A General System Design and Implementation of SQL Injection Precaution

Fang Xin
Hunan Institute of Science and Technology,YueYang,Hunan,414000,China
E-mail:fashion90@163.com

Fang Wei
HuNan Communications Research Institute,ChangSha,Hunan,410015,China

***Abstract*—SQL injection attack is very easy to implement intrusion detection, Attacker through the webpage address into the entrance, constructs a SQL statement, illegal access to the web resources. This paper introduces the SQL is injected into the formation reasons, SQL injection methods, to prevent SQL injection of several common measures, gives a general SQL prevent implantation procedure..**

Key words- SQL injection; attack; detection; ASP.

I. FOREWORD

We open a web site, for example: http://61.187.92.238:5008/news_more.asp? Lm=62', Add a single quotation mark in the back of the address bar, what will happen? There will be an error message:

Microsoft JET Database Engine error '80040e14'
Syntax error in string expression in the query in'id=62''.
/news_more.asp，line 18

The single quotation is executied by the program! This is a SQL injection vulnerability, Through a injection tool is very easy to get the Web database information, This is a very dangerous thing.

II. SQL INJECTION PRODUCTION

Programmer programming level is the main reason causing SQL injection vulnerability, A junior programmers tend to ignore the filtered risk field. For example: in the design of user login system, We need to judge username and password , general code as follows:

```
Dim Username，Password
name＝Request（“name”）
Password＝Request（“Password”）
SQL=”Select * from user where name=”’&name&’” and password=”’&Password&’””
```

On the surface these code without any problems, but for dynamic SQL statement and the variable in the SQL statement is not filtered out some dangerous character, so that you can inject. In the case of do not know the username and password, only need to input user name and password in ' or ' = or ', can be successfully landing. Because ' or '= ' or ' is the result of a Boolean value, for a program is always true, so you can be successfully landing.

SQL injection detection usually have two ways, use manual detection and use tool to detect.

A. Manual detection

Manual detection is adopted in some websites link address input some illegal string, according to return results to determine whether a site can be injected. The most common is the single quotes test method and “1= 2” test method.

Single quote test is in the final surface with single quotes, if returned " Microsoft JET Database Engine error'80040e14'" error message, it indicated the presence of SQL injection vulnerability.

The 1=2 testing method is input”1 =2”after the URL, if the result is: BOF or EOF is a" true", or the current record has been deleted, the required operation requires a current record. It shows that the connection address existing SQL injection vulnerability.

B. Tool detection

The most commonly used detection tools: D injection tool, NBSI scan tool, WEB marginalia integrated detection tools, these tools can be related websites to download.

III. A GENERAL SYSTEM DESIGN AND IMPLEMENTATION OF SQL INJECTION PRECAUTION

According to the author's experience, summarizes some measures against SQL injection:

A. Using the detection method for testing;

Use testing tools and manual detection method, Check the website , if found loopholes, filter and check the address parameter

B. Modify the IIS parameter setting;

SQL injection intrusion is based on the ASP error information. You can set the IIS parameter no matter what ASP error, only give an error message, HTTP 500 error [1], The attacker can't from the prompt information to obtain useful information for invasion. This method is simple and effective, disadvantage is that will bring a lot of inconvenience when program debug.

C. Prevent cross-site data send;

D. The receive Request function data determine and filtering;

Use replace()[2] function to filter out single quotes and some of the characters, to prevent SQL injection.

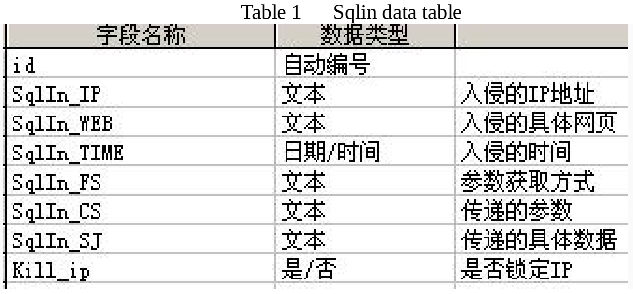
E. Use redirection technology to realizate of pseudo static page;

Through rewriting the component address mapping function, dynamic page address redirection static page, hiding the actual path, in order to improve the security of pages.

F. Using stored procedure send the parameter.

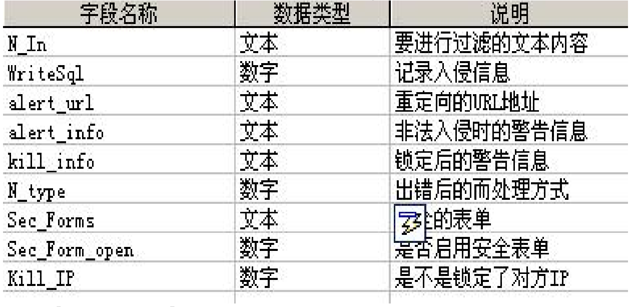
According to the above mentioned some preventive measures, to prepare a general to prevent SQL injection system. The main design idea: the data input legitimacy inspection, if found to invasive sign data, record the IP address, and according to the specific circumstances locked the IP address against further invasion. Procedures used in the two main data table.

Table 1 Sqlin data table



字段名称	数据类型	
id	自动编号	
SqlIn_IP	文本	入侵的IP地址
SqlIn_WEB	文本	入侵的具体网页
SqlIn_TIME	日期/时间	入侵的时间
SqlIn_FS	文本	参数获取方式
SqlIn_CS	文本	传递的参数
SqlIn_SJ	文本	传递的具体数据
Kill_ip	是/否	是否锁定IP

Table 2 Config data table



字段名称	数据类型	说明
N_In	文本	要进行过滤的文本内容
WriteSql	数字	记录入侵信息
alert_url	文本	重定向的URL地址
alert_info	文本	非法入侵时的警告信息
kill_info	文本	锁定后的警告信息
N_type	数字	出错后的而处理方式
Sec_Forms	文本	[illegible]全的表单
Sec_Form_open	数字	是否启用安全表单
Kill_IP	数字	是不是锁定了对方IP

The core code:

For character validity check code:

```
function CheckAll(form)   {
   for (var i=0;i<form.elements.length;i++)      {
      var e = form.elements[i];
      if (e.name != 'chkall')         e.checked =
form.chkall.checked;
      }
    }
```

System settings page of the main code:

```
sub config()
    …….
            <td height="30"  align="right">Current
file path：</td>
            <td align="left">&nbsp; <input
name="path" type="text"
value="<%=server.mappath(".")&"\"%>" class="textfield"
size="100"></td>
          </tr>
           <tr align="center" >
            <td height="30"  align="right"> The
characters Need to filter: </td>
            <td align="left">&nbsp; <input
name="N_In" type="text" value="<%=N_In%>"
class="textfield" size="100">
            Use &quot; |&quot; separate
     </td>
          </tr>
          <tr align="center" >
            <td height="30" align="right"> Record the
information：</td>
            <td align="left">&nbsp; <select
name="WriteSql">
        <option value="1" <%if WriteSql=1 Then
response.write "selected"%>>Yes</option>
        <option value="0" <%if WriteSql=0 Then
response.write "selected"%>>No</option>
            </select></td>
          </tr>
          <tr align="center" >
            <td height="30" align="right">Lock IP：
</td>
            <td align="left">&nbsp; <select
name="Kill_IP">
        <option value="1" <%if Kill_IP=1 Then
response.write "selected"%>>Yes</option>
        <option value="0" <%if Kill_IP=0 Then
response.write "selected"%>>No</option>
            </select></td>
          </tr>
         ……
  end Sub
```

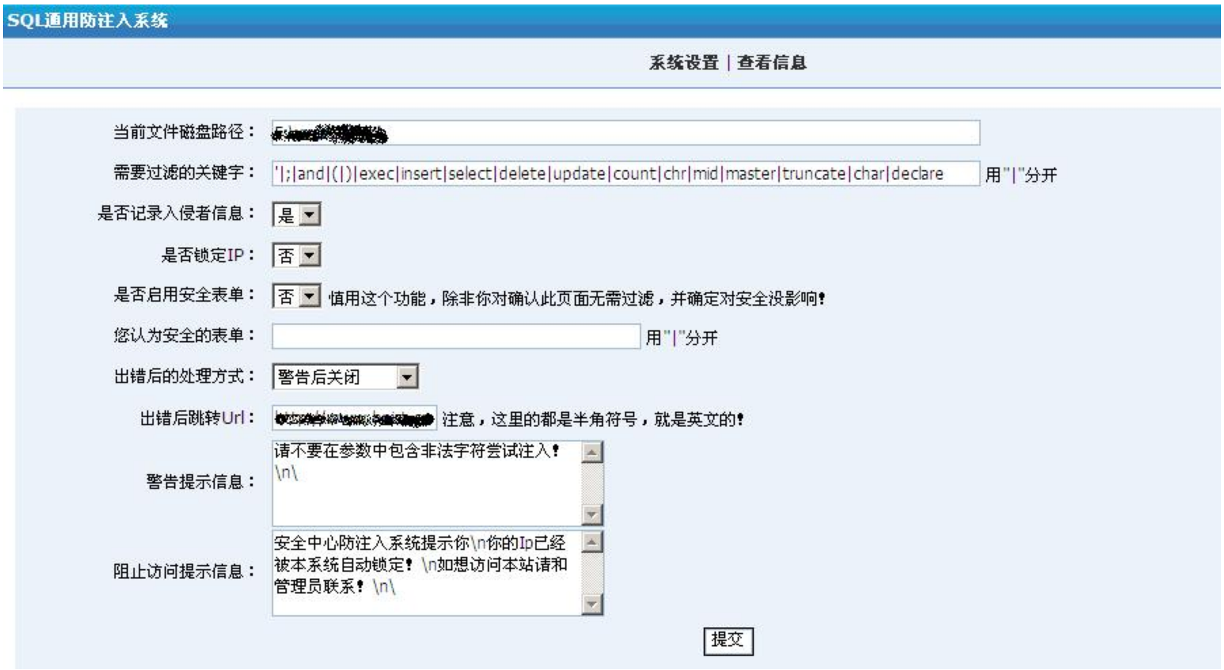
Information view the main code:

```
Sub Main()
……
<td width="4%" height=30>ID</td>
 <td width="11%" height="30"><font
color=red>Operate IP</font></td>
 <%
 If Kill_IP Then
%>
 <td width="4%">Lock</td>
 <%
 End If %>
 <td width="28%">Operate page</td>
 <td width="5%"> Submit method</td>
 <td width="10%"> Submit parameters
 </td>
 <td width="28%"> Submit data
 </td>
 <td width="10%"> Operate time </td>
</tr>
<form action="<%=url%>?Action=act" method=post
```

```
name=check>
        <%do while not rs.eof and i<listnum
        n=n+1%>
        <tr align="center" >
             <td height="30" bgcolor="#EBF2F9"><input
name="ID" type="checkbox" id="ID"
value=<%=rs("id")%>></td>
             <td height="30" bgcolor="#EBF2F9"
><%=rs("SqlIn_IP")%></td>
               <%
          If Kill_IP Then
        %>
             <td height="30" bgcolor="#EBF2F9" >
             <%if rs("Kill_ip")=true then
                            response.write "<font
color='red'>Locked</font>"
                    else
                           response.write "<font
color='green'>Unlocked</font>"
                    end if
             %></td>
                      <%
          End If %>
        ……
        end Sub
```

IV. Test

Operation the system will enter the management interface, as shown in Figure 1, You can set parameter freely, The information you set will be stored in the data table.



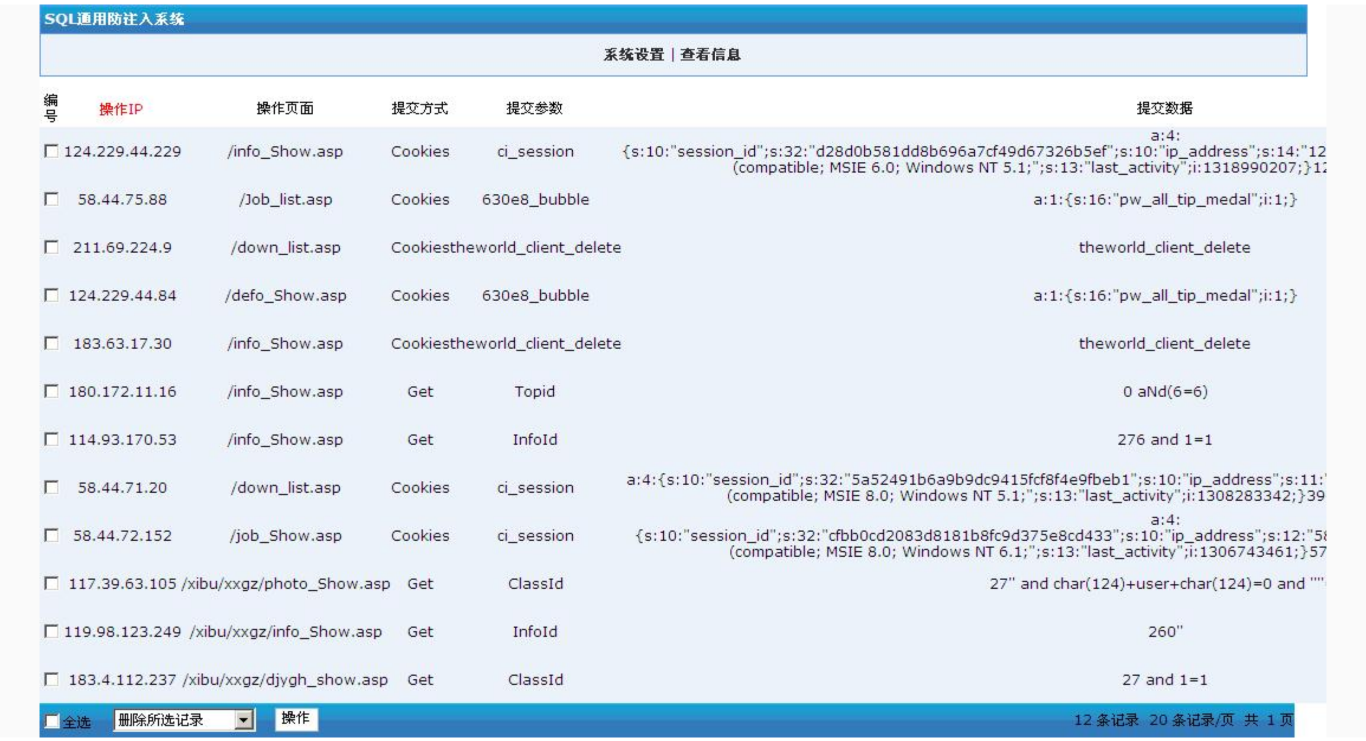
SQL通用防注入系统

系统设置 | 查看信息

当前文件磁盘路径：	[redacted]
需要过滤的关键字：	'|;|and|(|)|exec|insert|select|delete|update|count|chr|mid|master|truncate|char|declare 用"|"分开
是否记录入侵者信息：	是
是否锁定IP：	否
是否启用安全表单：	否 慎用这个功能，除非你对确认此页面无需过滤，并确定对安全没影响!
您认为安全的表单：	用"|"分开
出错后的处理方式：	警告后关闭
出错后跳转Url：	[redacted] 注意，这里的都是半角符号，就是英文的!
警告提示信息：	请不要在参数中包含非法字符尝试注入! \n\
阻止访问提示信息：	安全中心防注入系统提示你\n你的Ip已经被本系统自动锁定! \n如想访问本站请和管理员联系! \n\

Figure 1　system parameter setting interface

Click the"查看信息" into the view of information interface, as shown in Figure 2, You can see the visitors ‘s information.



SQL通用防注入系统

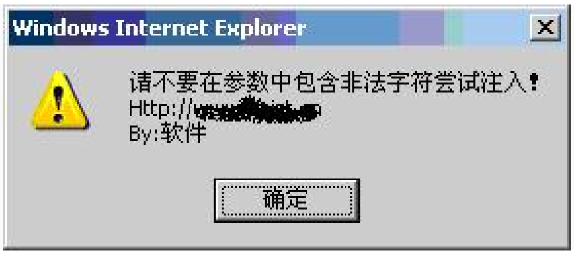
系统设置 | 查看信息

编号	操作IP	操作页面	提交方式	提交参数	提交数据
□	124.229.44.229	/info_Show.asp	Cookies	ci_session	a:4: {s:10:"session_id";s:32:"d28d0b581dd8b696a7cf49d67326b5ef";s:10:"ip_address";s:14:"12 (compatible; MSIE 6.0; Windows NT 5.1;";s:13:"last_activity";i:1318990207;}12
□	58.44.75.88	/Job_list.asp	Cookies	630e8_bubble	a:1:{s:16:"pw_all_tip_medal";i:1;}
□	211.69.224.9	/down_list.asp	Cookies	theworld_client_delete	theworld_client_delete
□	124.229.44.84	/defo_Show.asp	Cookies	630e8_bubble	a:1:{s:16:"pw_all_tip_medal";i:1;}
□	183.63.17.30	/info_Show.asp	Cookies	theworld_client_delete	theworld_client_delete
□	180.172.11.16	/info_Show.asp	Get	Topid	0 aNd(6=6)
□	114.93.170.53	/info_Show.asp	Get	InfoId	276 and 1=1
□	58.44.71.20	/down_list.asp	Cookies	ci_session	a:4:{s:10:"session_id";s:32:"5a52491b6a9b9dc9415fcf8f4e9fbeb1";s:10:"ip_address";s:11:" (compatible; MSIE 8.0; Windows NT 5.1;";s:13:"last_activity";i:1308283342;}39
□	58.44.72.152	/job_Show.asp	Cookies	ci_session	a:4: {s:10:"session_id";s:32:"cfbb0cd2083d8181b8fc9d375e8cd433";s:10:"ip_address";s:12:"58 (compatible; MSIE 8.0; Windows NT 6.1;";s:13:"last_activity";i:1306743461;}57
□	117.39.63.105	/xibu/xxgz/photo_Show.asp	Get	ClassId	27" and char(124)+user+char(124)=0 and ""
□	119.98.123.249	/xibu/xxgz/info_Show.asp	Get	InfoId	260"
□	183.4.112.237	/xibu/xxgz/djygh_show.asp	Get	ClassId	27 and 1=1

□ 全选 删除所选记录 操作 12 条记录 20 条记录/页 共 1 页

Figure 2 The system to view interface

If you attempt to address bar enter the illegal characters will pop up warning window, as shown in Figure 3, and according to the set of modified IP lock, if the IP locked you can't visite the websit again, will pop up warning window tell you your Ip is locked..



Windows Internet Explorer

请不要在参数中包含非法字符尝试注入！
Http://[redacted]
By:软件

确定

Figure 3 input the illegal characters warning window

V. Summary

In this paper, from a simple example introduction of SQL injection, introduced the SQL injection causes, detection methods and preventive measures, Design and implementate a general prevent SQL injection system, the system in the Win2003 debugging through, This system has been used in some website.

References

[1] http://www.jb51.net/article/26013.htm

[2] Wu Renjie.Web program design [M]. Beijing: China Railway Press,2009, 126-127

[3] Sebesta translated by Wang Chunzhi .Web program design [M]. Beijing: Tsinghua University press,2011