# 记一次拿webshell过程

说明：目标靶机是自己搭建的一个用asp写的cms，因此整个过程做起来的十分简单，说白了就是脚本小子跑跑工具，但不管如何，这种拿sehll的思路十分经典，因此在此与大家分享一下。因为涉及很多经典的工具所以篇幅有点长。

整个流程：

信息收集：

用nmap扫描发现目标主机和开放端口

用AWVS扫描主机发现漏洞和后台页面

漏洞利用：

用sqlmap拆解字段

手工注入

暴力破解：

用burp暴力破解密码

上传木马

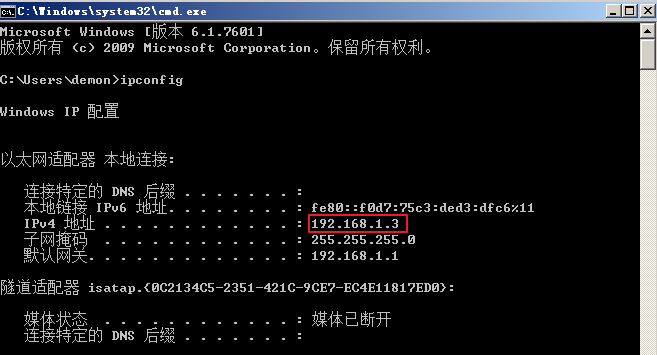
图片马

最后菜刀拿shell

基本过程就是这样

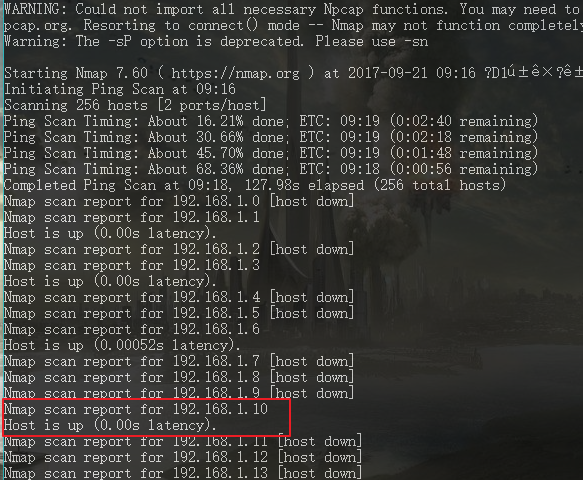
## 信息收集

首先查看攻击机的IP地址：



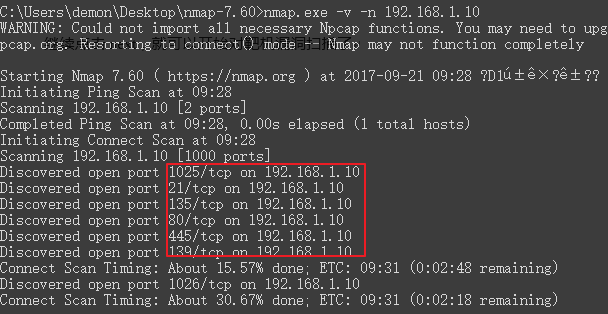
因为靶机和攻击机处于同一网段，但不知道靶机IP，所以用nmap扫描网段发现主机

命令行：nmap -v -n -sP192.168.1.0/24



这里靶机IP地址为192.168.1.10，下面继续用nmap扫描靶机开放的端口和系统指纹

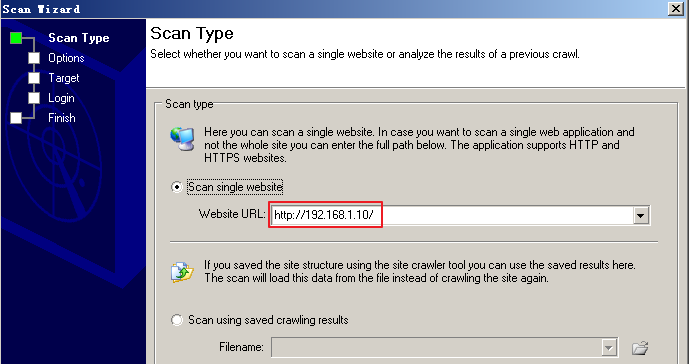
命令行：nmap -v -n -A 192.168.1.10

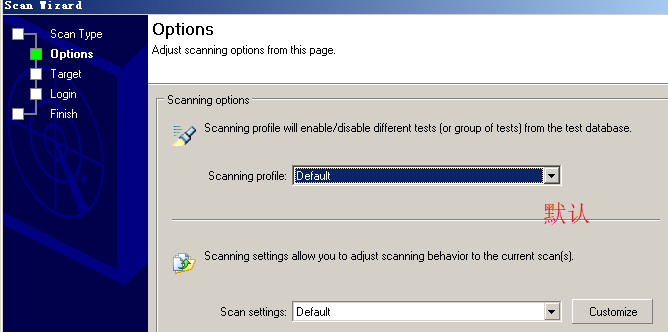


目标主机开启了80端口，在浏览器上访问靶机80服务

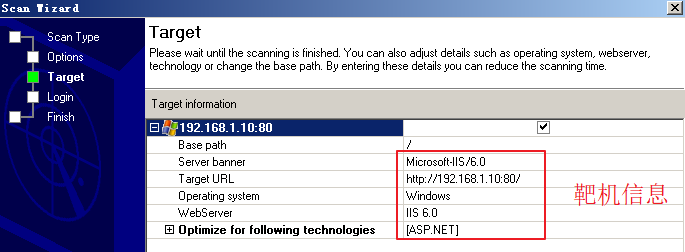


然后用AWVS对靶机扫描，看看有哪些高危漏洞存在





其他配置保持默认，一路点击next



继续点击next，就可以开始对靶机漏洞扫描了

扫描完成后可以看到两部分：一个是网站文件结构，一个是漏洞列表

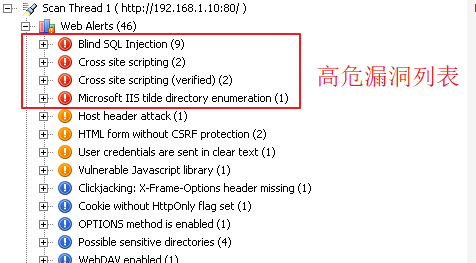


admin 很明显是后台登陆页面

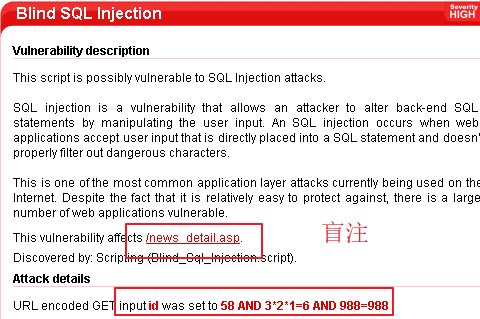
editor 是编辑器程序

inc 是配置文件，里面包含数据库账号密码等信息

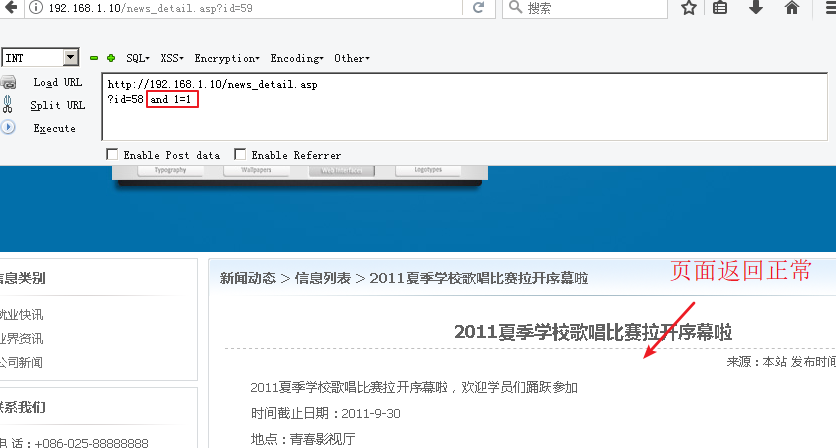
uploadFile 上传目录的文件

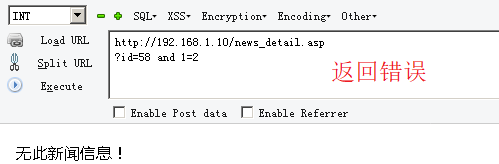


## 漏洞利用



用火狐hackerbar先手工注入，访问漏洞页面: http://192.168.1.10/news\_detail.asp?id=58



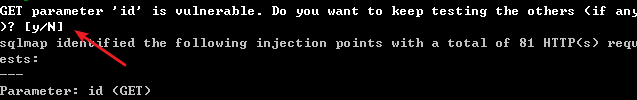


说明缺失存在注入漏洞，继续拆解表and exists(select \* from [admin] ) > 0

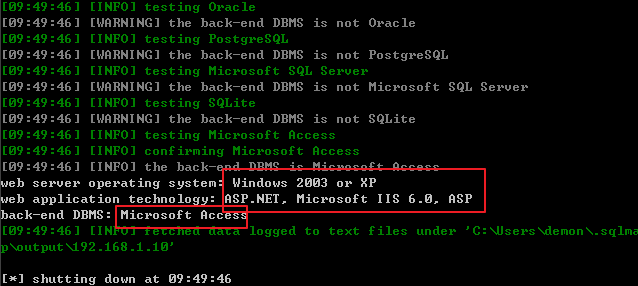
但是这里猜了很多次表名，依然没有猜中，人品不好，没事用sqlmap来扫一下

命令：sqlmap.py -u “<http://192.168.1.10/news_detail.asp?id=58>”

遇到这种选项默认回车即可



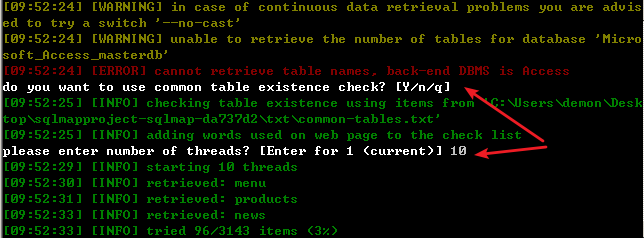
扫描完成后可以看到靶机信息，说明有注入漏洞

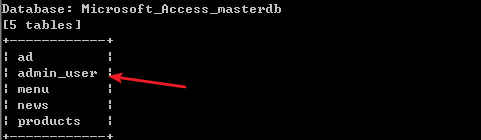


拆解字段

命令：sqlmap -u “<http://192.168.1.10/news_detail.asp?id=58>”--tables

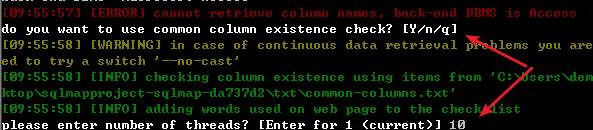
遇到下面两个选择一个默认回车，第二给10线程拆解表

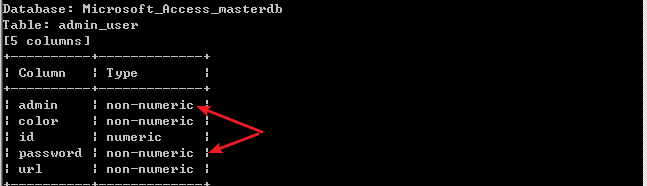


原来表名是admin\_user，管理员账号密码百分之99会放在admin\_user表里

继续拆解字段，命令：

sqlmap -u “<http://192.168.1.10/news_detail.asp?id=58>” -T admin\_user --columns





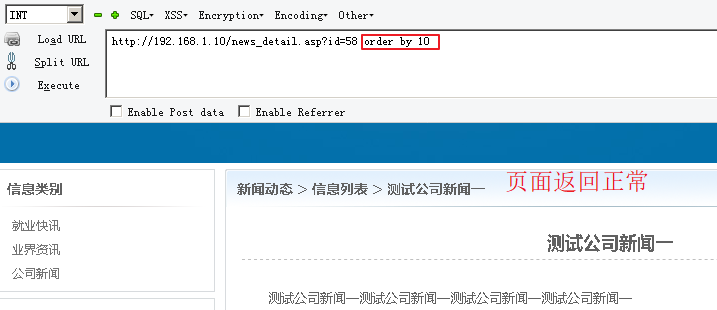
可以看到两个关键的字段，此时你可以继续暴力破解后台账号密码，也可以手工order by

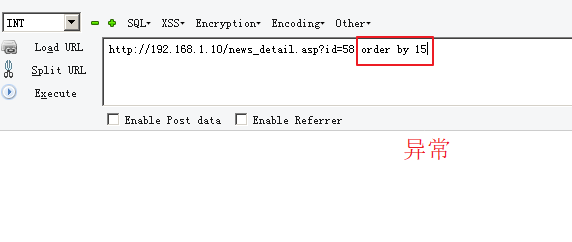
## 暴力破解

如果继续用sqlmap暴力破解字段，命令如下：

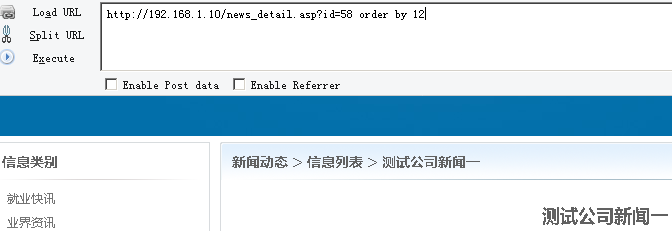
sqlmap -u “<http://192.168.1.10/news_detail.asp?id=58>” -T admin\_user -C ”admin,password” --dump

但是我觉得用order by会更快更有效率，所以下面order by 拆解数据

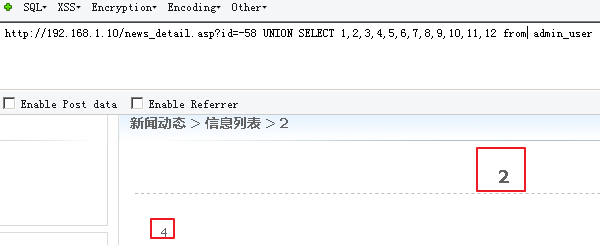




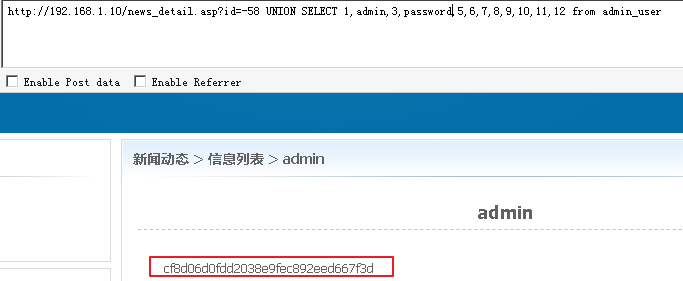
就这样使用二分法，对字段长度不断缩小范围，来确定字段长度，这里确定为12



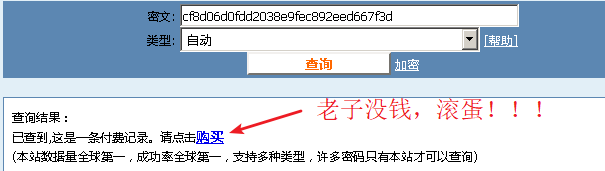
然后构造union语句，爆出数据显示字段位置，注意58前面加了负号让他报错



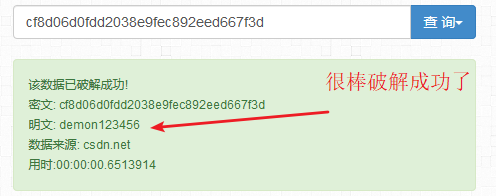
可以看到字段位置是2和4，现在把2和4替换成向拆解的字段admin和password



账号密码就出来了，但是密码是md5加密的，所以还得解密一下，去[www.cmd5.com](http://www.cmd5.com)解

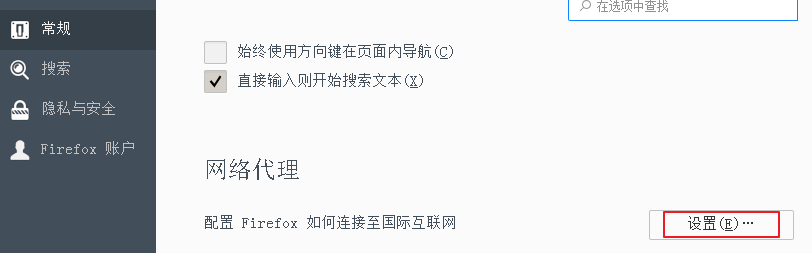


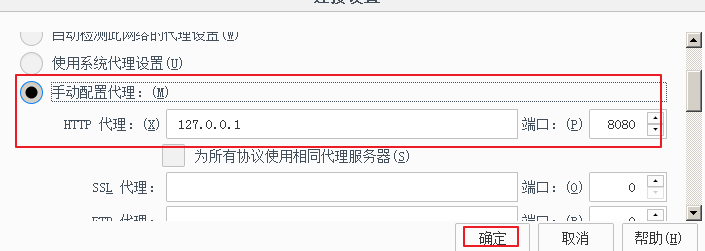
还有一个解密网站：<http://www.chamd5.org/?mst>



当然考虑到人品不好的朋友，可以使用burp来暴力破解密码

开启burp 然后在火狐浏览器设置一下代理，默认8080端口





设置好后，访问刚刚用AWVS扫描到的后台页面<http://192.168.1.10/admin/index.asp>

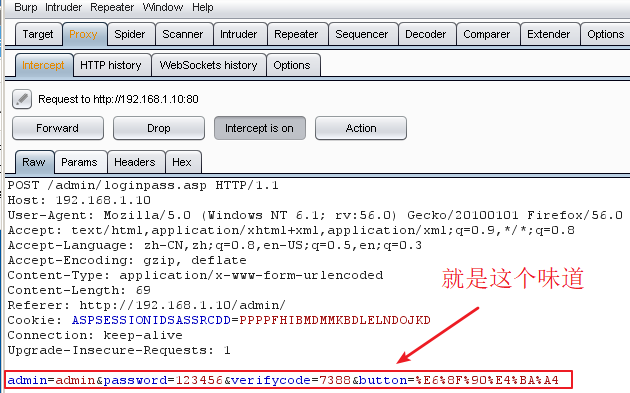
并在账号密码验证吗填写一下内如，如下：因为我们已经通过order by 拆解出用户名了，所以账号填写：admin，密码随便填，验证码填对的

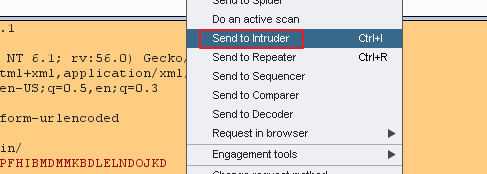


单击提交，切换到burp抓带登陆信息的http包

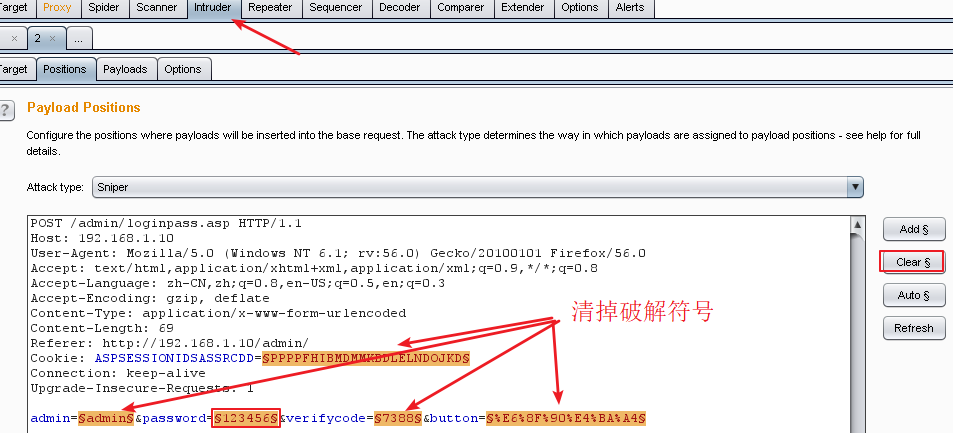


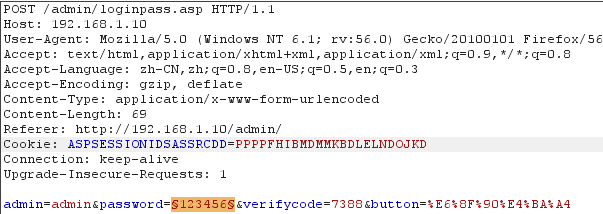
遇到下面这个包不要放行，右键选择send to intruder



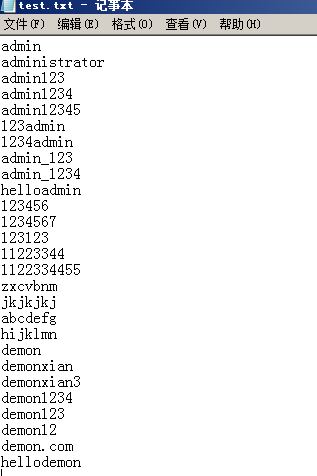


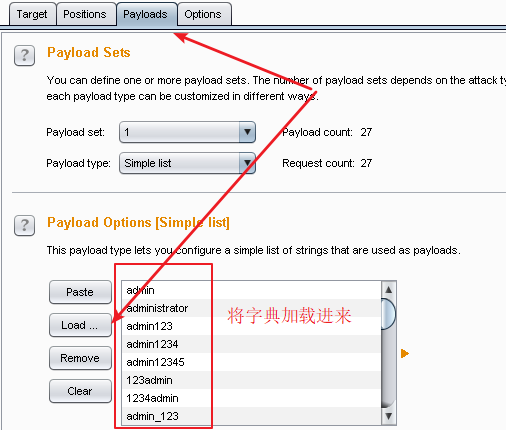
除了密码不用清掉破解符，其他都要去掉，选中点旁边的clear $(类似)

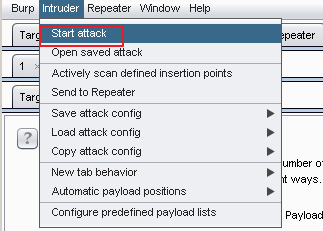


结果如下：

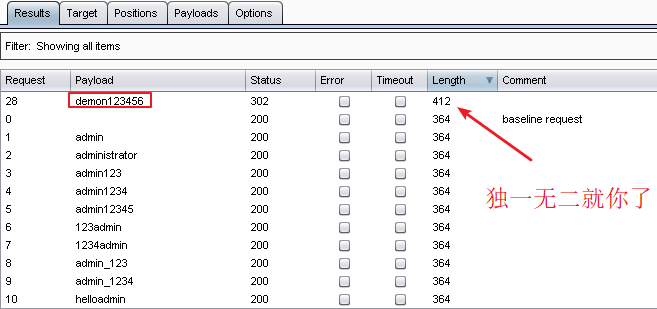
准备一个破解字典，越强大越有概率破解







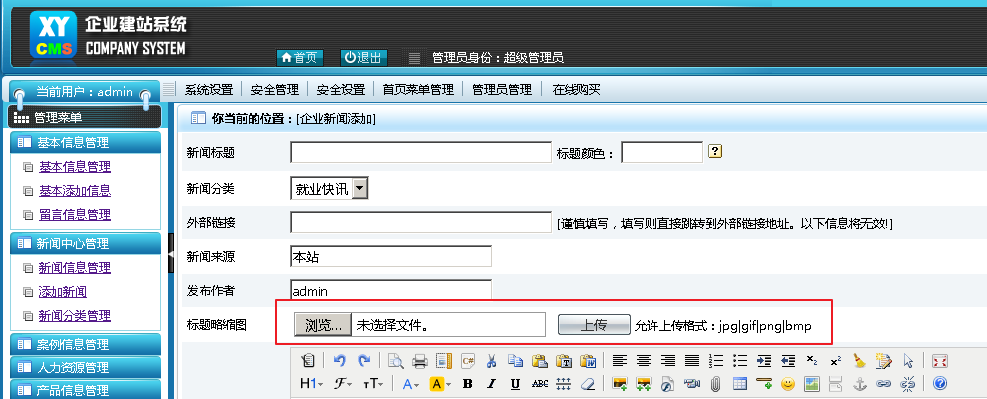
点击start attack开始破解，破解完成后，通过返回独一无二的长度来确定，如下



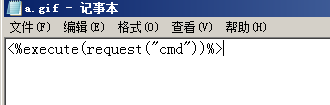
有了账号密码后，关闭代理和burp用破解到的账号密码来登陆

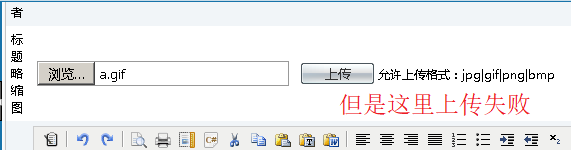
## 木马上传

在后台界面找到类似的上传按钮



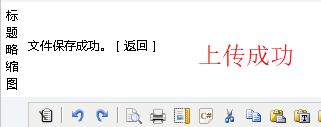
制作一个图片马，因为该页面是asp写的，所以要用asp的一句话木马，命名为a.gif

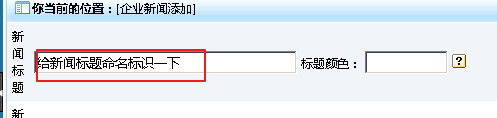


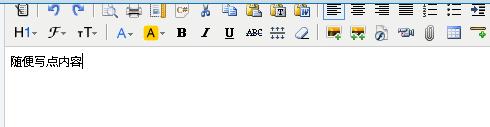


很有可能文件太小，没有到达图片的大小，另外最好在最前面加一个GIF89a



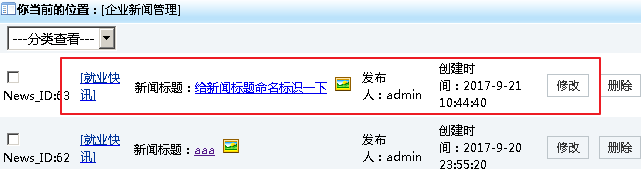




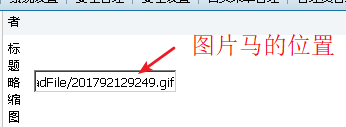




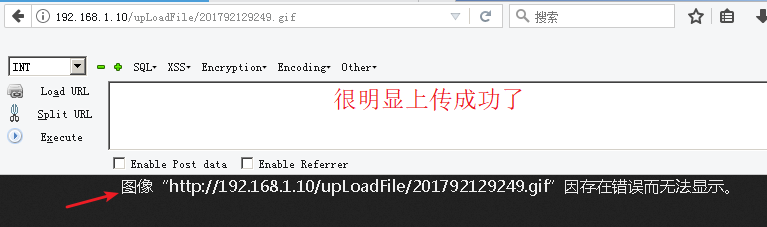
然后在新闻管理上可以看到我们添加的新闻



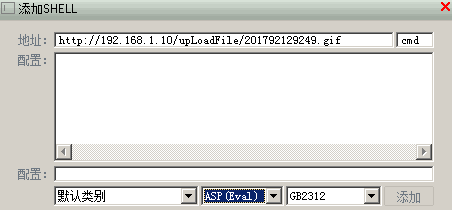
点击进去可以看到我们上传后图片马改名的格式和位置



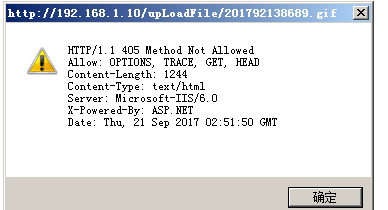
将其复制在浏览器上访问确认存在



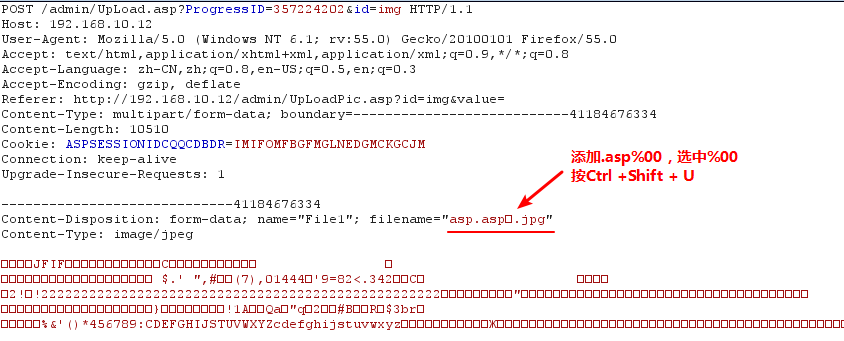
使用菜刀连接一下



直接连接是连不上的，因为图片并没有被当成asp文件来解析



burp抓包尝试使用00截断来改名。



送到repeater重放发包，可惜还是被改成固定格式的名字了

