www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 05, May 2022, pp : 259-261

e-ISSN : 2583-1062
Impact Factor : 2.205

SQL INJECTION ATTACKS AND PHISHING ATTACKS PREVENTION IN SOCIAL NETWORKING SITES

Miss. Shefali Thakare[1], Prof. P. V. Mhalle[2]

[1]PG Scholar, CSE Department, P R Pote college of engineering and management , Amravati, India

2Assitant professor, CSE Department, Rajiv Gandhi Institute of Technology , Mumbai, India

ABSTRACT

Web applications are presently used for online administrations, for example: long range informal communication, shopping and managing accounts and so forth. Web applications deals with complex user information. Unauthorized access can lead to collapse of a system; even can harass the existence of a company or a bank or a branch. SQL injection attack belongs to one of the means of database security attack. It can be efficiently protected by database security protection technology. This paper gives detailed survey about the main form of SQL injection attack.

Keywords: SQL, WEB, Injection Attack, Prevention Technology.

1. INTRODUCTION

SQL injection is to cheat the server to execute malicious SQL commands by inserting SQL commands into the query string of Web form submission or input domain name or page request.

SQL injection revelations have been SQL injection revelations have been communicated significantly unsafe for the database. Vital databases are absolutely accessible by attacker by injecting SQL queries that are retrieved by web application. As customer information is frequently kept in these databases, important information is lost and the security breach. Attackers can even use a SQL injection exposure is used by attackers for controlling and making the web application structure worse. A class of code-injection attacks is pointed by SQL Injection; customer gives the data which is incorporated into a SQL query in such a way that part of the customer's information to be known by SQL codes. SQL commands given by attacker straight away to the database, through these vulnerabilities. These attacks are dangerous to any Web application that gets data from customers and goes along with it into SQL request on a key database.

2. 2. LITERATURE SURVEY

2.1 Background History

What is SQL Injection?

The so-called SQL injection is to cheat the server to execute malicious SQL commands by inserting SQL commands into the query string of Web form submission or input domain name or page request. For example, many previous video websites leaked VIP membership passwords mostly by submitting query characters via WEB form, which is particularly vulnerable to SQL injection attacks when the application program. SQL injection attacks occur when dynamic SQL statements are constructed using input content to access the database. SQL injection also occurs if the code uses stored procedures, which are passed as strings containing unfiltered user input. Hackers can get access to the website database through the SQL injection attack, and then they can get all the data in the website database. Malicious hackers can tamper with the data in the database through the SQL injection function and even destroy the data in the database. As a web developer, you hate this kind of hacking. It's necessary to understand the principle of SQL injection and learn how to protect your website database by code.

What is Phishing Attack?

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.

Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 05, May 2022, pp : 259-261

e-ISSN : 2583-1062
Impact Factor : 2.205

An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

3. PROPOSED WORK

3.1 Basic Idea

As networks and internet have advanced many offline services have been changed to online services. Nowadays, most online services consist of web services. The ability to access the web from any place at anytime is a great advantage; however, as the popularity of the web increases, attacks on the web increases as well. Most of the attacks made on the web target the vulnerability of web applications

SQL-Injection Attack (SQLIA) is not as damaging to systems using and operating web applications as other attacks, but because of its ability to obtain and charge the sensitive information, such as military systems, banks, and e-business, etc are exposed to a great security risk.

Many divisions are researching a variety of methods to detect and prevent SQLIAs, and the most preferred techniques are Web Framework, Static Analysis, Dynamic Analysis, Combined Static and Dynamic Analysis, and Machine Learning Techniques.

The Web Framework provides filtering methods using the user's input data. However, it is only able to filter special characters therefore, other attacks cannot be prevented. Static Analysis methods analyzes the input parameter type therefore it is more effective than filtering methods, but attacks using the correct parameter types cannot be detected. Dynamic analysis can scan vulnerabilities of web applications without rewriting it however this method is also not able to detect all SQLIAs. Combined Static and Dynamic Analysis can compensate for the weaknesses in each method and is highly proficient in detecting SQLIAs. The combined usage of Static Analysis and Dynamic Analysis method is very complicated.

3.2 Existing System

Although web application can be classified as programs running on a web browser, web applications generally have a Tree-tier construction as shown in Figure 3.1.

i. Presentation Tier: receives the user's input data and shows the result of the processed data to the user. It can be thought of as the Graphic User Interface (GUI). Flash, HTML, Javascript, etc. are all part of the presentation tier which directly interact with the user.

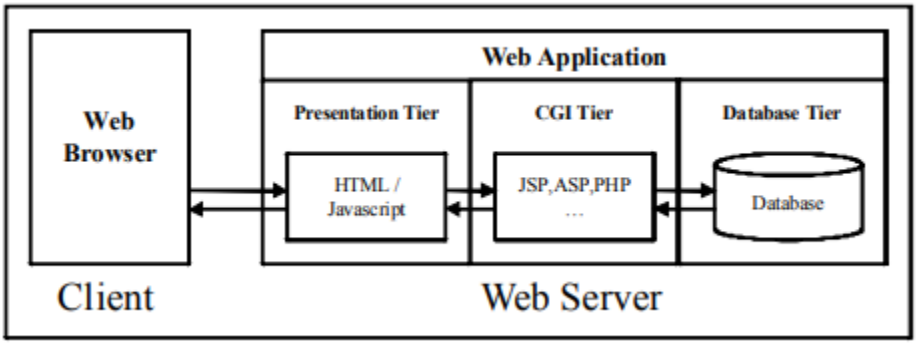

Figure 3.1: Existing System

ii. CGI Tier: also known as the Server Script Process, is located in between the presentation tier and database tier. The data inputted by the user is processed and stored into the database. The database sends back the stored data to the CGI tier which is finally sent to the presentation tier for viewing. Therefore, the data processing within the web application is done at the CGI Tier. It can be programmed in various server script languages such as JSP, PHP, ASP, etc.

iii. Database Tier: stores and manages all of the processed user's input data. All sensitive data of web applications are stored and managed within the database. The database tier is responsible for the access of authenticated users and the rejection of malicious users from the database.

4. RESULTS AND DISCUSSION

This dissertation introduces the SQL injection detection mechanism and protecting web applications from SQL injection attacks. Digital era of technology expects attack free systems making more secure sharing of data. Proposed method makes web applications with ability to detect the code injection (SQL injection) attacks before losing any data makes systems more secure. Combining existing SQL injection detection mechanisms to develop more strong mechanism to make web application more robust is best with result as it's expected from this proposed method.

5. CONCLUSION

SQL injection attackers are smarter and more comprehensive in finding vulnerable websites. There are some new methods of SQL attack. Further study is done for making use of new algorithm to encrypt data query for preventing SQLIA, the query change plan is required.

6. REFERENCES

[1] Ke Wei, M. Muthuprasanna, Suraj Kothari," Preventing SQL Injection Attacks in Stored Procedures", Australian Software Engineering Conference,2006.

[2] Chen Ping, Wang Jinshuang, Pan Lin, Yu Han," Research and Implementation of SQL Injection Prevention Method Based on ISR",IEEE, International Conference on Computer and Communications,2016.

[3] Debabrata Kar, Suvasini Panigrahi," Prevention of SQL Injection Attack Using Query Transformation and Hashing",IEEE, 3rd IEEE International Advance Computing Conference (IACC),2013.

[4] Puspendra Kumar, R.K. Pateriya, "A Survey on SQL Injection Attacks, Detection and Prevention Techniques", INTERNATIONAL CONFERENCE ON COMPUTING, COMMUNICATION AND NETWORKING TECHNOLOGIES (*ICCCNT*), 2012.

[5] Li Qian, Zhenyuan Zhu, lun Hu, Shuying Liu, "Research of SQL Injection Attack and Prevention Technology", International Conference on Estimation, Detection and Information Fusion,2015.

[6] B.Hanmanthu, B.Raghu Ram, Dr.P.Niranjan," SQL Injection Attack Prevention Based on Decision Tree Classification", 9th International Conference on Intelligent Systems and Control (ISCO), IEEE, 2015.

[7] Aditya Rai, MD. Mazharul Islam Miraz, Deshbandhu Das, Harpreet Kaur, Swati," SQL Injection: Classification and Prevention", 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021.

[8] William G.J. Halfond, Jeremy Viegas, and Alessandro Orso, (2006) "A Classification of SQL Injection Attacks and Countermeasures", 2006 IEEE

[9] Ankita Kushwah, Gajendra Singh (2014) "Sql Injection Attacks: Prevention for All Types of Attacks", International Journal of Emerging Engineering Research and Technology Volume 2, Issue 2, May 2014, PP 37-42

[10] Gregory T. Buehrer, Bruce W. Weide, and Paolo A. G. Sivilotti (2005) "Using Parse Tree Validation to Prevent SQL Injection Attacks" , 2005 ACM -59593-204-4/05/09