Protection of Web Application against Sql Injection Attacks

Sonam Panda, [1] Ramani S[2]
VIT University, Vellore, India

Abstract: *SQL injection attack is the most common attack in websites now-a-days. Some malicious codes gets injected to the database by unauthorized users and because of this attack, the actual database can be stolen or destroyed or modified or the device can be taken control by the hacker. The main cause of this type of attacks is poor coding by the developers. Hence, the login phase is more vulnerable to SQL injection attack and prevention technique should be applied on this phase to secure the database. In this paper, some predefined methods are discussed and hybrid encryption method is applied in the database to avoid attack on login phase. This applied hybrid encryption method is a combination of Advanced Encryption Standard (AES) and Rabin cryptosystem. These two level encryption methods are applied to a system where faculty's information are kept and the designing of this system are done by using PHP and MYSQL.*

Keywords: *SQL injection attack, hybrid encryption, AES, Rabin, PHP*

I. Introduction

With the rising use of internet, web application vulnerability has been increasing effectively. SQL injection attack is an easiest method of attack in which attackers inject some SQL codes to the original code in the database to get sensitive information or to destroy the information. History says SQL injection attack has been there around for years and now this is a popular method to exploit the security system.

Different techniques and methods have been developed and used to protect the database. But still attackers use this method very often because they are finding it easy to type a few deformed SQL commands into the front-end as well as back-end application. Types of SQL injection are tautologies, illegal/ logically in corrected queries, union queries, piggy backed queries, blind injection, timing attacks etc. [3][4]. Attackers inject codes using tautology statements into the authentication phase to enter into the database, which says 1=1 is always true and so the injected query becomes true even if the wrong username and password are being entered. Similarly they use logically incorrect queries to get an error message and this message works as a hint for them to find out some information. Single quotes, double quotes and backslashes are generally used in query to make these incorrect codes work correctly. Union operator is used while injecting codes to join the injected query to the original query. Piggy backed queries are those which use semicolons with injected codes to make duplicate codes work along with original ones. Hackers use blind SQL injection attack by asking some true or false questions if error messages are costumed by programmer. To make a delay in operation, attackers use timing attack and by taking the advantage of this, attacker hacks the username and password with the use of BENCHMARKS.

Cryptography is an absolutely necessary field that ensures the security of database. By applying encryption method, database attacks can be prevented. Encryption of data helps to change the data into a format that is not readable [1]. Without the proper key, this format can't be deciphered even if attacker hacks the information. Application of encryption in login phase makes it difficult for unauthorized users to access the database. Indrani Balasundaram et al. (2011) proposed a query encryption method using hybrid encryption in which two layer of encryption was applied i.e. AES and RSA encryption [2]. The method of encryption which combines a symmetric and an asymmetric encryption method to take the advantages of each type of method is called hybrid encryption method. In symmetric key encryption, one common key is used by sender and receiver where as in asymmetric key encryption, two keys are used (a public key and a private key). This paper proposes a technique which is similar to previous paper but here Rabin encryption method is applied instead of RSA as Rabin cryptosystem is said to be a good replacement of RSA cryptosystem. Between these two, AES is a symmetric key cryptography where Rabin cryptosystem is an asymmetric or public key cryptography.

The other part of the paper includes related work about SQL injection attack, work done, implementation and discussion and conclusion respectively.

II. Related work

Ettore Merlo et al. (2006) presented an approach which detects insider and outsider threat in SQL injection attack and the implementation was done in PHP [8]. Hasan Kadhem et al. (2009) proposed mixed cryptography to encrypt database [6]. Atefeh Tajpour et al. (2010) did a survey on all types of SQL injection attacks and prevention methods and evaluated all approaches [5]. Indrani Balasundaram et al. (2011) proposed a hybrid encryption (PSQLIA-HBE) to prevent SQL injection attack where they used AES encryption and RSA cryptosystem in the login and verification phase to make the authentication scheme more secure.

III. Work Done

Some predefined methods like quote block function, regular expressions, parameterized queries are used to avoid quotes and strings because their presence have important roles in SQL injection attacks. Especially in PHP, there are predefined codes using these methods to escape from SQL injection attacks [7]. So these are used in this project and for preventing greater exploitation encryption methods are used.

The model proposed by Indrani Balasundaram et al. is used in this paper also. The only difference is that here, Rabin cryptosystem is used instead of RSA cryptosystem as it is a good replacement to RSA. So, basically the system model is an adaption of previously proposed model. The system model includes three phases i.e. registration phase, login phase and verification phase.

1. In registration phase, a new user registers his/her name by selecting unique username and password and the data get sent to server and when server receives the username and password, it saves these information in the database in a table and along these data; server keeps a unique key for each username generated by the server itself. Then server sends back a confirmation request to the client.

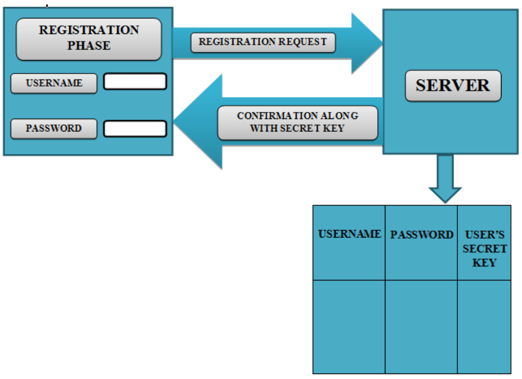


Fig 1: model of registration phase

2. In login phase, when a registered user tries to login, the username and password get encrypted by applying AES encryption algorithm which uses user's secret key. After that, a query gets generated automatically using the encrypted username and password. Then Rabin encryption is used to encrypt the query where server's public key is used to encrypt the query and once it gets encrypted it is sent to the server.

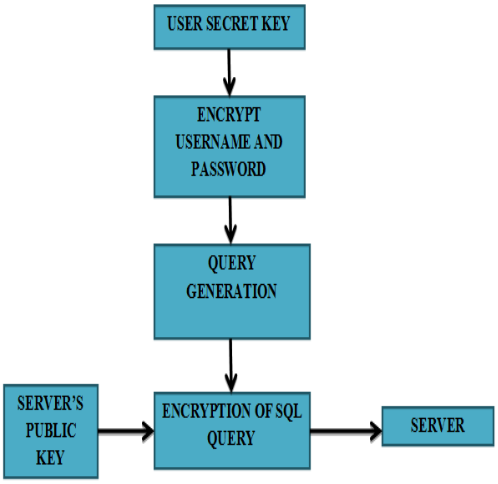


Fig 2: model of login phase

3. In verification phase, when server receives the query, it uses Rabin decryption method to decrypt the query where the server's private keys are used. Server then checks the username and password and again the username and password gets decrypted using AES decryption algorithm. After getting decrypted, if the username and password match to the database table, the login request gets accepted.

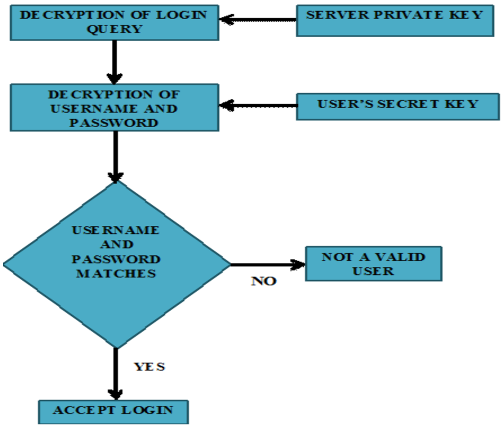

DECRYPTION OF LOGIN QUERY
SERVER PRIVATE KEY
DECRYPTION OF USERNAME AND PASSWORD
USER'S SECRET KEY
USERNAME AND PASSWORD MATCHES
NO
NOT A VALID USER
YES
ACCEPT LOGIN

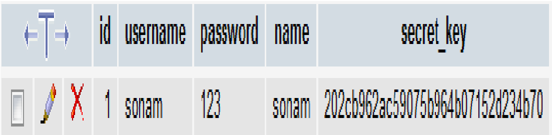
Fig 3: model of verification phase

A little more work is added i.e. after login, a user can search for the faculty's information. The faculty information contains the faculty name, employee id, school name, course title, time, date; slot etc. and one can search by the employee id to know about the information related to the id.

IV. Implementation

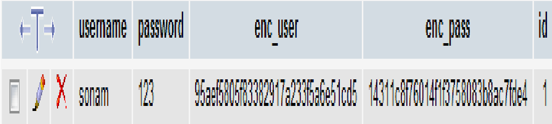
The whole implementation is done in windows operating system and the code is developed by using HTML, PHP and MYSQL. PHP has its own predefined commands such as 'mysql_real_escape_string' and 'stripslashes' which are used in this project. So first part of the paper includes a little survey based on predefined function. Net Beans IDE 7.0 and Wamp Server are used for the implementation.

In second part, the system model is an adaption of the model proposed by Indrani Balasundaram et al. (2011). They have implemented the model using core java but here PHP and MYSQL are used. In database, separate tables are there for AES encryption, Rabin encryption, Rabin decryption and AES decryption and all tables have a common column i.e. id. For example,



	id	username	password	name	secret_key
	1	sonam	123	sonam	202cb962ac59075b964b07152d234b70

Fig 4: Secret Key Generation after Registration



	username	password	enc_user	enc_pass	id
	sonam	123	95aef5805f83382917a233f5a6e51cd5	14311c8f76014f1f3758083b8ac7fde4	1

Fig 5: Sample Example of AES Encryption in Database

The third part consists of four tables i.e. school, faculty, course and slot. All these tables are connected to each other by primary key. So when user searches by giving any employee id, it retrieves the related information. This system is to provide information to students as well as teachers when they need.

V. Conclusion and Future Work

In this paper, various types of SQL injection attacks as well as predefined prevention methods are discussed. Then the hybrid encryption method is used which includes AES encryption and Rabin's cryptosystem. The reason behind the use of two layer of encryption is that it will be more secured. SQL query is generated and encrypted by Rabin's cryptosystem because even if hackers hack the information and decode the AES encryption part, it will still be more difficult for them to know about the encrypted query. Between Rabin and RSA, it is difficult to say which cryptosystem is better. So Rabin encryption is applied in this paper because it is a good alternative to RSA and in some cases Rabin is a little faster than RSA. This proposed method is an attempt to add some more security to databases to avoid SQL injection attack.

References

[1] Berhrouz A Forouzan et al., Cryptography and Network Security, New Delhi: McGraw-Hill

[2] Indrani Balasundaram et al. "An authentication scheme for preventing SQL injection attack using hybrid encryption (PSQLIA-HBE)" Euro journal publishing, 2011.

[3] XuePing-Chen "SQL injection attack and guard technical research" 2011.

[4] Varian Luong "Intrusion detection and prevention system: SQL injection attacks", 2010.

[5] Atefeh Tajpour et al. "Evaluation of SQL Injection Detection and Prevention Techniques" Second International Conference on Computational Intelligence, 2010.

[6] Hasan Kadhem et al. "A Novel Framework for Database Security based on Mixed Cryptography" Fourth International Conference on Internet and Web Applications and Services, 2009.

[7] Ettore Merlo et al. "Automated protection of PHP applications against SQL injection attacks" IEEE 2007.

[8] Ettore Merlo et al. "Insider and outsider threat sensitive SQL injection vulnerability analysis in PHP" IEEE 2006.