

Exhausting RC4 and Blowfish Encryption Techniques in Injection Attacks

Dr.P.Senthil Pandian

HOD-Department of Computer Science and Applications,
Farouk Educational Trust, Perambai, Villupuram District, Tamilnadu – 605110.

Abstract

SQL Injection Attacks (SQLIAs) are emerged nowadays as one of the most serious threats to the security of database-driven web applications. SQL injection attacks are one of the most critical vulnerabilities in web applications that software developers must address. The vulnerabilities can be harmful because they allow an attacker to access the database underlying an application. Using SQLIAs, an attacker may able to read, modify, or even delete database information. In many cases, this information is sensitive and its loss can lead to problems such as identity theft and fraud. In this paper, the problem of SQL injection attack is addressed using three different prevention mechanisms. The first technique allows single word inputs only by matching malicious symbols with the list maintained which can prevent almost all types of SQLIAs. The second one is the well-known parameterized query used to handle these types of attacks & the last technique makes use of RC4 and blowfish encryption mechanism instead of AES which will drastically improve the performance by encrypting the confidential fields in much less time as compared to AES encryption method.

Keywords- SQL injection; SQL injection detection; SQL injection prevention; Web application attacks.

I. INTRODUCTION

Internet is the huge basket of information which is widely used for communication. Sometimes, this communication channel becomes insecure for exchanging information and hence, the principles of information security are violated. These attacks not only make the attacker to breach the security and steal the contents of database but also to make changes and manipulate both the database schema and contents. No database is safe in web applications. Also, the dynamic web applications accept user inputs through parameters. Major threat to dynamic web applications are SQL Injection attacks (SQLIA). *An SQL injection attack occurs when an input from user contain SQL keywords so that dynamically generated SQL query changes the intended function of that SQL query* (MeiJunjin, 2009). In this attack, the attacker inserts a portion of SQL statement via not sanitized user input parameters into the original query and passes for example, a web application may invite the user to fill a form, post a comment, to submit a username and password for authentication. An attacker can enter the following input through user interface:

Username: 'OR 1=1--' AND Password: 'OR 1=1--'

This injected command would generate the following query:

SELECT user info FROM users WHERE id='1' OR 1=1--' AND password = '1' OR 1=1--';

Because the given input makes the WHERE clause in the SQL statement which is always true (a tautology) the database returns all the user information in the table. Lack of input validation in web applications causes hacker to be successful. Today, most of the web applications use a multi-tier design, usually three tiers: a presentation, a processing and a database tier.

The presentation tier in the HTTP web interface, and it displays information related to the data processing within the web application is done at the CGI tier. It can be programmed in various servers.

It implements the software functionality and the database users and the rejection of malicious users from the database. SQLI vulnerabilities and attacks occur between the Presentation tier and the CGI tier. Basically, the SQLIA process can be explained in three phases:

- i) An attacker sends the malicious HTTP request from a client to the web application as input.
- ii) Generates a SQL statement
- iii) Submits the SQL statements to the back end database server.

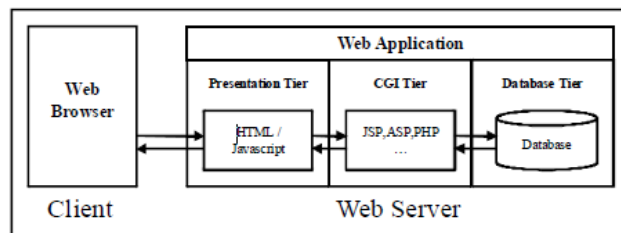


Fig. 1. Web Application Architecture

When an authenticated user enters its Username and Password, the Presentation tier uses the GET or POST method to send the data to the CGI tier. The SQL query within the CGI tier connects to the back end database and this paper is organized in five sections as follows. Section 2 presents the types of attacks. Related work of SQLIA detection and prevention techniques is discussed in section 3. Proposed technique is provided in section 4 and the results are shown in section 5. Finally, conclusion is provided in section 6.

II. TYPES OF ATTACKS

For a successful SQLIA, the attacker should append a syntactically correct command to the original SQL query.

Tautology

This type of attack represents to the SQL manipulation category in which attacker can inject malicious code into more than one conditional query statement to be evaluated always true. It is mostly used to bypass authentication. For example, in this type the queries are of the form:

*Select * FROM accounts where name = 'sonakshi' OR 1= 1 - -;* which gives all the rows as output because '1=1' is always true.

A. Illegal/Logically Incorrect queries

Here the intention of attacker is to gather information about the type and structure of back end database that is being used in web. These database error messages often contain useful information that allow attacker to find out the vulnerable parameter in an application and the database schema. This attack will return a default error webpage, which reveals important data. Mainly syntax errors are used to perform this attack. For Example: *Select * FROM accounts WHERE login='AND pwd='AND Pin = convert (int, (select table_name from information_schema.tables where xtype='u'))*. This is the mysql php syntax. Here, the attacker tries to extract the user table (xtype='u') from metadata table i.e. *tables*, after which the query is being converted to an integer, for that the system will throw an error because of illegal type conversion. The type of error message generated, will tell the attacker about the type of SQL Server being used.

B. Union query

This type of attack is mainly used to extract data. The output of this attack is that the database. Its format is; 'UNION SELECT < part of injected query>', where the query after UNION keyword is fully under control of the attacker so that he/she can retrieve data from any table. For example: *SELECT * FROM user WHERE id= '1111' UNION SELECT * FROM member WHERE id='admin' - ' AND Password= '1234'*; Injected query is concatenated with the original SQL query using the keyword UNION in order to get information related to other tables from the application.

C. Piggy-backed query

Here, the additional query is injected into the original one. As a result, database has to process multiple queries simultaneously. Database treats this query as two different queries which are separated using the delimiter (;). Normally the first query is legitimate query, whereas the following query could be illegitimate. Then the query will be produced as: *SELECT * FROM users WHERE id= 'admin' AND password = '1234'; DROP TABLE user;--;* Because of ";" character, database accepts both queries and executes them. The second query is illegitimate and can drop user table from the database.

D. Stored Procedure attacks

In this attack, the attacker tries to execute already present stored procedures in the database. Through this, the attacker identifies the current database being used, hence causing harmful effects. For example, Consider a SQL query; `SELECT id FROM users WHERE login= "+@Name+", and pwd= " + @passwd+" and pin= " + @pin+" ' .` To perform this attack, the attacker injects `' ; SHUTDOWN;`

E. Inference attacks

Here, the attacker observes the response of the webpage after injecting some malicious code into it. Usually this attack takes place when attacker cannot use the error messages generated by the database. "Timing Attacks" and "Blind Injections" are the two kinds of inference attacks techniques. These are as discussed as follows:

1) Blind Injection

The developers hide error details from the attackers, so that they won't get any help from the database. In this case, the attacker faces a generic page provided by developer, instead of an error message.

2) Timing Attacks

A timing attack lets an attacker, gather information from a database by observing timing delays in database responses. This technique makes the use of "if-then" statement which causes the SQL engine to execute a long running query or a time delay statement depending upon the logic injected. In time based attacks, attacker introduces a delay by injecting an additional `SLEEP(n)` call into the query. For example, `declare @varchar (8000) select @s=db_name()if(ascii(substring(@s,1,1)) & (power(2,0)))>0 waitfor delay '0:0:5'`

In the above query, database will pause for five seconds if the first bit of the first byte of the name of current database is 1. Then the code is injected to generate a delay in response time when the condition is true.

III. RELATED WORK

The researchers have proposed various methods to address the SQL injection problem and there are many solutions proposed in the literature. These are discussed below and it proposed an authentication mechanism to prevent SQL injection attack using Advance Encryption Standard (AES). In this method, encrypted username and password are used to improve the authentication process with minimum overhead. The method has proposed three phases, in the first phase i.e. *registration phase*, server sends a registration conformation. In the second phase i.e. *login phase*, user can access the database from server. The username and password is encrypted by using Advance Encryption Standard (AES) algorithm by applying user secrete key and the SQL query is generated using encrypted username and password. Then the query will be sent to server. In the third phase i.e. *verification phase*, server gets the login query and verifies the corresponding users secrete key. If they matches then the decrypted username and password is checked from user account table. If it matches, then user is accepted otherwise rejected and then it has given a model to block SQL injections which is based on verification information.

They have combined two approaches and created a new hybrid algorithm which works by applying the hash code with encryption for more security. In this approach, two extra columns are needed, one for storing the hash values of username and another one for storing the hash values of password.

When the account of users is created for the first time, the hash values are calculated and stored in user table. The hash values are calculated at runtime using stored procedure when user logs into the database. The values which are calculated at runtime are matched with stored hash values in database table. Thus, if user tries to inject to the query, the proposed method will automatically detect the injections as malicious content & rejects the values. Therefore, it cannot bypass the authentication process. Its advantage is that hackers do not know about the hash value concept. A similar approach to protect web applications against SQL Injection in which the authors has discussed some predefined methods and also proposed an integrated approach of encryption method with secure hashing. The technique works by creating two columns by DBA for storing username and password in the same way. The secure hash values are generated at runtime using stored procedure if a user wants to login to the database. These values are stored in login table when the user's account is created first time. If a user wants to login to the database, his/her identity is verified via username, password and secure hash values.

IV PROPOSED METHOD

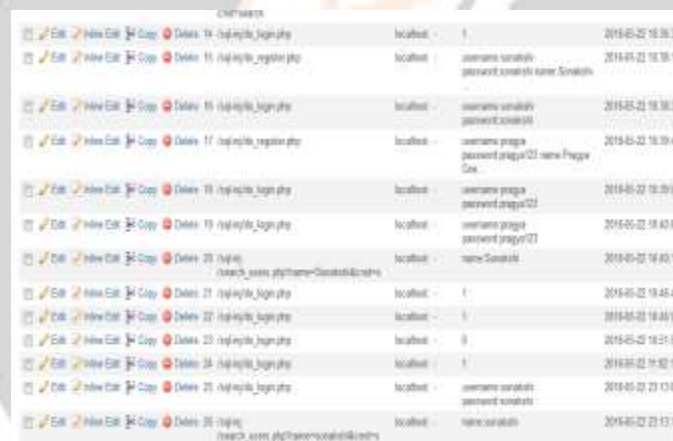
On studying the various SQL injection prevention techniques, a new technique is proposed in this paper for preventing the database against SQL injection attack. In the proposed approach, the security is provided in three different phases, such as:

1) *Input Validation using query tokenization and log maintenance at login phase*

At the login phase, user is allowed to enter single word instead of multi-words which is the basic cause of SQL injection attacks. By the use of single word, possibility of attack is reduced to minimum. In this way, malicious activity is detected if a user enters username or passwords using multi-words e.g. 'OR 1=1-'. In this example, there is a space after "OR" so, it is treated as multi-word input. Almost all types of SQL injection attack types are prevented by allowing single word input only. At the same time, the input is tokenized, and list of various known malicious symbols or tokens are maintained in a log file.

The validation process at login phase checks the entered input and matches it with malicious known symbol list. If a match is found, then further access is restricted and that user is considered as malicious one. In the proposed scheme, the IP address of malicious user's system along with date, time and page of application from which the entry is made is saved for future reference.

It will help to keep a check on malicious activity in future as well. System will continuously observe user's login detail and compare it with saved database and looks for particular IP address who has visited the page given number of times & if found to be malicious is blocked for further access. The input entered by users is stored in logs table as shown in fig. 1 below.



| IP Address | Location | Username | Password | Timestamp |
|-------------|-----------|----------|----------|---------------------|
| 192.168.1.1 | localhost | admin | admin | 2018-05-22 18:38:33 |
| 192.168.1.1 | localhost | admin | admin | 2018-05-22 18:38:31 |
| 192.168.1.1 | localhost | admin | admin | 2018-05-22 18:38:32 |
| 192.168.1.1 | localhost | admin | admin | 2018-05-22 18:39:40 |
| 192.168.1.1 | localhost | admin | admin | 2018-05-22 18:39:37 |
| 192.168.1.1 | localhost | admin | admin | 2018-05-22 18:40:00 |
| 192.168.1.1 | localhost | admin | admin | 2018-05-22 18:40:12 |
| 192.168.1.1 | localhost | admin | admin | 2018-05-22 18:40:47 |
| 192.168.1.1 | localhost | admin | admin | 2018-05-22 18:40:59 |
| 192.168.1.1 | localhost | admin | admin | 2018-05-22 18:21:00 |
| 192.168.1.1 | localhost | admin | admin | 2018-05-22 18:32:17 |
| 192.168.1.1 | localhost | admin | admin | 2018-05-22 18:13:08 |
| 192.168.1.1 | localhost | admin | admin | 2018-05-22 18:13:14 |

Fig.1. Log entries of users is stored in logs table of database

Use of Parameterized queries

Using dynamic SQL queries is the root cause of SQL injection vulnerability. OWASP also recommends the use of parameterized queries as the first choice of prevention techniques for this vulnerability (Infosec Institute). A dynamic query directly uses user's input into the query. While the SQL Parameterized Query forces the user to implement the logic of SQL query first and then inserting the user input values into it.

This forces the SQL query to be built before entering any user input in it. The SQL query is sent as a query, and the database knows exactly what this query will do, and only then it will insert the username and passwords as values. This means they cannot affect the query, because the database already knows what the query will do. So in this case it would look for a valid username and password not the malicious values.

They takes less time to encrypt the same lines of input if is done with AES algorithm. Another advantage is, RC4 algorithm is also symmetric i.e. the same key is used for encryption & decryption which takes less storage space to store a single public key. The process works by encrypting the user's registration & login details using RC4 algorithm or blowfish at backend. Whenever a new user registers his account, a unique secret key is generated and stored. At the time of login, the generated secret key is matched with the stored one, if a user is valid only then

his/her information is decrypted otherwise it is present in encrypted form on backend server so that attacker cannot understand the exact data values.

Fig .2.Login form

In the above Fig. 1, the user has tried to login through injection, so if user tries to read the password of any other user through search page then he won't get succeed because the password is present in encrypted form at backend. The same can be seen in figure 2.

| Id | Username | Password | Name | Email | Mobile | Gender |
|----|----------|----------|------------|--------------------|------------|--------|
| 5 | praga | #,Dior5E | Praga Goel | praga123@gmail.com | 9876543210 | Female |

Fig.3. Encrypted password values at backend

V IMPLEMENTATION AND RESULTS

As an instance, a text file of size 5 KB approximately, is read, and its encryption and decryption time is noted corresponding to AES encryption algorithm, RC4 and Blowfish algorithm respectively in table 1 given below. Also, it can be seen in graph 1 which shows blowfish has least time complexity among all three encryption algorithms.

TABLE I. Encryption, decryption and total time

| Algorithm | Enc. Time(sec.) | Dec. time(sec.) | Total time (sec.) |
|-----------|-----------------|-----------------|-------------------|
| AES | 0.499 | 0.494 | 0.993 |
| RC4 | 0.048 | 0.031 | 0.079 |
| Blowfish | 0.002 | 0.002 | 0.004 |

The graph 2 shows the total time taken by all the three encryption algorithms given in table 1. Clearly, it can be seen that AES takes the more time to encrypt and decrypt the input fields than RC4 and blowfish algorithms.

CONCLUSION

The paper presented a novel and applicable technique for protecting web applications from SQLIAs. The approach consists of allowing single word user inputs only, that will automatically eliminate all sources of attack vulnerabilities.

The next approach used is Rc4 and blowfish encryption methods which will enhance performance due to their less time complexity. AES is very complex encryption standard while RC4 is very old and simple. Both RC4 and Blowfish are faster in performance as compared to AES technique. Since, the technique is developed at application

level, it requires no modifications in the existing runtime system and imposes less execution overhead to reduce SQL injection attacks almost in every way.

REFERENCES

1. Marzi, H. and M. Li, 2018. An Enhanced bio-inspired trust and reputation model for wireless sensor network. pp.1159-1166.
2. Prasuna, A. Valarmathi and Selvi, 2018. Finite state Markovian model for trustworthy reliable communication in dynamic Reconfigurable Wireless Sensor Network architecture. In Emerging Trends in Engineering, Technology and Science (ICETETS), International Conference.
3. Karthik, N. and V.S. Dhulipala, 2019. Trust calculation in wireless sensor networks. In Electronics Computer Technology (ICECT), 2019 23rd International Conference.
4. Liu, Zhaoyu, Anthony W. Joy and Robert Thompson, 2019. A dynamic trust model for mobile ad hoc networks. Distributed Computing Systems, 2004. FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends of. IEEE,
5. Mármol, F.G. and G.M. Pérez. 2019. TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks. Communications, 2019. IEEE, 2009. pp.1-5.
6. Ganeriwal, S. and M.B. Srivastava, 2020. Reputation- Based Framework for High Integrity Sensor Networks. In Proceedings of ACM workshop security of ad hoc and sensor networks, pp: 66-67.
7. Yao, Z., D. Kim and Y. Doh, 2020. PLUS: Parameterized and localized trust management scheme for sensor networks security. In Proceedings of third IEEE international conference on mobile adhoc and sensor systems, pp:437-446.
8. Boukerche, A., X. Li and K. EL-Khatib, 2020. Trustbased security for wireless ad hoc and sensor networks. Computer Communications, pp.2413-2427.