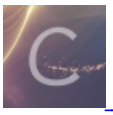
实验吧 —— web完整渗透测试实验指导书（图片版）

原创

烟敛寒林o 于 2018-09-02 23:37:43 发布 1001 收藏

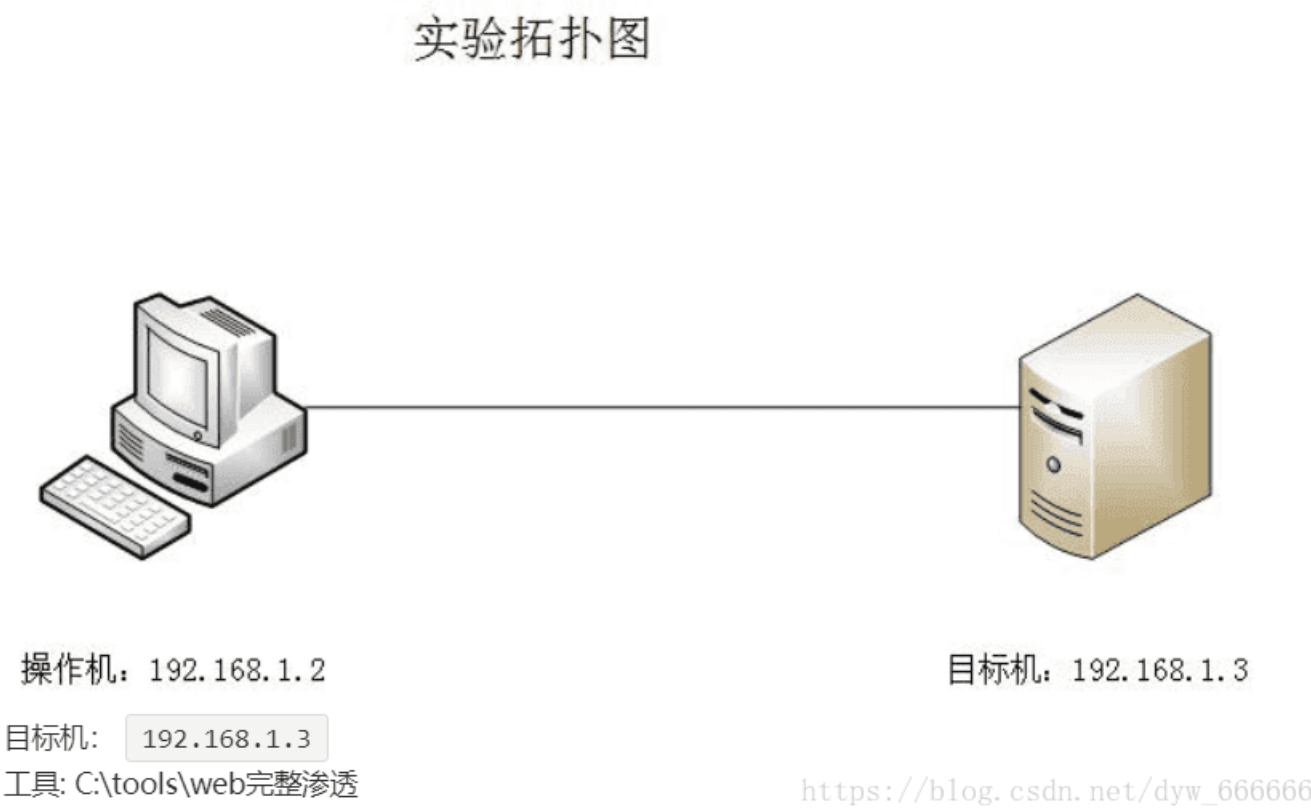
分类专栏： ★ Security

本文链接：https://blog.csdn.net/dyw_666666/article/details/82320867



web完整渗透测试实验指导书（图片版）

【实验环境】



目标机： `192.168.1.3`

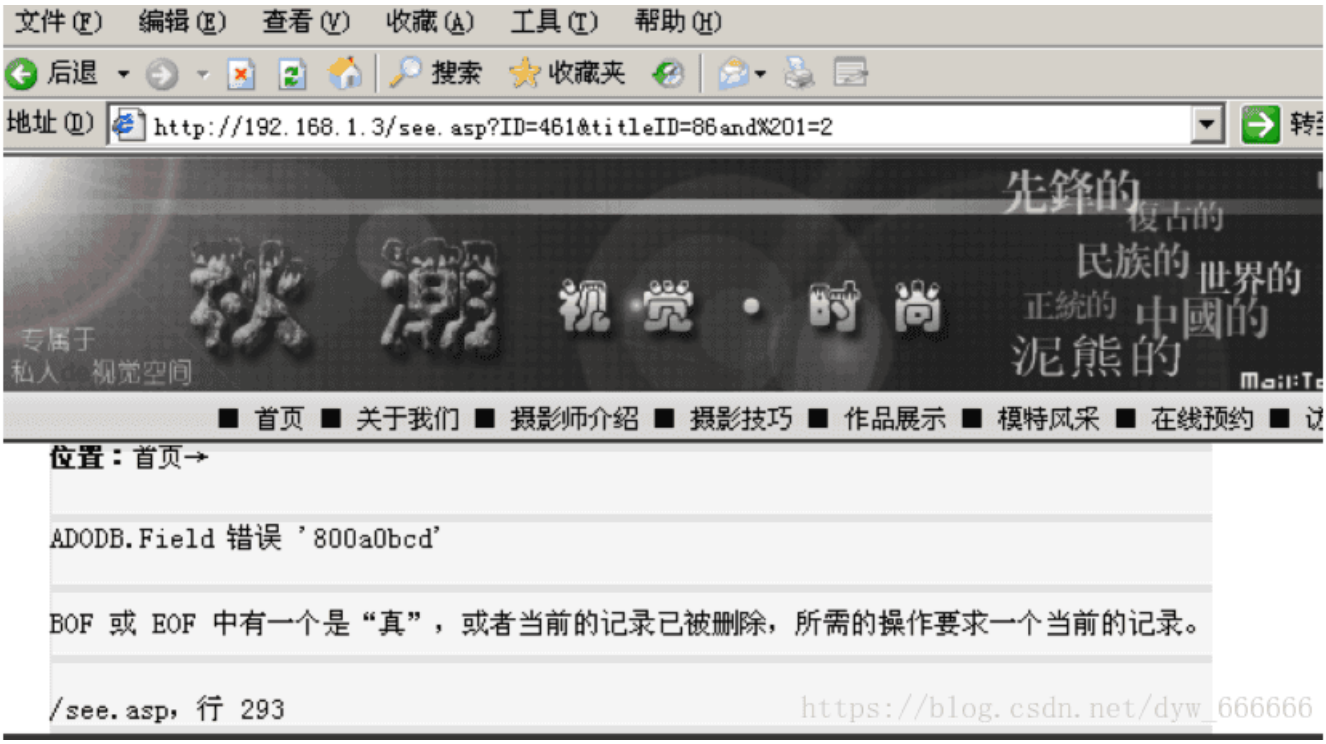
工具: C:\tools\web完整渗透

一、检测网站安全性

1.1我们浏览网站 `http://192.168.1.3`页面，寻找漏洞时，一般情况下会通过扫描软件进行扫描，在这里，我们就不演示扫描过程了，我们直接找到个链接来测试，打开【`http://192.168.1.3/see.asp?ID=461&titleID=86`】这个链接，在后面随便添加个「'」号，发现页面报错。 如图1所示

1.2如上图所知，我们输入’后，直接提示数据库错误界面，第一反映是该网站存在注入漏洞，我们用语句来确认该网站是否存在注入，我们输入 `http://192.168.1.3/see.asp?ID=461&titleID=86and 1=1` 。如图2所示

1.3我们在网站中输入 `http://192.168.1.3/see.asp?ID=461&titleID=86and 1=2，` 返回错误界面，一般来讲，当我们再网站尾部输入and 1=1和and=2 返回页面不同的情况下，且出现数据库报错的话，我们通常认为，该站点必存在SQL注入漏洞。如图3所示

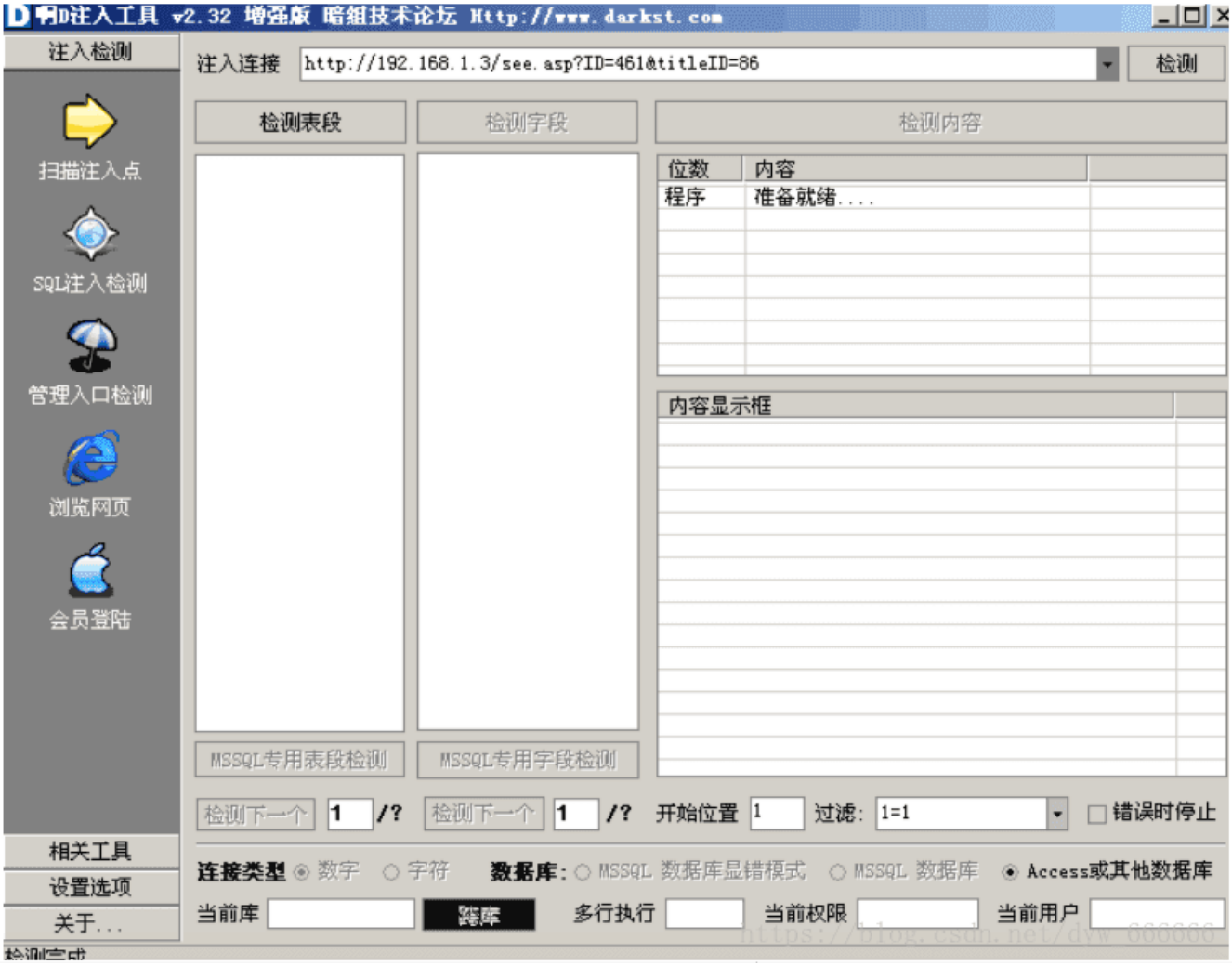


二、使用注入工具破解管理员用户、密码

2.1在c:/tools/web完整渗透测试实验/啊D注入工具文件夹下，打开啊D注入工具。如图4所示

2.2把存在注入点的url复制到啊D注入工具中，选择左侧的SQL注入检测。如图5所示

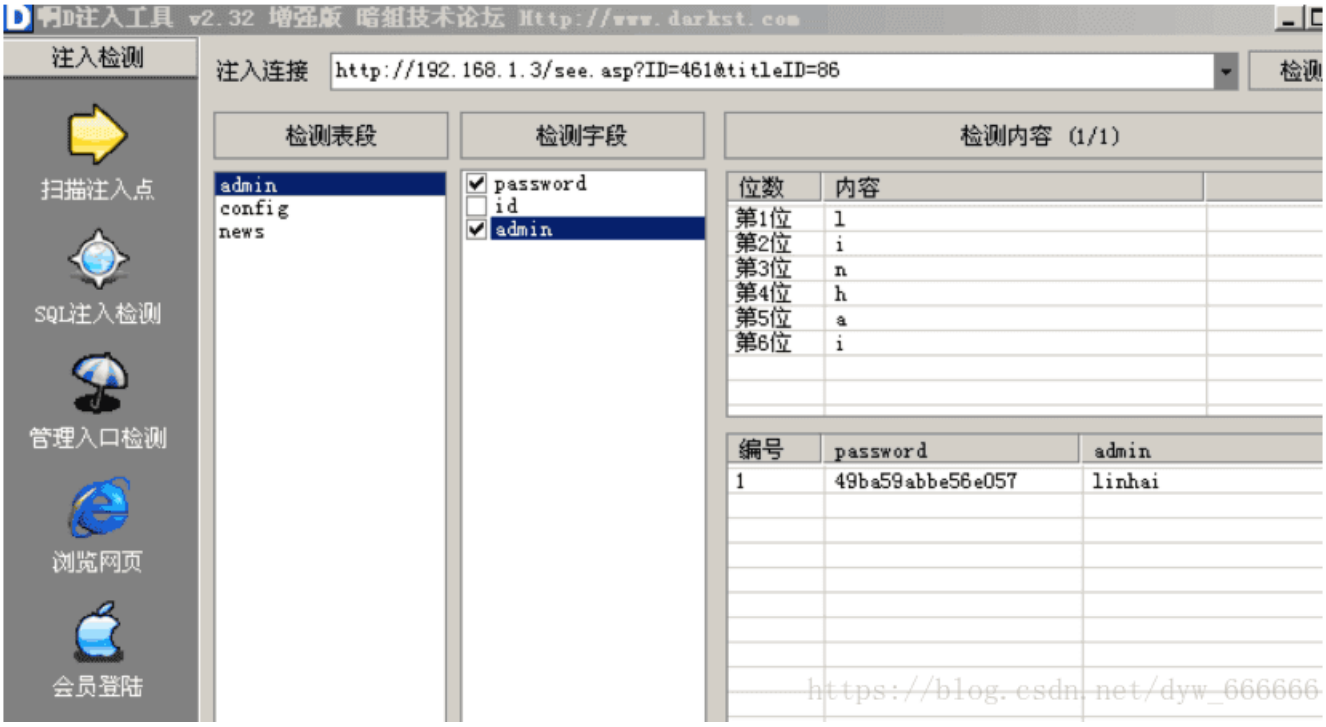
2.3我们点击『开始检测』，如果该网站存在注入，工具的下方会提示我们，并且提示我们该网站的数据库类型。如图6所示



2.4我们选择『检测表段』，就是探测数据库的所有表段名称。如图7所示

2.4我们选择『admin』段，然后开始选择『检测字段』，这里我们选择admin表段的原因在于基本上所有的管理员用户名和密码存放在admin表段。如图8所示

2.5我们选择password和admin，然后选择『检测内容』，破解对方的用户名和密码。如图9所示



三、使用工具破解md5密码

3.1我们得到的管理员密码是通过MD5值加密的，我们可以通过本地的MD5破解软件进行破解，打开C:\tools\web完整渗透\md5破解文件夹，打开md5crack.exe,这个md5crack就是通过字典的形式来破解md5值，所以具有一定的运气性，当然你的字典强大，跑成功密码的概率就高。如图10所示

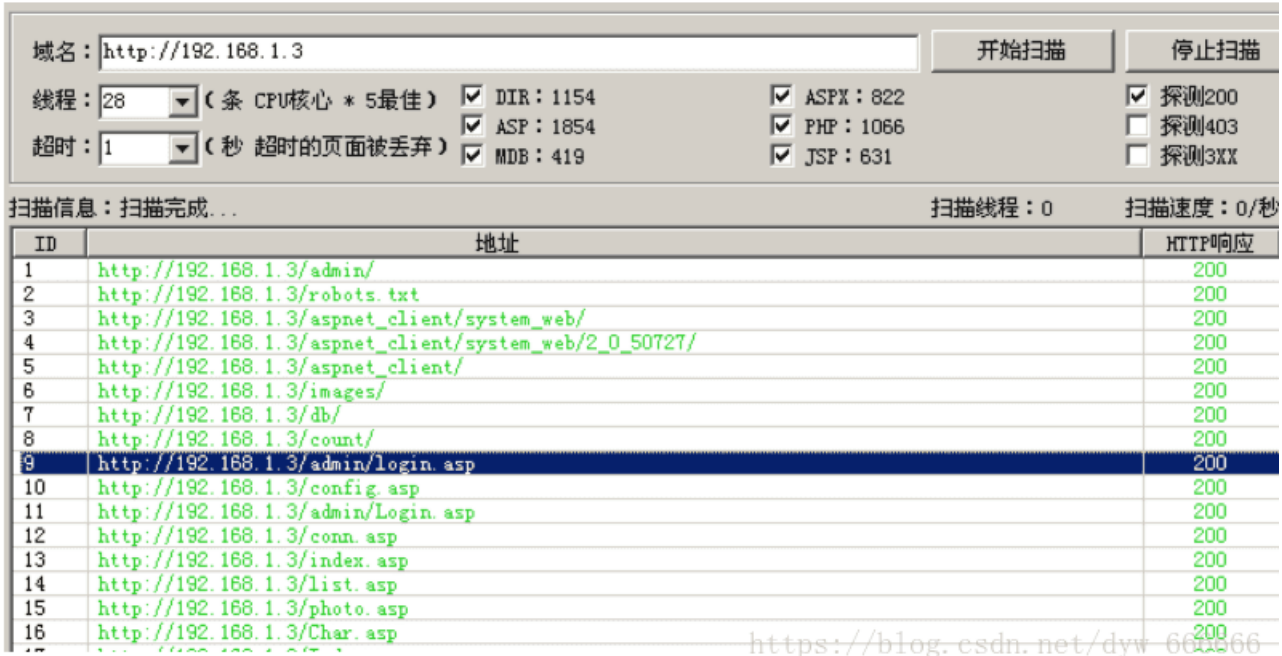
3.2我们在软件里面输入我们得到的md5值，软件会自动为我们破解出明文密码，这里能破解成功依赖于我们不错的密码字典，不是所有复杂的密码都能够被破解，如果有网络环境的同学，再实地测试时，可以通过访问 `http://www.cmd5.com来进行对md5值的破解` 。如图11所示

3.3至此，我们得到网站管理密码的明文，明文为123456。

四、找寻登录网站管理后台。

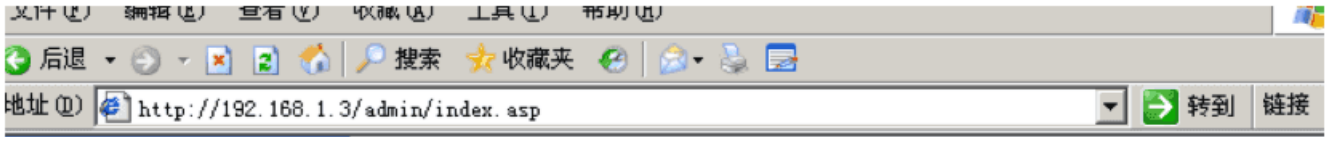
4.1我们拿到了管理员的明文用户名和密码，现在需要我们来进入后台了，一般情况下，网站的后台都是 `xx.com/admin/或者是xx.com/system等，一般情况下，我们可以通过扫描软件来探测网站管理后台，我们打开C:\tools\web完整渗透\御剑后扫描文件夹，打开御剑后台扫描工具.exe` 。如图12所示

4.2我们打开后，把我们需要探测的网站放进工具中，点击『开始扫描』。如图13所示



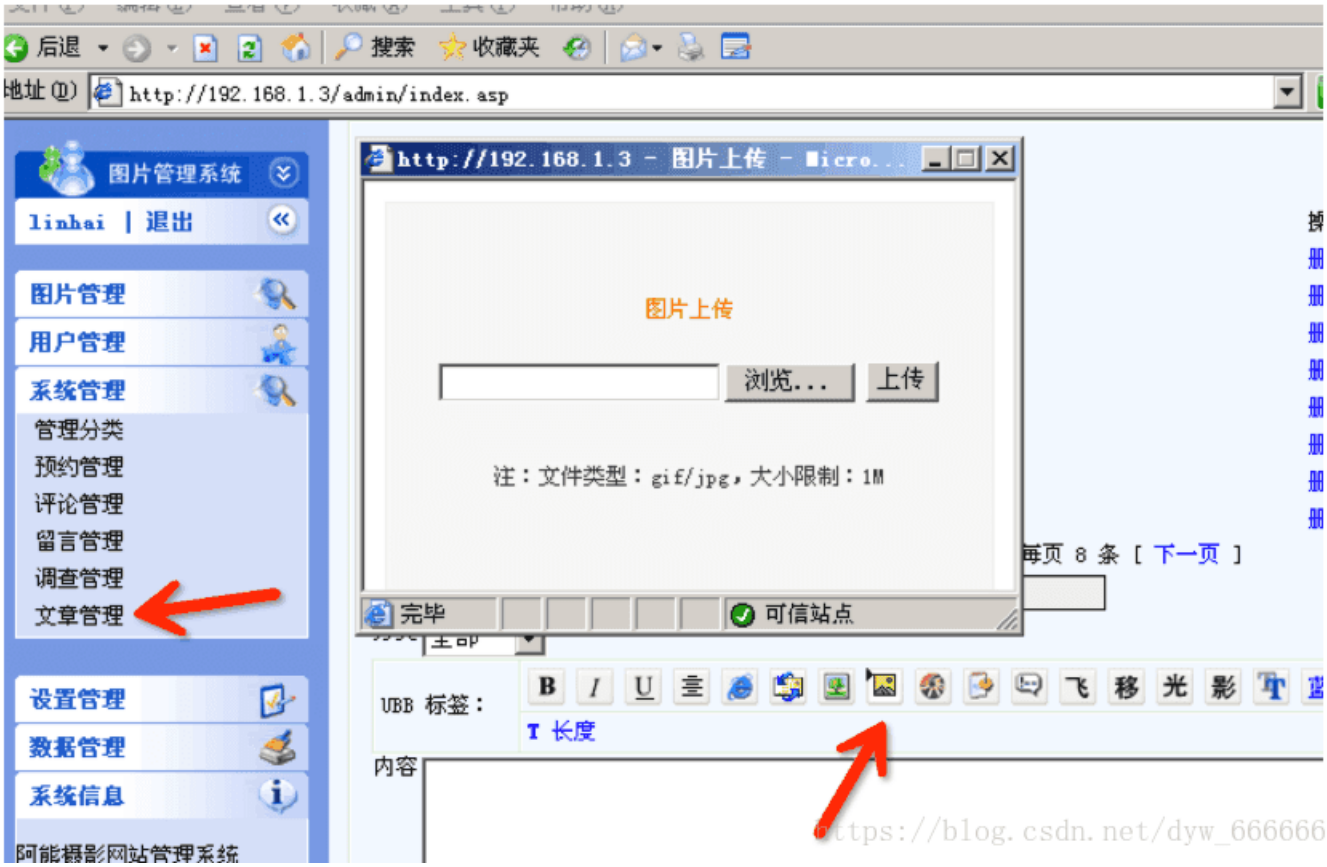
4.3我们通过扫描可以基本判定：`http://192.168.1.3/admin/login.asp`,我们打开该后台。 如图14所示

4.4 我们输入已经破解出来的管理员用户名：linhai 密码:123456，成功登录后台。如图15所示

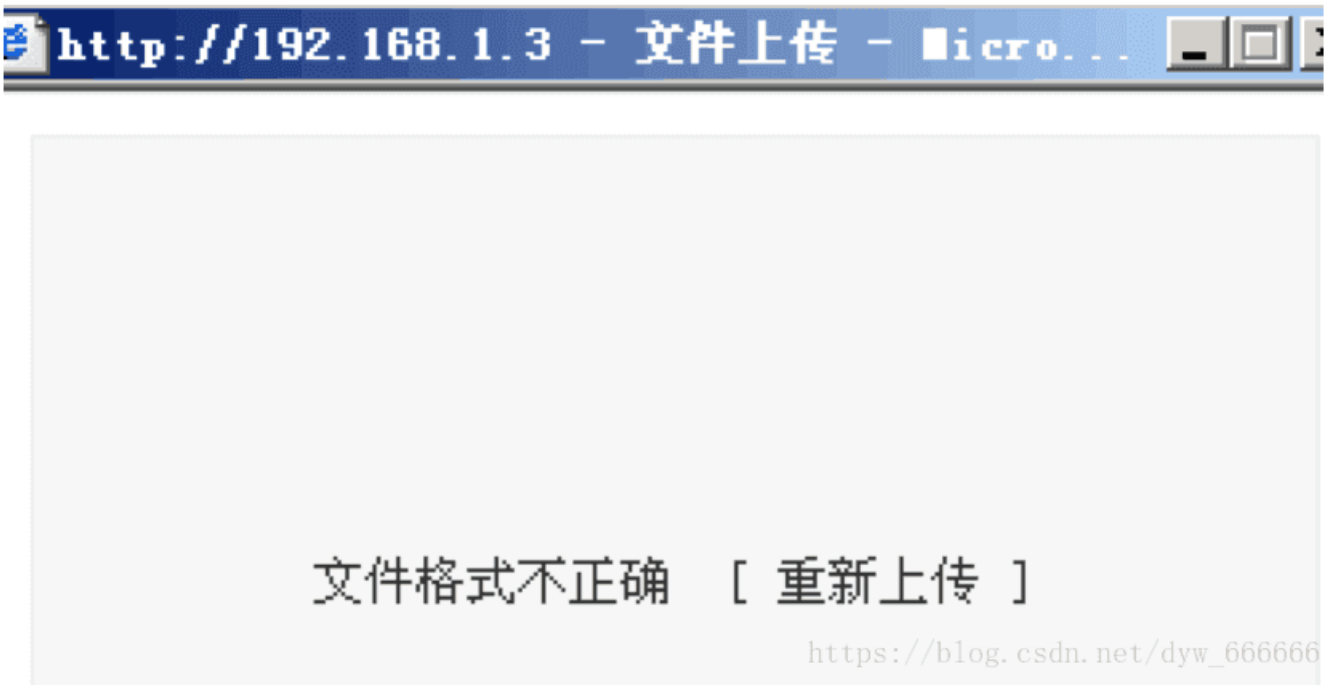


五、拿到网站webshell

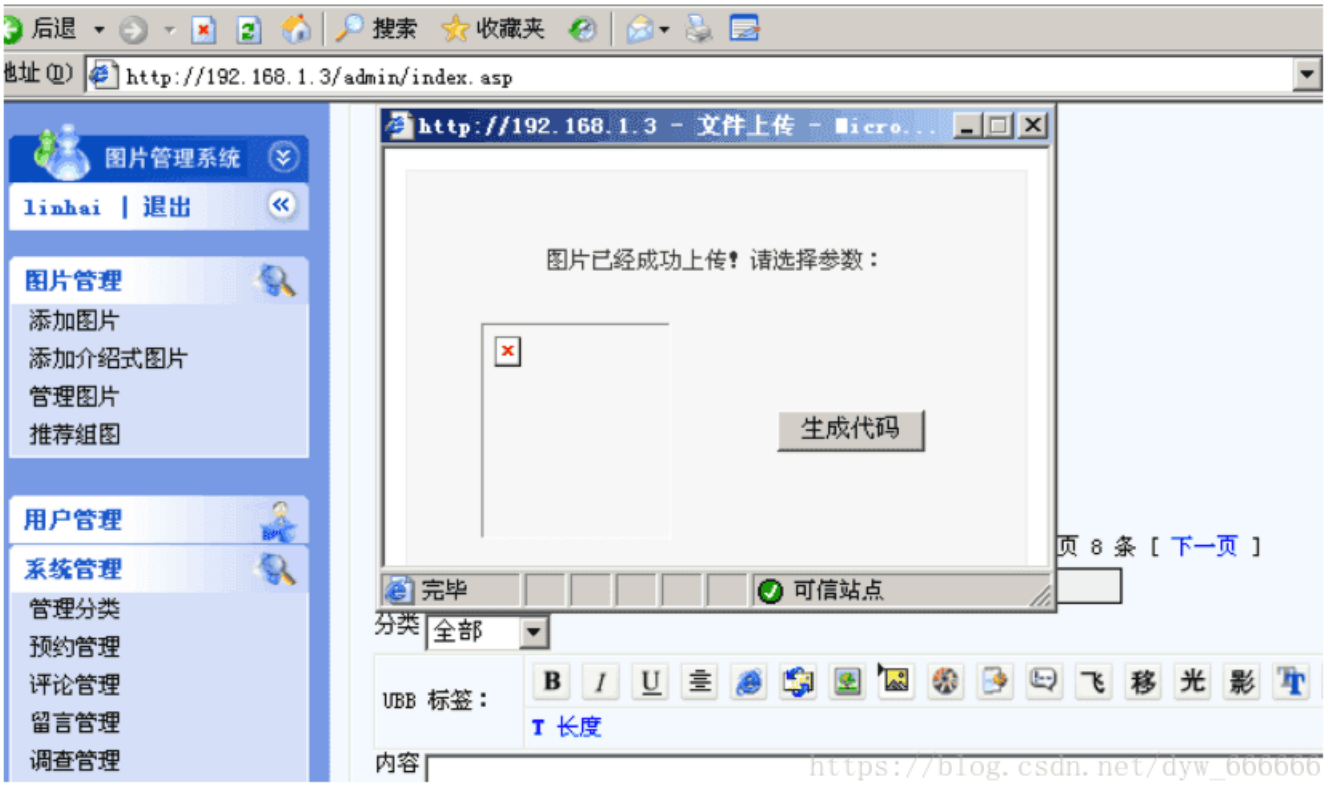
5.1我们既然已经进入了管理后台，那为了保持网站权限的持久性，我们需要拿到webshell,一般在后台拿shell的方法很多，具体的需要看网站后台的具体情况，就我们的站看，我们先打开『文章管理』，打开图片上传。如图16所示



5.2我们上传asp木马看看，木马在C:\tools\web完整渗透\木马文件夹中，我们直接上传该木马。如图17所示



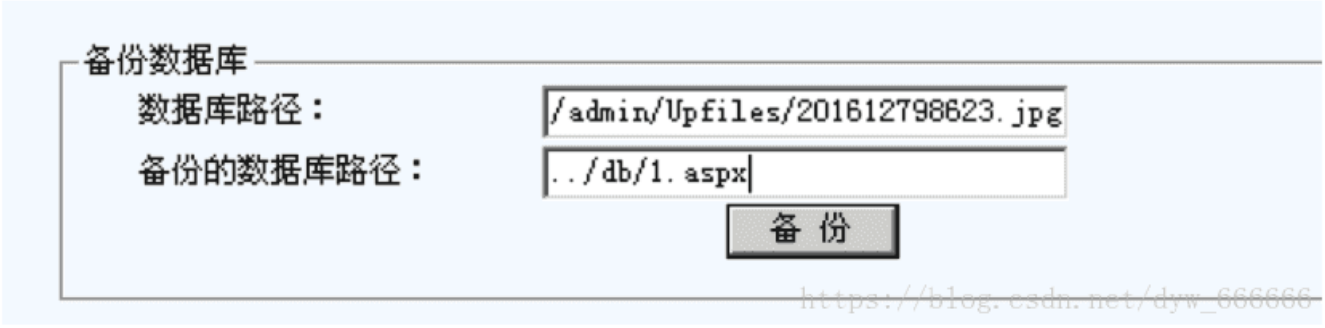
5.3我们把我们的木马更改下后缀名，原来的木马名称是mm.aspx,我们改为mm.jpg，然后上传，发现可以上传成功。如图18所示



5.4我们上传成功后，右键照片属性，看下它上传的位置，记录下来。如图19所示

5.5我们上传成功后，因为上传的图片，不能解析成木马脚本，正好我们的这个网站有备份数据库功能，我们可以通过备份数据的方式，重新命名脚本文件，使其能够作为木马脚本被执行，我们打开网站左侧的『数据管理』操作项，选择『备份/恢复数据库』。如图20所示

5.6在备份数据库中，数据库路径后面，填上我们刚才上传图片的地址，例：刚刚我获得的图片路 `http://192.168.1.3/admin/Upfiles/201612798623.jpg` .那我们在数据库路径后面填写『../admin/Upfiles/201612798623.jpg』.再备份的数据库路径后面我们填写『../db/1.aspx』.这样做的目的是把我们上传的jPG后缀的木马，重新备份成aspx文件，使我们的木马能够正常运行。如图21所示



5.7我们点击备份后，我们访问 `http://192.168.1.3/db/1.aspx`就是我们的木马地址了，木马的密码是77169,至此，我们就拿到了这个网站的webshell.。 如图22所示