A Study of SQL of Injections Techniques and their Prevention Methods

Yash Tiwari
MS Software Engineering
Vellore Institute of Technology
Vellore

Mallika Tiwari
B-Tech Computer Science
Graphic Era University
Dehradun

ABSTRACT

Rapid evolution of technology and increasing necessity of storing data and securing it as well gave rise to various techniques to secure it along with the new innovative malicious techniques to have a hazardous impact on the organization by wrecking the database and manipulating data. In this paper we have presented various techniques that are being used by such attackers called sql injections and their prevention methods these attacks are targeted towards web applications using databases and are injected through the input fields meant for taking information such as username or password. Such codes injected combines with the already present sql code and form a query that solves the purposes of the attacker if vulnerable to such attacks.

General Terms

Cyber security, authentication, forge identity.

Keywords

Sql injection, data security, inference, tautology.

1. INTRODUCTION

In the modern era computers and information have a big impact on our lives. Everyday staggering amount of data is added to the databases worldwide. Escalating numbers of users and their increasing dependency for the digital information and communication is a proof how important securing the information is. Thus with the advancement in useful technology the rise of the malicious and destructive data is no exception. One of the major threat to the information stored in databases is called sql injection. In this paper presentation of various types of vulnerabilities and techniques of sql injection are presented along with their prevention methods.

2. SQL INJECTIONS

SQL a structured query language is a standard language chosen for relational databases is used for defining and structuring databases along with its manipulation. Most dialects that are being used today are partially based upon SQL-92.

SQL injection is a series of sql statements which are given as input to the application and along with the 'query' in the application the sql statements behave differently which may have hazardous results.

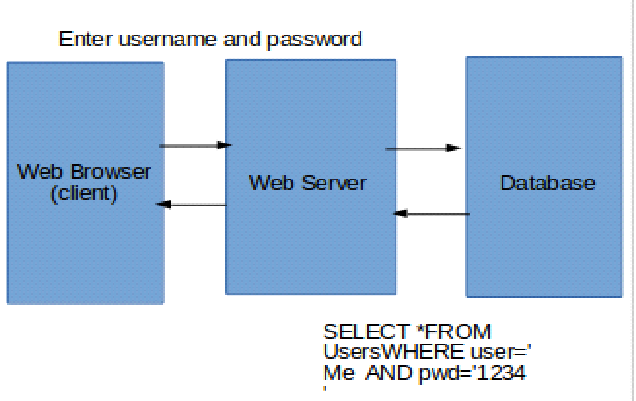
Enter username and password
Web Browser (client)
Web Server
Database
SELECT *FROM UsersWHERE user=' Me AND pwd='1234 '

Fig 1

2.1 Consequences of Injection

The code injected in the application can manipulate the information and structure of the database by using just few statements. Being common and efficient technique it is very important for the developers and administrators to consider it a major concern. The injection can delete insert data.

It can forge user identity and commit crimes. In many cases the entire data is manipulated resulting in database shutdown and huge loss of time and money.

3. TECHNIQUES AND PREVENTION

There are many ways of implementation of sql injection which are adopted by the attackers depending on their desired result.[1]

3.1 Tautology

[2][3][4]

The database authentication work on the basic principle of authentication in which the input is matched with the information in the database but if instead of authentic input some conditional statements are given which will always result in a true value and the authentication gates are bypassed thus this technique is called tautology. This method can also return some information which can be used in further attacks.

For example:

Let’s suppose the developer wrote the username query as

select name from users where name='user' and password='pasdwd';

and in the username field if the input be given as (' OR '1'='1) which will always be true.

The input will behave as select name from users where name=' 'OR '1'='1' and password=' 'OR '1'='1' ;

Such attacks can be prevented by input validation, by checking the type,size,format and range and not letting the input bypass the authentication.

For example, by giving the error “Password field can not be left empty” in case when the attacker uses tautological statements in the passoword field.Parameterised queries can be used instead of injecting the values directly into the command..

3.2 Interference

[5]
When the structure of the database or the information is needed which can be used for further attacks inference technique is used which tends to be more hazardous. The basic principle of inference is to inject the code in order to get some error which contains the data needed for the further process. Inference attacks are based on the conditional statements.

For example::

Malicious parameter (inference attack on SQL Server).

1; IF SYSTEM_USER='systemadmin' SELECT 1/0 ELSE SELECT 6

Query generated (two possible outcomes for the injected IF).

SELECT name, email FROM members WHERE id=1; IF SYSTEM_USER='systemadmin' SELECT 1/0 ELSE SELECT 6

If error is thrown by the database that shows the database is run by the system adminitrator i.e 'sa'

Some times by using the delay of response from the database is also used for gathering information which is called 'timing attacks'.Such attacks can be prevented using the functions that validates the input and scan for the terms like 'insert','delete',drop','update' as these terms are commonly used for sql injections.Comment delimiter like '--' must be scanned and eliminated and banning the ip temporarily can be useful in defending the application against attacks.

3.3 Injecting Union Query

[6][7]
Union statements are used for returning information from two different tables and its not necessary for the selected columns to be of the same data type.

For example 2,

' UNION SELECT name, type, id FROM objects;--

The '--'can comment out the rest of the sql code and apostrophe in the beginning closes the quote in the SQL statement. This may show the attacker the names of the objects used and their types, the attacker may know the table name and further use it.

For example 1:

SELECT SALARY_INFO from members where

username=’’ and password=’’ UNION SELECT

BASIC_INFO from memberswhere member_id=’29012;

The query will return the basic information of the member with the id=29012 ,the union query contains set operators and the main query is resulting Null value.

Such attacks can be prevented by setting maxlength in the fields to set a restriction in the number of characters to be used and encrypting information. Using stored procedures which can validate input and allow the password to pass in but it will not allow it to be in any result set. Stored procedures should be well written as they may cause potential harm if the code is buggy.

3.4 Stored Procedures

[7]
Databases contain defined stored procedures which triggers events according to the condition. The attacker injects malicious codes which triggers the stored procedures according to their desired result.

For example, using 'shutdown' may trigger the database to shutdown.

It is very important to validate the input properly before any processing in the database as stored procedure being helpful in defending database can also prove to be fatal to it.

3.5 Piggy Bagged Query

[8][9][10]
In this kind of attack queries are added to the original query and vulnerable database receives and executes a query which consists a number of other queries with different function. The first query is legal one and the appending queries are the code that is injected for malicious activity. With this method most of the functions can be implemented thus making this technique a fatal move.

By using the techniques mentioned above the attacker can gain important information like username and by forging identity and using piggy back method the password field of the authentication page can be filled using query

pass = ' OR (SELECT COUNT(*) FROM member)=10 AND "='

and along with the pre defined query the statement will be completed as

select name from members where name=’member1’ and pass= ‘= '

OR (SELECT COUNT(*) FROM members=10 AND ' '=’ ‘ ;

After many hit and trials the attacker can know the number of users in the database also the data can be inserted using 'insert into' clause if the query results the value 'true’. For such attacks the formation of proper functions which can scan and eliminate malicious code having suspicious terms .Encrypting the data and not letting it show in any result is a smart choice.

3.6 Alternate Encoding Technique

[10][11][12]
In some cases attackers inject hexadecimal,ASCII and unicode character encoded texts and bypass the well defensed system. The techniques for preventing the injections are not always useful in the case of alternate encoding.

For example:

SELECT * FROM members WHERE login= " AND pass=' ';exec(char(Ox73687574646j776e)) '

The char() function used returns the actual characters of encoding of characters. This encoded string is interpreted by the database as the shutdown command.

4. CONCLUSION

A number of injection techniques are reviewed along with the methods to prevent them. Data security is an important issue and by the use of proper techniques like encryption of the data, accessing the database using an account with as less privileges that are necessary and assurance of data validation with proper use of stored procedures and parameterized queries and using ORM framework can secure the data from the intruders.As data security is a major concern for every organization it is as important as any other thing envolved in the development of products and organization.Every threat has a prevention method and by using advance engineering skills and proper understanding of the possible threats computers and the information can be secured from the attacks.Better database design,intelligent queries and using advance detections gives better security and can handle the major threat of sql injections.

5. FUTURE WORK

The usage of automated injecting bots are very much common and more sophisticated and complex techniques are being evolved by the attackers giving technology a chance to evolve the defensive techniques. With our research and survey of the techniques used for injecting malicious codes and by reviewing their defensive techniques its observed that by securing the query language by innovation of defensive database design and implementation of the schema in a more secured way.

There is a good chance that a design can be evolved which doesn't have the loopholes like the traditional schema and which won't need injection preventive techniques. As there are a number of combination of injection techniques which are hazardous and as the time is passing the need of securing data is increasing and data security has become our major concern.

6. REFERENCES

[1] Atefeh Tajpour, Maslin Massrum and Mohammad zaman Heydari."Comparison of SQL Injection detection and prevention techniques," in proceeding of 2nd international conference on education technology and computer(ICETC)

[2] C Anley. Advanced SQL Injection in SQL ServerApplications. White Paper Next Generation Security Software Ltd., 2002. http://www.nextgenss.com/papers/advanced sql injection.pdf

[3] M. Howard and D Le Blane. Writing Secure Code. MicrosoftPress, Redmond, Washington, second edition, 2003.

[4] S.McDoland. SQL Injection. Modes of Attack, defence andwhy it matters. White paper, GovernmentSecurity.org, April 2002.

[5] Asha. N,M. Varun Kumar,Vaidhyanathan.G of Anomaly Based Character Distribution Models in the,"Preventing SQL Injection Attacks", International Journal of Computer Applications (0975 – 8887) Volume 52– No.13, August 2012

[6] A brief introduction for sql injections and vulnerabilities are described in the website of W3resources. http://www.w3resource.com/sql/sql-injection/sql-injection.php

[7] C. Anley. Advanced sql injection in sql server applications. http://www.nextgenss.com/papers/advanced_sql_injection.pdf.

[8] Xiang Fu, Kai Qian. SAFELI-SQL Injection Scanner Using Symbolic Execution. Proceedings of the 2008 workshop on Testing, analysis, and verification of web services and applications. ACM(2008).

[9] S. W. Boyd and A. D. Keromytis. Sqlrand: Preventing sql injection attacks. ACNS, 2004.

[10] Y. -W. Huang, S. -K. Huang, T. -P. Lin, and C. -H. Tsai,"Web application security assessment by fault injection and behavior monitoring," in Proceedings of the 12th international conference on World Wide Web,ser. WWW'03, 2003, pp. 148–159.

[11] Diallo Abdoulaye Kindyand Al-Sakib Khan Pathan,"A survey on SQL injection:vulnerabilities,attacks and prevention techniques," in 2011 IEEE 15thinternational symposium on consumer electronics.

[12] M. Howard and D. LeBlanc.Writing Secure Code. Microsoft Press,Redmond, Washington, second edition, 2003.