Recursively Accrual Authentication of Web Application against SQL Injection Attack

Raut S.P.
Asst. Prof
Dattakala Faculty of Comp. App.
Bhigwan, Pune, India

ABSTRACT

Web applications allow legitimate website visitors to submit and retrieve data to/from a database over the Internet. Web applications are used for collecting information, and analyze it. Sql injection is one of the most dangerous attacks which are used to access database without authentication. SQL is used to retrieve; insert data to/from the database .Using sql command make it a malicious code for attack at authentication section of front end of web application and send to the server. This process is known as SQL injection authorization attack.SQL injection authorization attack easily gets entry in the database and catches all information from database.

This paper illustrates the method for prevention from SQL injection authorization attack i.e. recursively authentication or double authentication. Automatically authentication will increase. We are going to implement recursive method on web based program using string inputs and its ASCII value

General Terms:

Web application, authentication, and Increase authentication

Keyword:

ASCII, recursive authentication, double authentication

1. INTRODUCTION:

SQL injection is a technique often used to attack data driven applications. [1]This is done by including portions of SQL statements in an entry field in an attempt to get the website to pass a newly formed rogue SQL command to the database. [2]Here we have SQL command for retrieving information from database and also insert, delete information .It is a common process of user authentication in login form. Change the logic of original one and put some extra logic from self in SQL statement. If tautology is giving result true then automatically control, goes to database tier.

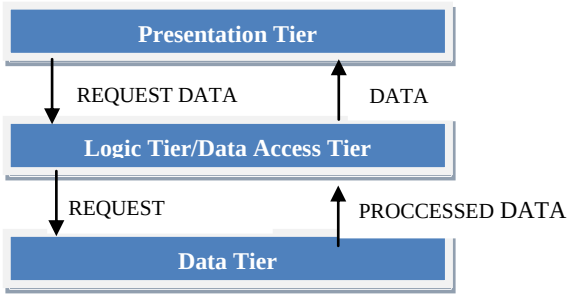

Fig.1: Client Server Architecture [4]

Above diagram shows the client server three tier architecture. In presentation tier prepare and send query which is received by logic tier. In logic tier/Data Access process on this query and send to data tier. Data tier send back response to logic tier /Data Access then logic tier will send presentation tier.[3]Use of SQL injection technique malicious query send to logic tier but due to malicious code Logic tier will confuse and he will access Data from Data Tier.[5].This type cannot detect to firewall, other security software's.[6]This concept is known as SQLIA (SQL Injection Attack).SQLIA is caused due to insufficient validations; lack of control of SQL query as well as lack of coding techniques. We need increase coding technique as well coding quality for best performance.

2 .PROBLEM OF AUTHENTICATION

Login page is mostly used for authorization of particular web application. Whenever you have logged in successfully you will go to next page otherwise it will give error message 'invalid credential'.

We have one table names as users. We have two fields username and password. Use of this field authenticate to coming request. (See figure 2)

user_name	user_pass
Sandesh	raut
pranav	kulkarni
sandip	kadam

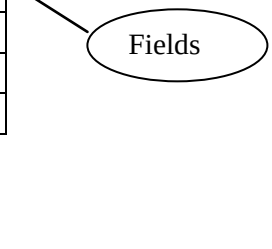

Fig.2: user table with data

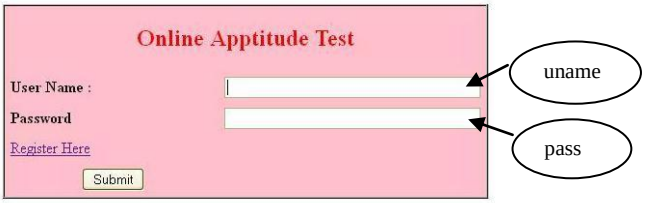

Fig.3: Simple login form

Above figure shows the login form for online aptitude test and having two fields uname and pass and working at presentation layer. Then send uname and pass to logic tier for processing with query.

```
$result =mysql_query ("SELECT * FROM users
WHEREusername='$_POST [uname]' AND password='$_POST[pass]'");
```

Fig.4: SQL Query for check authorization

If result of above query is true then user is authenticated otherwise query will be denied. Suppose entering user name

and password is like:

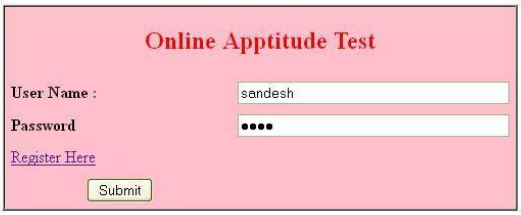

Fig.5: SQL Query for check authorization

Then query will be like this:

```
$result =mysql_query("SELECT * FROM users where
username='sandesh' AND password=’raut’");
```

User sandesh will be authorized because username is sandesh and password is raut in table; but malicious attack is received from application layer by entering code through SQL i.e. SQL Injection return always true query because of tautology.

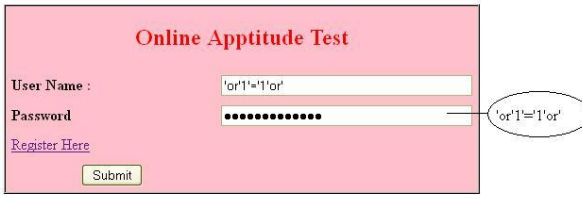

Fig.6: Malicious code with login form

```
$result =mysql_query("SELECT * FROM usersWHERE
username=’’or'1'='1'or''AND password=’’or'1'='1'or'');
```

Fig.7: Malicious code of SQL query

Whenever we analyze the above query result is always true because of the tautology. See highlighted area of figure 7, WHERE clause username is null with OR clause .In OR clause tautology is used ‘1’=’1’ always return true result. And password also return true because of ‘1’=’1’ will true. In OR condition at least one condition must be true.

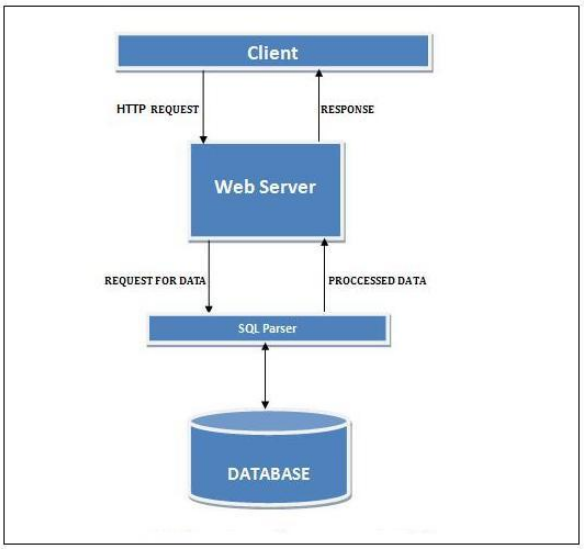

Fig.8: Single Authentication Method

Above figure shows the single authentication method .Here query is requested from html form and request is send to web server and then web server convert in sql and sql parser get appropriate data, but this is single authentication .If he break authorization then any one can access Database . So we have here a new technique called as double authentication or recursive authentication.

3. RELATED WORK

Different techniques have been invented for controlling SQL injection attacks. [7]San-Tsai Sun, Ting Han Wei, Stephen Liu, Sheung Lau have classified different type of attacks. But we are going to concentrate on bypassing authentication. This paper illustrates bypassing authentication. We have to need username and password. By pass authentication is used for unauthorized access to database. [8] Asha. N, M. Varun Kumar, Vaidhyanathan.G proposed two levels at database level of authentication. Same query request to evaluate by all different SQL based database. In this paper if one sql request is to evaluate will be true then same request to evaluate will true on all other database. Database security protection is based on new mechanism.[9] This paper shows that one model who has dived into two component first component check authorization and then find out intrusion came or not .if it is then alarm will raised otherwise query will execute. This method proposed by AmiraRezk, H. A. Ali, S. I. Barakat. [10] Here we have another given byNikita Patel, Fahim Mohammed,SantoshSoni illustrate categories of sql injection attack like predefined choice, blind variables mechanism, Parameterized statement, input validations. We are using GET method in form then prevention fails because of entering malicious query directly in URL (unified resource locator).

Fig.9: SQL Injection attack through address bar

[11]IndraniBalasundaram,E. suggest mechanism to prevent sql injection attacks. This paper illustrates the authentication process using secret key. This paper shows three phases i.e .registration, login and verification. In registration phase

username, password will be created with its secret keys. In login phase username, password encrypted using advance encryption standard algorithm by applying user secret key. And last verification phase whenever server receive request for username and password then he will match username and password with secret key.

4. PROPOSED TECHNIQUE

Whenever user request to web server for authentication and then web server access data from database but we have one problem with single authentication is that when request send to web server using SQL injection (String input) then web server conflict from string because tautology has been used in single authentication method but we are introducing new technique that is **Recursive authentication or Double authentication.** In this method we have two different modules.

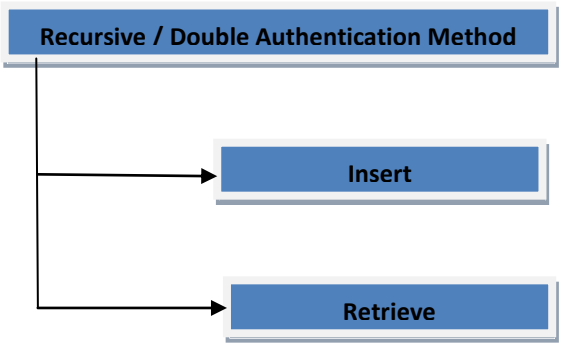

Fig.10: Modules of Recursive Authentication or Double Authentication

Before we start this method we must rebuild user table like this (see figure11 and 12)

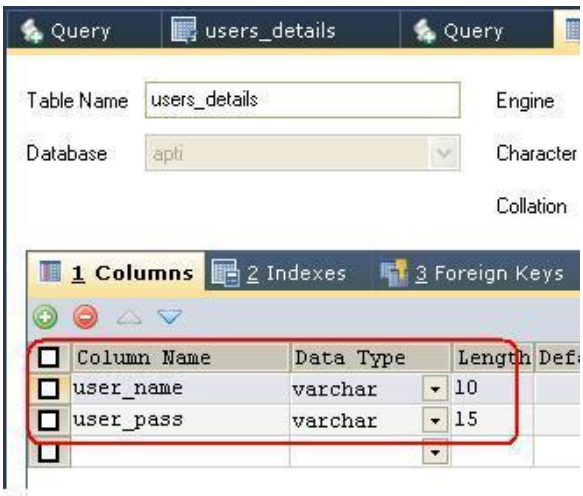

Fig.11:user table

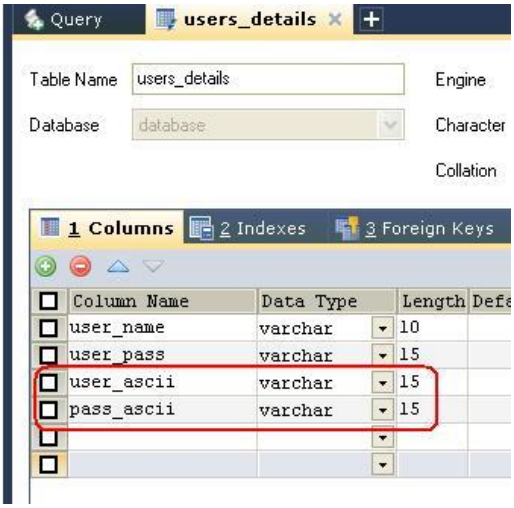

Fig.12: Rebuild user table

The above two diagram (Figure 11 and Figure 12) shows that user table and extended user table respectively. The user table is having only two field i.e. user_name and user_pass using two fields. We have to identify authorization of user. In another approach two more fields should be added i.e. user_ascii and pass_ascii for username and password fields respectively (see figure 12).

Let's go back to recursive authentication module. As we know that every letter, symbol, digit etc. have their ASCII value. Earlier you had used simple text name and text password for authentication. But new approach 'Recursive Authentication method' use ASCII values for user authorization. on the basis of ASCII value we are going to show Architecture of 'Recursive Authentication Method / Double Authorization Method'.

In insert module whenever we register username at web server get ASCII value of every character in username and password value then all ASCII values which came from username add with each other and insert into user_ascii field. Then with password field does like username field .Count ASCII values from password field then add with each other and insert into pass_ascii field. ASCII value calculate using ord inbuilt function in PHP.

In retrieve module web server follows below architecture:

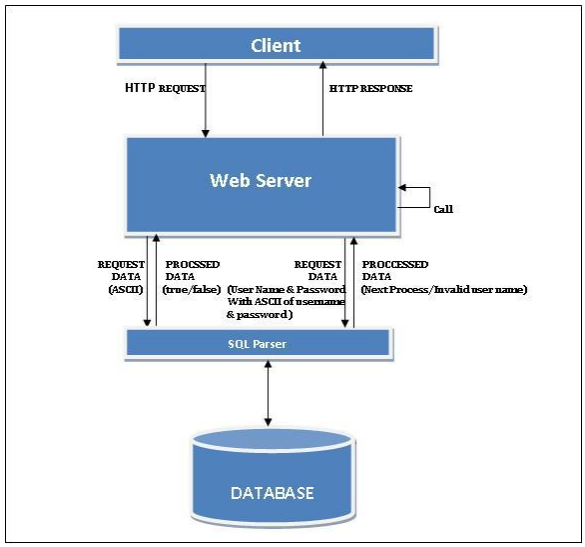

Fig. 13: Architecture of Recursive/ Double Authentication Method

The above architecture shows the' Recursive Authentication Method. In this method certain steps will be created:

A. Client request to web server for user authentication
B. Web server get value from client request
C. ASCII value will be prepare taken from client.(using inbuilt function)
D. Send to database for identifying of that ASCII which is get in STEP C
E. If ASCII value found of username and password in database then return true otherwise false(It's a first call)
F. If STEP E will true then find out the user from the database using username field value, password field value, user_ascii and pass_ascii (user_ascii and pass_ascii calculated STEP E)(This is second call)
G. If STEP F will true then execute STEP I
H. If STEP E will return false then execute STEP J
I. Give appropriate positive response
J. Give negative response

Above we have seen step of 'Recursive / Double Authentication'. Step no E and Fare called first call and second call respectively. First web server calculates ASCII values of username and password field and then finds out that ASCII values present in database .If it is true then it find s username and password of ASCII values ofuser_ascii and pass_asciiusing username field value, password field value, user_ascii and pass_ascii .Otherwise it gives negative response.

5. CONCLUSION AND FUTURE SCOPE

Authentication is major concept in accessing database. Mostly authentication is done using username and password. My paper conclude that user authentication process should do Recursive authentication or Double authentication User verified double i.e. username and password and its ascii values.

But we should improvement in future of this authentication process. When we want to access database then we must provide username and password. This authentication has done using recursive authentication method but when entering in application/website some attackers attack on application or websites using some technique. So we need more authorization power when website or application is going on.So,I should implement some technique of recursive authentication method in application or websites

6. REFERENCES

[1] HTTP://http://en.wikipedia.org/wiki/SQL_injection; "SQL Injection"

[2] William G.J.,Halfond and Alessandro Orso.2005,ASE'05,Long Beach, California, USA,AMNESIA: Analysis and Monitoring for Neutralizing SQL Injection Attacks

[3] IndraniBalasundaram.,Dr. E. Ramaraj.2011.An Effective Approach for Protecting Web from SQL Injection Attacks. IJCSNS International Journal of Computer Science and Network Security

[4] Multitier Architecture http://en.wikipedia.org/wiki/Multitier_architecture

[5] VeeraVenkateswarammaP.2012.An Effective Approach for Protecting Web from SQL Injection Attacks. International Journal of Scientific & Engineering Research

[6] William G.J. Halfond and Alessandro Orso. Combining Static Analysis and Runtime Monitoring to counter Injection Attack

[7] San-Tsai Sun, Ting Han Wei, Stephen Liu, SheungLau.Classification of SQL Injection Attacks

[8] Asha. N, , M. Varun Kumar, Vaidhyanathan.G.2012 Preventing SQL Injection Attacks.International Journal of Computer Applications.

[9] AmiraRezk, H. A. Ali, S. I. Barakat.2012. Database Security Protection based ona New Mechanism. International Journal of Computer

[10] Nikita Patel, Fahim Mohammed, SantoshSoni.2011 SQL Injection Attacks:Techniques and Protection mechanismsInternational Journal on Computer Science and Engineering (IJCSE)

[11] IndraniBalasundaram,E.Ramaraj.2011.An authentication Mechanism to prevent SQL Injection Attacks. International Journal of Computer Applications