ISSN 2395-1621

Implementation on Data Modification Attack using the MD5 Algorithm

[#1]Dipika Jagtap, [#2]Priyanka Kesare, [#3]Piyush Shah, [#4]Swapnil Gawai,
[#5]Prof. H.A.Hingoliwala

[1]dipikag.jagtap@gmail.com,
[2]kesarepriyanka1996@gmail.com,
[3]piyush7020@gmail.com,
[4]swapnilgawai13@gmail.com

[#1234]Department of Computer Engineering,
[#5]Professor, Department of Computer Engineering,

JSPM's JSCOE Hadapsar, Pune, Savitribai Phule Pune-41, India.

ABSTRACT

In today's world , many issues in internet security and privacy. We use internet in travelling, E-Commerce site, social media, banking, study etc. But we often face the problems with the privacy of the network system and private data. To increase use of web application and data complexity, web services is going to a multi-tiered design wherein the web server runs the application front-end logic and data is outsourced to a database or file server. The Intrusion detection system plays a key role in computer security technique. But it also has drawbacks of its own. To overcome those drawbacks Duel Security technique is introduced based on ecommerce application. We are implementing duel security using MD5 algorithm and hashing function, an in built web server of windows 7 ultimate, with My SQL Server. This System presents those models the network behaviour of user sessions across both the front-end web server and the back-end database. For that purpose duel security system is used. Duel security prevent attacks and prevents user from unauthorized updating from his/her account.

Keywords: Anomaly detection, Virtualization, Multi-tier web application, Data leakage detection.

ARTICLE INFO

Article History

Received: 2nd June 2019

Received in revised form :

2nd June 2019

Accepted: 5th June 2019

Published online :

6th June 2019

I. INTRODUCTION

Database is a major component of each and every organization. But to store data in database is not sufficient for any organization, since they have to deal with all issues related to database, from which one of the main issue is database security. We deals with the basic approach that determines whether data stored in database is tampered or not. Any business cannot afford the risk of an unauthorized user observing or changing the data in their databases. Web services are widely used by people. Web services and applications have become popular and also their complexity has increased. Most of the task such as banking, social networking, and online shopping are done and directly depend on web. As we are using web services which is present everywhere for personal as well as corporate data they are being attacked easily. Attacker attacks backend server which provides the useful and valuable information thereby diverging front end attack. Data leakage is the big issue for industries & different institutes. It is very hard for any system administrator to find out the data leaker among the system users. It is creating a serious threat to organizations. It can destroy company's brand and its reputation.

Most of the IDS examine the attack individually on web server and database server. In order to protect multi-tiered web services an efficient system call Intrusion Detection System is needed to detect attacks by mapping web request and SQL query, there is direct causal relationship between request received from the front end web server and those generated for the database backend. Dynamic web site allow persistent back end data modification through the HTTP requests to include the parameters that are variable and depend on the user input. Because of which the mapping between the web and the database rang from one to many as shown in the mapping model.

The **MD5 algorithm** is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption.

MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function MD4. The abbreviation "MD" stands for "Message Digest."

SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

To create a system for intrusion detection on static and dynamic web pages (creating session ID's for each user containing the web front end [HTTP] and back end [SQL server]) also make it able to prevent those intrusions from attacking the web pages and it should be able to find out the perpetrator.

II. PROPOSED SYSTEM

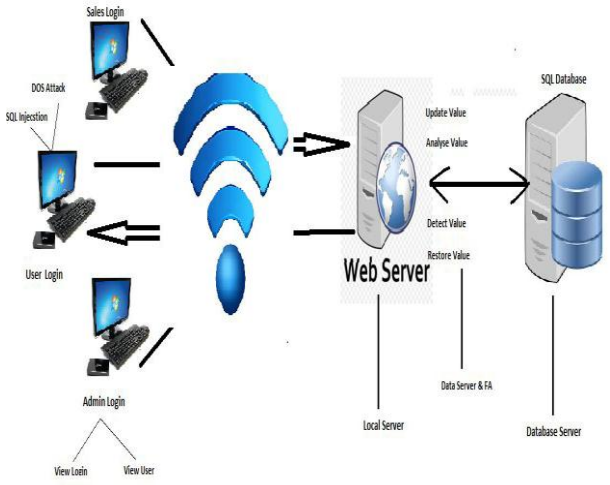


Fig 2. System architecture

In this proposed system there are three modules-Admin, Sales Department and user. All these three modules are connected with the Wi-Fi. At the user side if any sql injection attack and DOS attack is happen then it will be prevented immediately at that time so, user cannot move forward. Admin is the authorized person, he will keep watch on all the user activities and profile and also check log table. He will check first if server is running (on) or stop (off) and at run-time if any value may get changed or any modification is done then it will be an attack. At the back-end admin will analyze this value and detect it. He will restore the initial value automatically within a second of time.

III. METHODOLOGY

MD 5 Algorithm:

Step 1. Append Padding Bits. The message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512.

Step 2. Append Length.

Step 3. Initialize **MD** Buffer.

Step 4. Process Message in 16-Word Blocks.

Step 5. Output.

Module Explanation:

User Module:

User has a authorized login access. He can update all personal information. User can buy a product by login from his account .He also can give authority to generated secure encryption process.

Sales Department:

Sales department work as a attacker. Here attacker may change the database value of any product without authentication.

Admin Module:

Admin is the authorized person, he will check all the user activity , records as well as profile. He also watch the tampering on changing the values from data base.

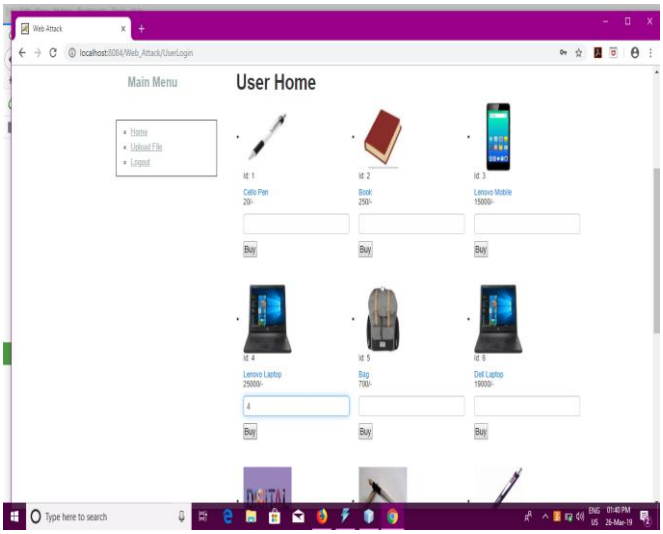
Advantages:

1. The proposed system provides authencation.
2. It also prevents hacking.
4. The system prevents identity theft.

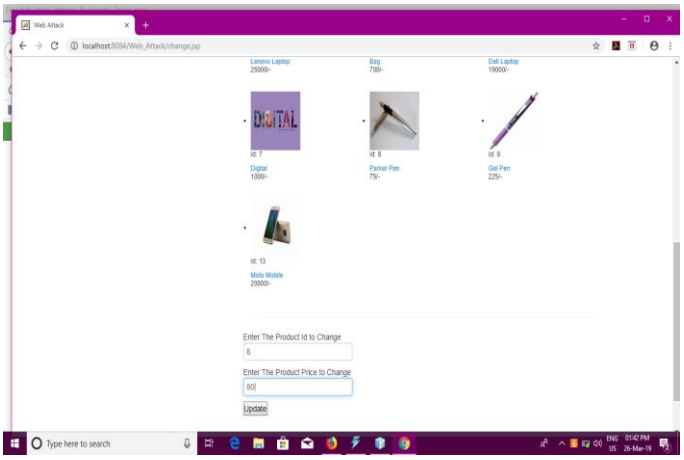
IV. SCREENSHOTS OF MODULES

1. Home Page: We design the home page of data security with identify web attack using the java and jsp. Here show the different tab for individual activity to each.

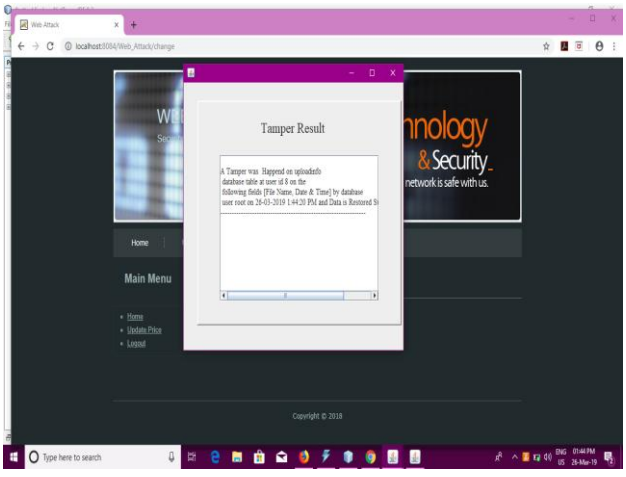
2. User Home: After successfully user login system provide the product list with different attribute for purchasing the product.



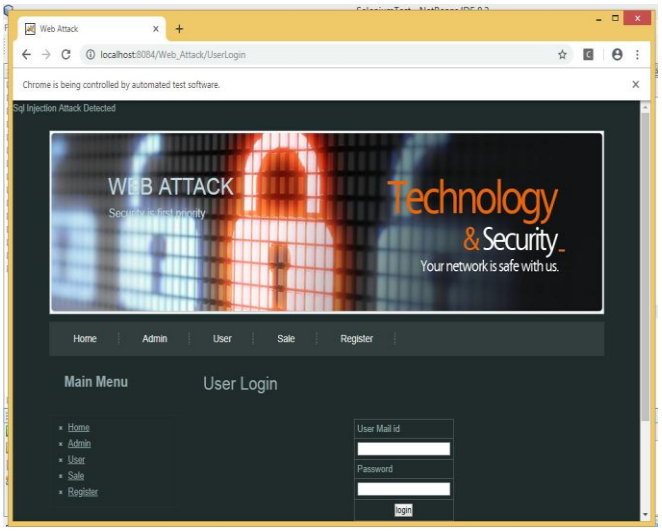
3. Sales Home : Sales home is the impornt panel because of the attcker come here and change the produt value gussing the sales username and password.



4. Tamper Result : After attack happen from sales panel then server give the support to the web attack. Here we design the server to identify the live attack from web server as well as database server.



5. SQL Injection Attack Detected: Here we also check the SQL injection attack on user login phase. SQL injection means unauthorised user can use different symbolic query to machine the database server and try to access the user panel. Here we avoid the symbolic query to SQL injection attack.



V. CONCLUSION

This is an Application of Modified data detection system through unauthorized access. By using MD5 algorithm we are restoring modified data again.

VI. FUTURE WORK

In future we can analyze the SQL Injection attack and Cross Site Scripting attack can be installed on wide range of machines having different operating systems and platforms.

REFERENCE

[1] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, New Publicly Verifiable Databases with Efficient Updates, IEEE Transactions on Dependable and Secure Computing, In press, 2015.

[2] Anmin Fu, Shui Yu, Yuqing Zhang, Huaqun Wang, Chanying Huang, "A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users" IEEE, 2016.

[3] Ekta Naik, Ramesh Kagalkar, "Detecting and Preventing Intrusions In Multi-tier Web Applications", International Journal of Scientific & Engineering Research, Volume 5, Issue 12, December-2014.

[4] V. Vu, S. Setty, A.J. Blumberg, and M. Walfish, A hybrid architecture for interactive verifiable computation, IEEE Symposium on Security and Privacy (SP), pp.223-237, IEEE, 2013.

[5] S. Pearson and A. Benameur. "Privacy, security, and trust issues arising from cloud computing." Proc. Cloud Computing and Science, pp. 693–702, 2010

[6] Nikhil Khandare, Dr. B. B. Meshram, security of online electronic transactions, ISSN: 2320-8163, Volume 1, Issue 5 (Nov-Dec 2013), PP.53-58B.

[7] HatoonMatbouli & Qigang Gao, "An Overview on Web Security Threats and Impact to E-Commerce Success", 978-1-4673-1166-3/12 2012 IEEE.

[8] Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

