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( ) function to filter out single quotes and some of the characters, to prevent SQL injection.

E. Use redifiction technology to realitate of pseudo static page:

Through rewriting the component address mapping function, dynamic page redisdirection 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>
<thead>
<tr>
<th>Table 1</th>
<th>Sqlin data table</th>
</tr>
</thead>
<tbody>
<tr>
<td>字段名称</td>
<td>需要数据类型</td>
</tr>
<tr>
<td>id</td>
<td>印动编号</td>
</tr>
<tr>
<td>SqlIn_IP</td>
<td>文本</td>
</tr>
<tr>
<td>SqlIn_WP</td>
<td>文本</td>
</tr>
<tr>
<td>SqlIn_TIME</td>
<td>日期/时间</td>
</tr>
<tr>
<td>SqlIn_F5</td>
<td>文本</td>
</tr>
<tr>
<td>SqlIn_CS</td>
<td>文本</td>
</tr>
<tr>
<td>SqlIn_SF</td>
<td>文本</td>
</tr>
<tr>
<td>Kill_ip</td>
<td>否/是</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2</th>
<th>Config data table</th>
</tr>
</thead>
<tbody>
<tr>
<td>字段名称</td>
<td>数据类型</td>
</tr>
<tr>
<td>$in</td>
<td>文本</td>
</tr>
<tr>
<td>WriteSql</td>
<td>数字</td>
</tr>
<tr>
<td>alert_wl</td>
<td>文本</td>
</tr>
<tr>
<td>alert_info</td>
<td>文本</td>
</tr>
<tr>
<td>Kill_info</td>
<td>文本</td>
</tr>
<tr>
<td>K_type</td>
<td>数字</td>
</tr>
<tr>
<td>Sec_Form</td>
<td>文本</td>
</tr>
<tr>
<td>Sec_form_slam</td>
<td>数字</td>
</tr>
<tr>
<td>Kill_IP</td>
<td>数字</td>
</tr>
</tbody>
</table>

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()
......
end Sub
```

Information view the main code:
```
Sub Main()
......
<% If Kill_IP Then
    <td width="4%" height="30">Lock</td>
%>
End If<%
```

<form action="/?Action=act" method=post size="100">
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.

![system parameter setting interface](image)

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.
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.

![Figure 3 input the illegal characters warning window](image)

### 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

