College of Engineering,

Sector no. 26 Nigdi Pradhikaran Pune - 411044

ABSTRACT

With the increasing penetration of Internet in our daily chores of life, almost everything is available on click of a button. In recent years, Internet has not just been a commodity but necessity, a lot of things can be done with the help of internet; From ordering Food to booking a Taxi everything is available by a touch on our handheld devices. But still there are something for which there has been no Centralized Web System available which could help mankind in certain ways. The purpose of this project is to create a centralized server for lost valuables and way to access it securely. We believe that valuable has a more sentimental value than the monetary value. We intend to create a user sourced database which contains list of valuables along with their attribute. Users who have lost their valuable can look it up using search which requires user to enter specific details to negate fraud attempts.

Keywords: Online Kiosk, Lost and Found, Valuable, SQLIA, Captcha, OTP, TOMCAT, APACHE, MySQL, JavaScript

ARTICLE INFO

Article History

Received: 9th December 2017

Received in revised form :

9th December 2017

Accepted: 12th December 2017

Published online :

12th December 2017

I. INTRODUCTION

At present scenario it has been observed that people are intended to serve society with goodwill, but sometimes due to technical constraints their efforts do not reach the desired results. Our topic relates to such incidents where people have found some valuable product and want to hand over it to authentic owner. Captcha/OTP can be used to reduce possible attempts with automated script attack to brute force the authentication. Fraud user's database can be maintained with a Public ID (e.g. Aadhar Card, PAN Card). SQL injection attacks(SQLIA) are the most serious threats to WEB program security, while dynamic analysis may effectively defend SQLIA. An intention-oriented detection approach is proposed to represent all the database operations expected by WEB programmers. It intercepts the requests before user submission and drops the unintentional ones. A language named SQLIDL is proposed to express the user intention of database operations and is used to transform SQL requests into string sets formalized by the deterministic finite automata (DFA). SQLIDL currently implements the regular expression representation of table names, column names, values and store procedure names. The prototype implementation is evaluated on Security Bench and the results demonstrate all existing SQL attack patterns can be correctly detected with acceptable run-time overhead.

II. LITERATURE SURVEY

[1] Zhanwei Cui, Jianping Zeng*, Chengrong Wu, Shiyong Zhang , "Design and Implementation of a New Database Security Model Based on Hopping Mechanism." 2015.

Database security is an important part of information security. With the background of login verification, this paper proposes a database security model based on hopping mechanism and gives theoretical analysis to it. In the theoretical analysis, we give the specific expression of the probability of successful attack and theoretical deducation of the expression. Finally, we establish the prototype of the model and carry out an experiment to validate it. The final experiment shows that the result accords with the theoretical analysis and the model we established has a high efficiency in the database security and can offer a new direction for the database security research.

[2] Gaurav Dubey Vikram Khurana Shelly Sachdeva, "Implementing Security Technique on Generic Database."2015.

Database maintenance has become an important issue in today's world. Addition or alteration of any field to an existing database schema cost high to a corporation. Whenever new data types are introduced or existing types are modified in a conventional relational database system, the physical design of the database must be changed accordingly. For this reason, it is desirable that a database should be flexible and allow for modification and addition of new types of data without having to change the physical database schema. The generic model is designed to allow a wide variety of data to be accommodated in a general purpose set of data structures. This generic mechanism for data storage has been used in various information systems such as banking, defense, e-commerce and especially healthcare domain. But, addressing security on generic databases is a challenging task. To the best of our knowledge, applying security on generic database has not been addressed yet. Various cryptographic security techniques, such as hashing algorithms, public and private key algorithms, have already been applied on a database. In this paper, we are proposing an extra layer of security to the existing databases, through Negative Database technique. The advantages of the negative database approach on generic database has been demonstrated and emphasized. Correspondingly, the complexity of the proposed algorithm has been computed.

[3] Jianhua Lu, Yuhai Sun, Qiuyuan Shen, Yi Li, "A Design of Solution to Database Security Based on Multilayer Intrusion Tolerance."2012

The traditional solution to database security has a drawback that it can not 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.

[4] Xu Ruzhi , Guo jian, Deng Liwu , "A Database Security Gateway to the Detection of SQL Attacks."2010.

With the rapid development of Internet, more and more web applications based on database appeared, thus the databases face the threats. Because of the SQL attacks, people pay much attention to the security of database on the internet. This paper presents a solution that is a database security gateway deployed between web server and database server. The paper describes the architecture of the database security gateway, and focuses on the research of the attack protection module, including the construction of secure rules library, the process of SQL statements filtering, the improvement and application of Sunday pattern matching algorithm. The database security gateway has been carried out in power industry and has good effect.

[5] Mao Chenyu, Guo Fan, "Defending SQL Injection Attacks based-on Intention Oriented Detection."2016.

SQL injection attacks(SQLIA) are the most serious threats to WEB program security, while dynamic analysis may effectively defend SQLIA. An intention-oriented detection approach is proposed to represent all the database operations expected by WEB programmers. It intercepts the requests before user submission and drops the unintentional ones. A language named SQLIDL is proposed to express the user intention of database operations and is used to transform SQL requests into string sets formalized by the deterministic finite automaton (DFA). SQLIDL currently implements the regular expression representation of table names, column names, values and store procedure names. The prototype implementation is evaluated on SecuriBench and the results demonstrate all existing SQL attack patterns can be correctly detected with acceptable run-time overhead.

[6] Ping He, Yuan Lv, Yan Yi, Jianchun Cai, "Study and Design of Database Protection System for Sql Attacks."2015.

SQL attack prevention measures are a hotspot of network security research in recent years. In this paper, the principle and characteristics was introduced firstly, then SQL attacks and preventive measures were given. After the concept of prevention model structure and model built, the prevention work process of the model was summarized.

[7] Hanna Mazzawi , Gal Dalal , David Rozenblat , Liat Ein-Dor , Matan Ninio , Ofer Lavi, " Anomaly Detection in Large Databases using Behavioral Patterning."2017.

We present a novel approach for detecting malicious user activity in databases. Specifically, we propose a new machine learning algorithm for detecting attacks such as a stolen user account or illegal use by a user. Our algorithm relies on two main components that examine the consistency of a user's activity and compare it with activity patterns learned from past access. The first component tests for self-consistency, to determine whether the actions performed by a user are consistent with previous patterns. This engine is based on a probabilistic model that we developed to capture a user's normal behavior. The second component checks for global-consistency, to determine whether a user's actions are consistent with the past actions of similar users. We test our algorithm on access data from SQL databases. Experimental results show that we can keep false positive rates while retaining the overall accuracy level. An outlier detection engine based on the presented methods is now included in the standard offering of IBM InfoSphere Guardium1 with positive user feedback.

[8] S. Al-Sharif, F. Iqbal, T. Baker, A. Khattack, " White-hat Hacking Framework for Promoting Security Awareness"2016.

As the variety of new social media applications are developed at an ever-increasing rate, the number of related potential vulnerabilities and related attack vectors are also increasing. Traditionally, social engineering attacks have always been a major cause of concern for Information Security departments. However, the theft, abuse and manipulation of personal information for malicious purposes has become even prolific since the mass adoption

of social media and gaming applications by the average person, largely fueled by the boom in social media and gaming applications. These newly introduced and ever-evolving apps continue to introduce new vulnerabilities due to poor system design and coding practices and have led to a multitude of sophisticated attacks and digital crimes. Attacks such as, Malware infections, ransomware, Session Hijacking, SQL Injection, and Man-in-the-Middle attacks have been facilitated in part by the race to developing social media platforms, and applications. Hence, more effective countermeasures and prevention techniques are introduced to detect and minimize the resulting damage and losses associated with this trend. This paper presents a novel 'credentials crawling' proof of concept exploit to illustrate the ease with which such attacks can be launched.

III. PROPOSED SYSTEM

All the retrieved items are updated on the database by the local admin of the kiosk. When user wants to query the server, the user must authenticate by providing information of the valuable they are looking for.

Multiple query flooding is mitigated by OTP or Captcha based Turing test for human. Subsequently, malicious SQL injection attacks are prevented by sanitizing the inputs given by the user.

Logs of the session are securely stored on the database for future reference until they are purged.

Once the user authenticates successfully and finds a match for their query, they can visit the kiosk where the retrieved valuable is kept in custody. The user must furnish their identity proof while procuring their lost valuable.

IV. PROPOSED ARCHITECTURE

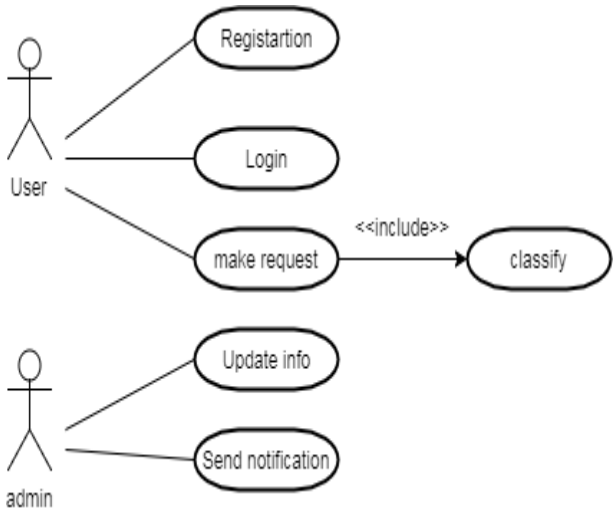

Fig. 1 Usecase Diagram

Secure Server with database and authentication mechanism. Security provided to the database. Front end where the user can search for lost valuables and also a mechanism where other users can list lost valuables.Physical containment of the lost valuable with attributes matching those populated in database. Database which keeps record of users along with their Public ID, i.e., PAN, Aadhar, etc..

V. CONCLUSION

Authentication plays a very important role in protective resources against unauthorized use. Several authentication processes exist from straightforward secret primarily based authentication system to overprice and computation intensive identification systems. Captcha/OTP can be used to reduce possible attempts with automated script attack to brute force the authentication. Fraud users db can be maintained with a Public ID(e.g. Aadhar Card, PAN Card). SQL attack prevention measures are a hotspot of network security research in recent years. After the concept of prevention model structure and model built, the prevention work process of the model was summarized.

REFRENCES

[1] Zhanwei Cui, Jianping Zeng*, Chengrong Wu, Shiyong Zhang , "Design and Implementation of a New Database Security Model Based on Hopping Mechanism." 2015.

[2] Gaurav Dubey Vikram Khurana Shelly Sachdeva, "Implementing Security Technique on Generic Database."2015.

[3] Jianhua Lu, Yuhai Sun, Qiuyuan Shen, Yi Li, "A Design of Solution to Database Security Based on Multilayer Intrusion Tolerance."2012

[4] Xu Ruzhi , Guo jian, Deng Liwu , "A Database Security Gateway to the Detection of SQL Attacks."2010.

[5] Mao Chenyu, Guo Fan, "Defending SQL Injection Attacks based-on Intention Oriented Detection."2016.

[6] Ping He, Yuan Lv, Yan Yi, Jianchun Cai, "Study and Design of Database Protection System for Sql Attacks."2015.

[7] Hanna Mazzawi , Gal Dalal , David Rozenblat , Liat Ein-Dor , Matan Ninio , Ofer Lavi, " Anomaly Detection in Large Databases using Behavioral Patterning."2017.

[8] S. Al-Sharif, F. Iqbal, T. Baker, A. Khattack, " White-hat Hacking Framework for Promoting Security Awareness"2016.

