Asian Journal of Information Technology 7 (8): 332-336, 2008
ISSN: 1682-3915
© Medwell Journals, 2008

Web Programming Practice to be Protective from SQL Injection

Thawatchai Chomsiri
Faculty of Informatics, University of Mahasarakham, Mahasarakham 44150, Thailand

Abstract: Growth of the internet has enabled many organizations to connect to the internet and also publish their web-site. There are great number of web-sites, which have a login form and possible infected security hole. Hackers can use the SQL injection technique to steal confidential data from web-servers, database-servers and other server; they can deface home-pages and/or control a server across the internet. This hole occurs from careless programming in CGI, ASP, PHP and JSP. Hacking using SQL injection cannot be protected against by firewall. This study proposes a method to be precedence in web programming with no hole, we present an approved solution that can completely protect against SQL injection; can be used as a formal tool to develop web programs with high security and leads to improve mend overall security levels on network.

Key words: SQL injection, hack, protection, web, programming

INTRODUCTION

Web services can be programmed using several script languages such as ASP, JSP, PHP and CGI. Many Web Application may be have input form (Fig. 1) for user can be send data from Brower to Web Application, input form is a channel for user can be input username and password to access system, or sometime they can use search-box for search data on web site. Web Programmer, which have a lack of knowledge on Web Security may be generate weak the Web Security; it's can open for hacker to use SQL injection (McClure *et al*., 2002) method to access system or damage data, for example, by pass authentication, illegal access to database, steal confidential data files, added unknown user to system and access to remote access to control server from anywhere. Hacking using SQL injection use port number 80 or 443, it's cannot protect by firewall.

SQL INJECTION BACKGROUND

In every member system, normally administer add member data to database, such as Oracle, SQL Server, MySQL and MS Access. When any users want to log into system, they must be use authenticate form (Fig. 1) for input correctly user name and password. Normally the form coding by HTML tag (Kurose and Ross, 2007), an example of code such as shown:

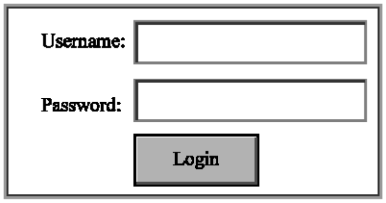


Fig. 1: Login form

```
<CENTER>
    <TABLE BORDER="1" CELLSPACING="0"
CELLPADDING="2">
    <TR><TD>
    <TABLE WIDTH="100%" BORDER="0" CELLSPACING="0"
CELLPADDING="2">
    <FORM ACTION="login.asp"
METHOD="post">
    <TR>
    <TD ALIGN="right">Username:</TD>
    <TD><INPUT TYPE="text" NAME="username"
SIZE="15"></TD>
    </TR>
    <TR>
    <TD ALIGN="right">Password:</TD>
    <TD><INPUT TYPE="password"
NAME="password" SIZE="15"></TD>
    </TR>
    <TR>
    <TD>&nbsp;</TD>
    <TD><INPUT TYPE="submit"
VALUE="LOGIN"></TD>
    </TR>
    <INPUT TYPE="hidden" NAME="VIEW"
VALUE="SQL">
    </FORM>
    </TABLE>
    </TD></TR>
    </TABLE>
</CENTER>
```

Login form will receive values username and password and a button, we click button went want to login into system, on click form will be pass values username and password to authentication system to

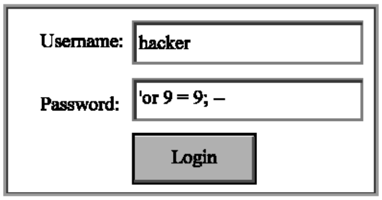

Username: hacker
Password: 'or 9 = 9; --

Fig. 2: By passing the authentication

Server Side Script (Forouzan, 2004), Such as ASP, CGI/Perl or PHP. Normally programmer code easy programming for get username and password to a part of SQL command and then pass to Database Server for searching data. In several Server Side Script coding such.

```
SQLQuery = "SELECT * FROM tbl_Users WHERE Username = ' " &
        strUsername &" ' AND Password = ' " & strPassword & " ' "
strAuthCheck = Get QueryResult (SQLQuery)
If strAuthCheck = " " Then
        boolAuthenticated = False
Else
        boolAuthenticated = True
End If
```

Programmer sometime coding a part of SQL login command Inline Script, as put all together it is complete SQL login command. That mean SQL login command is searching data from table of tbl_Users and field name is Username same as variable strUsername and field name is Password same as strPassword, after found data variable strAuthCheck will get data user but if not found (sometime come from not have user that specify or input wrong data) value in strAuthCheck will be get empty value, such it will be know authenticate pass or not.

By passing the authentication: As Input Form and Programming that introduce passed if we do not input value to form in both username and password, SQL login command from Server Side Script will put together values are

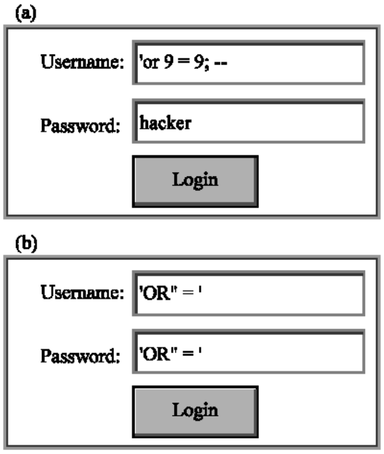
```
SELECT * FROM tbl_Users WHERE Username = ' ' AND Password = '
'
```

To show normally Login we input Username is somsri and Password is SuperGirl produce after Server Side Script brings both values put together prepared SQL command and SQL command such as.

```
SELECT * FROM tbl_Users WHERE Username =
  'somsri' AND Password = 'SuperGirl'
```

Hacker can be by pass authenticating (McClure *et al.*, 2005) by input SQL command such as in Fig 2.

When input data like Fig. 2 by SQL login and Server Side will be SQL command such as:


(a)
Username: 'or 9 = 9; --
Password: hacker

(b)
Username: 'OR" = '
Password: 'OR" = '

Fig. 3: By passing the authentication (2)

```
SELECT * FROM tbl_Users WHERE Username =
        ' hacker ' AND Password = ' ' or 9=9;-- '
```

Logic method indicate that X and Y or TRUE is forever truth although all X and Y are TRUE or FALSE from example X is Username = 'hacker' and Y is Password =‘’ and 9=9 also is TRUE, so Username = 'hacker' AND Password = ‘’ or 9=9;--‘ is X and Y or TRUE also is TRUE, so SQL login command is SELECT * FROM tbl_Users WHERE TRUE as same as SELECT * FROM tbl_Users that mean value from Database Server not empty.

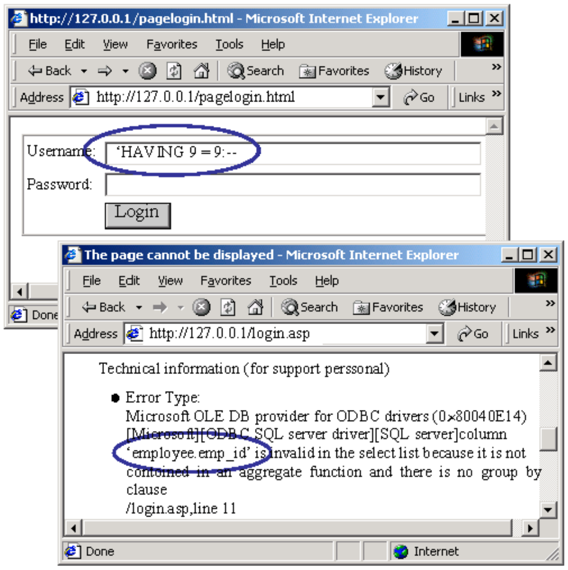
Symbol;-- mean the end of SQL command, then hacker input it to avoid last Single Quote (last Single Quote from Server Side) finally none empty string send back to strAuthCheck value, such as boolAuthenficated is TRUE, that mean authenticate pass.

By pass authentication can be done several solutions such as show in Fig. 3 a and b.

Try to get more information: Hacker begin to force to find field name and table name by input command to SQL login and to occur Error and then Brower show a little bit data in page error example such as Fig. 4, Hacker input HAVING code to occur Error and then hacker can know field name and table name both are table name is employee and first field name is emp_id and make error it again for more information.

Login to existing user: Hacker can be login like member such as login by specify UserID number or username by use Sub Query (Fig. 5).

Stealing file: Copy solutions depend on DBMS, in this study for example solutions how to hacker can be copy data file from SQL Server, call by pass CMD. EXE to


http://127.0.0.1/pagelogin.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://127.0.0.1/pagelogin.html Go Links
Login
Done
The page cannot be displayed - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://127.0.0.1/login.asp Go Links
Done Internet

Username: ‘HAVING 9 = 9:--

Password:

Technical information (for support perssonal)

- Error Type:
  Microsoft OLE DB provider for ODBC drivers (0x80040E14)
  [Microsoft][ODBC SQL server driver][SQL server]column ‘employee.emp_id’ is invalid in the select list because it is not contoined in an aggregate function and there is no group by clause
  /login.asp,line 11

Fig. 4: Use HAVING command to get field name

Stored Procedure name is xp_cmdshell (Chomsin, 2007), as hacker try to find data files that they want and then run command dir/s (Fig. 6).

Since, hacker find several solutions to get it such as copy this file to c:\Inetpub\wwwroot or copy to c:\Inetpub\ftproot and then download.

PROTECTION SCHEME

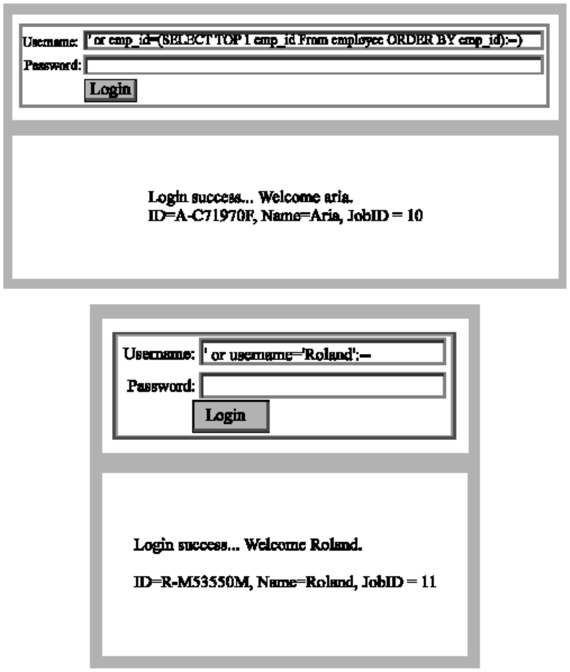
There are several solutions in order to protect data from hacker. Such as secure web programming, application firewall, IPS and HTTPS Hacking protection (Chomsiri, 2007) method. In this study, web focus on software improving by generated secure web programming and update traditional web program that contains risk point. At this study, we proposed several approved methods, that can be protected the data from hacker by using SQL injection.

Stealing file: In general, the hacker input special symbol, such as ‘ = ; - “ > < into input form on web page in order to added these symbol into SQL statements Inputting. If we can prevent special symbol inputting into web form, hacker cannot be access our system.

Filter the ‘(Single Quote Symbol), the hacker added these symbol into input form. If we can replace single quote symbol to space or dispose then hacker cannot be access our system.

Original code

```
SELECT * from UserTable
WHERE UserTable.username=' + strUser
```



Username: ' or emp_id=(SELECT TOP 1 emp_id From employee ORDER BY emp_id):--)

Password:

Login success... Welcome aria.
ID=A-C71970F, Name=Aria, JobID = 10

Username: ' or username='Roland':--

Password:

Login success... Welcome Roland.

ID=R-M53550M, Name=Roland, JobID = 11

Fig. 5: Login to existing user

```
+' and UserTable.password='
+ strPasswd +'
```

Normal case: Input-username = bobby password = abc 123

```
SELECT * from UserTable
WHERE UserTable.username=bobby'
and UserTable.password=' abc123 '
```

Hack case: Input - username=hacker password=x’ or ‘‘ =’

```
SELECT * from UserTable
WHERE UserTable.username=' hacker '
and UserTable.password=' x ' or " ='
```

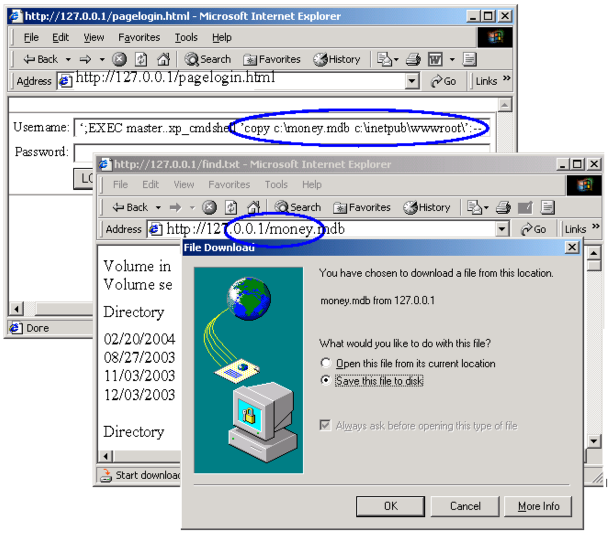
Protective code and hack case: Input - username=hacker password=x ' or " ='

```
SELECT * from UserTable
WHERE UserTable.username='hacker '
and UserTable.password='x or = '
```

Filter the = (Equal Symbol), In general Hacker added text such as or 1=1 to input form for make this SQL command truth. If we can replace equal symbol to space or dispose then hacker cannot be access our system.

Hack case: Input-username = hacker password = x’ or " = '

```
SELECT * from UserTable
WHERE UserTable.username=’hacker‘
and UserTable.password=' x' or " = ''
```



http://127.0.0.1/pagelogin.html - Microsoft Internet Explorer

Address: http://127.0.0.1/pagelogin.html

Username: ';EXEC master..xp_cmdshell 'copy c:\money.mdb c:\inetpub\wwwroot\';--

Password:

http://127.0.0.1/find.txt - Microsoft Internet Explorer

Address: http://127.0.0.1/money.mdb

```
Volume in
Volume se
Directory
02/20/2004
08/27/2003
11/03/2003
12/03/2003
Directory
```

File Download

You have chosen to download a file from this location.

money.mdb from 127.0.0.1

What would you like to do with this file?

○ Open this file from its current location

● Save this file to disk

☑ Always ask before opening this type of file

Fig. 6: Files searching and stealing (SQL server)

Protective code and hack case: Input - username=hacker password=x' or ' ' = '

```
SELECT * from UserTable
WHERE UserTable.username='hacker '
and UserTable.password='x ' or ''  ''
```

Filter the; (Semi Colon Symbol), In general hacker added between SQL command when use this symbol our can added SQL command >1. In other words, if hacker use;-- that Microsoft SQL Server mean the end of SQL command and then abandon other word next to symbol ;-- . If we can replace semi colon symbol to space or dispose then hacker cannot be access our system and SQL Error happen.

Hack case: Input-username=xxx' or 1=1;-- password=yyy

```
SELECT * from UserTable WHERE
UserTable.username='xxx'
or 1=1;--' and UserTable.password='yyy'
```

Protective code and hack case: Input-username=xxx' or 1=1;-- password=yyy

```
SELECT * from UserTable WHERE
UserTable.username='xxx' or 1=1 --' and
UserTable.password='yyy'
```

Filter the - (Minus Symbol), In last passage about symbol is;-- that Microsoft SQL Server mean the end of SQL command and then abandon other word next to symbol ;--. If we can replace minus symbol (-) to space then hacker cannot be access our system and SQL Error happen.

Hack case: Input-username=xxx' or 1=1;-- password=yyy

```
SELECT * from UserTable WHERE
UserTable.username='xxx' or 1=1;--' and
UserTable.password='yyy'
```

Protective code and hack case: Input - username=xxx' or 1=1;-- password=yyy

```
SELECT * from UserTable WHERE
UserTable.username='xxx' or 1=1' and
UserTable.password='yyy'
```

Filter the " (Double Quote Symbol), In general double quote symbol advantage same single quote symbol because some web programming use it and protection is important same single quote.

Filter the > (Greater Than Symbol) and < (Less than Symbol), hacker added this to generate a condition. If we can replace it to space or dispose then hacker cannot be complete command and SQL Error happen.

Hack case: Input - username= xxx' or salary>1000;-- password=yyy

```
SELECT * from UserTable WHERE
UserTable.username='xxx' or salary>1000
;--' and UserTable.password='yyy'
```

Although, we prevent special symbol such as ' = ;- "> < but member used it cannot log in complete then administrator have to advise policy to member do not use these symbol in username and password.

Limit input string length: Except to by pass authentication, used SQL injection to query data from database server or call Shell Command in Operating System by uses SQL command (Fig. 6).

In general username and password length is not >15 letters. Using long Input String prevent hacker to access successfully.

Encryption before Comparing with username and password: We have unintentionally discovered that in the case of encryption of password before insert to database such as MD5(strPasswd) will prevent hacking by SQL injection to certain level. For example, hacking by sending username=hacker and password=x’ or ‘ ‘ = ’ will make x’ or ‘ ‘ = ’ being encrypted. The result is that server cannot process SQL command that hacker want. But only encryption password cannot prevent this input username=xxx’ or 1=1;-- password=yyy because ;-- will cause SQL Server to abandon the followed letters. Encryption both username and password will be able to better prevent. However, encryption username is unnecessary for web programmer because Web Programmer, Developer or DBA cannot read user name from database directly, which may affect the system development.

From the experiment it is discovered that if we prevent by checking input string like the process in previous sections, we do not have to use this process. However, preventing input string must be conducted along side with previous section.

Transferring input from client side script to server side script: We have already discussed about preventing special symbol such as ‘ = ; - “ > < and limiting the length of Input String in the previous section, but creation of preventing code can be conducted in both Client Side Script and Server Side Script. Both 2 methods have different security.

Posting preventing script on Client Side Script, hacker can save it in computer and edit script then erase preventing code in order to send special symbols such as ‘ = ; - “ > < to server. Moreover, it is the chance to insert the long Input String. Thus, we should design web program to put the preventing code of the Input String on the Server Side Script.

Harden on DBMS: To strengthen the DBMS is a factor to increase the security. For example, we should erase unused Stored Procedure, which has the risk such as xp_cmdshell on SQL Server. Moreover, we should limit the right of user, which runs DBMS not to have unnecessary right; for example, do not run DBMS by the Administrator or Root right.

CONCLUSION

A great number of web-site in the world has vulnerable, which can be hacked by using SQL injection technique. Hacker can input abnormal string on input form to corrupt a system; string, which can break a system such as ' or 1=1;-- can change SQL Statement in server to working improperly and able hacker to remote attack to system.

In this study, we propose a method for write secure web-program such as ASP, PHP and JSP that can increase security level on a server and network.

We present many techniques for break SQL injection. We have study and experiment with many protection schemes.

Our result can be decide to use better method such as preventing special character (' " = < > ; -). This knowledge can use as a formal to write secure web-software for increase security level on network system.

REFERENCES

Chomsiri, T., 2007. HTTPS Hacking Protection. In: Proc. The 21st International Conference on Advanced Information Networking and Applications Workshops. AINAW’07, 10: 590-594. DOI: 10.1109/AINAW.2007.200.

Forouzan, B.A., 2004. Data Communications and Networking. 4th Edn. McGraw-Hill Companies, Inc. New York, USA. URL: http://www.bookpool.com/sm/0073250325.

McClure, S., S. Shah and S. Shah, 2002. Web Hacking: Attacks and Defense. 1st Edn. Addison-Wesley, Reading, Massachusetts. URL: http://www.bookpool.com/sm/0201761769.

McClure, S., J. Scambray and G. Kurtz, 2005. Hacking Exposed: Network Security Secrets and Solutions. 5th Edn. McGraw-Hill, New York, USA. URL: http://www.bookpool.com/sm/0072260815.

Ross, K.W. and J.F. Kurose, 2007. Computer Networking: A Top-Down Approach. 4th Edn. Addison-Wesley Longman, Inc., New York, NY. URL: http://www.bookpool.com/sm/0321497708.