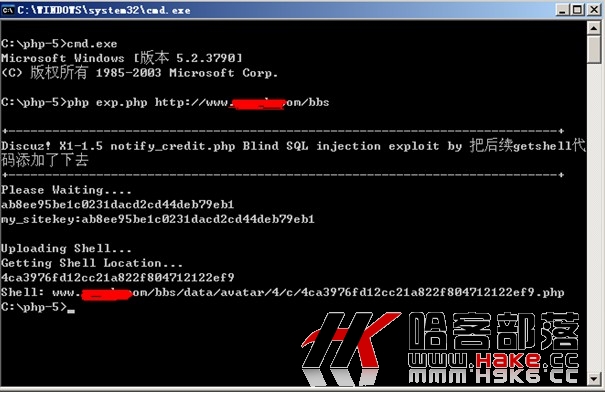
**文/图**

**作者:过河的卒**

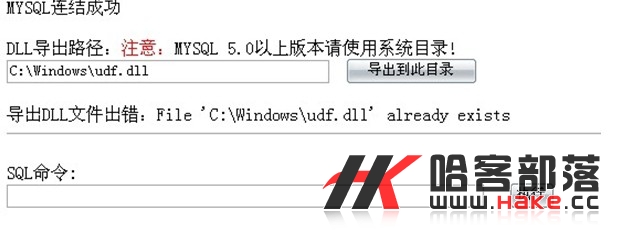
前几天闲来无事，朋友丢过来一个论坛，外观做的挺不错，像是一门户，仔细看了下有x1.5的论坛。立即上了toby57牛的oday，rp爆发成功写入一句话。



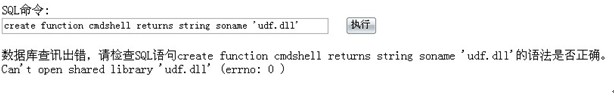
上了asp与php2款大马。我习惯配合着用，ws组件没有挂掉，服务器很配合的支持aspx，本想着提权就在眼前了，可是悲剧了。找到RECYCLER目录上传cmd与pr，执行pr程序卡死，免参数也一样。这条路已经走不通了，放弃。



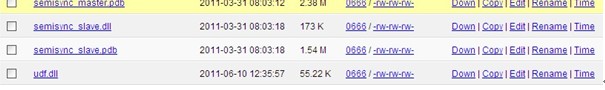
接下来自然而然想到mysql。于是找到config\_global.php文件，看到mysql用户名密码后大喜，上udf马连接成功。



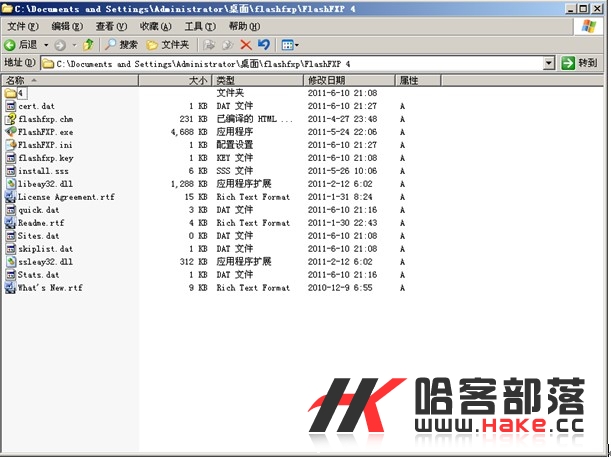
Udf已经顺利导出，然后开始创建函数，悲剧来了。出现了Can't open shared library 'udf.dll'



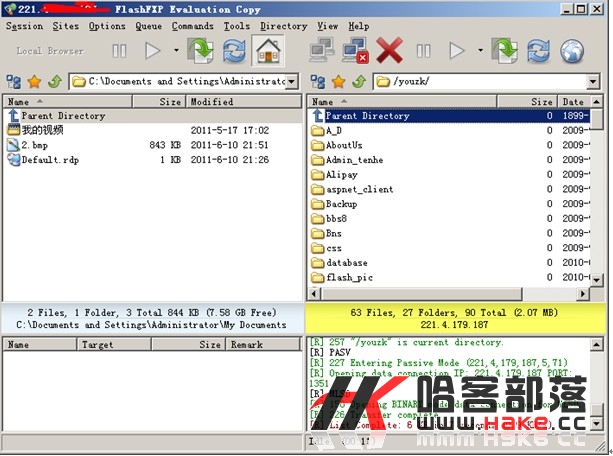
开始google，找到了一些办法，因为我对mysql不是很了解，看到资料上写到在5.1以及更高级的版本必须把udf.dll 倒入到mysql中的lib\plugin，然后创建函数才可以，还有5.1以及更高级的版本，不需要写dll的路径，不然会报错。按照教程顺利倒入。



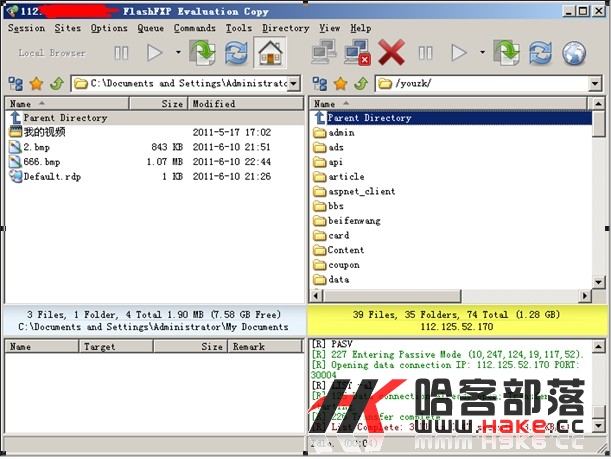
立即创建函数，依旧是上面的错误。这时候我有点抓狂了，怎么回事，rp不爆发了？貌似我天天给冠希哥还是敬香的啊，怎么不保佑我了。我又在网上找了很多mysql的方法，无一例外，全部失败。到这里了，敢问哥们你，你甘心么。我又看到它安装了360，想到用360五下shift，结果显示没安装360.，还有网上说利用mysql写入vbs到启动项，这个我不做尝试，因为要让服务器重启，你知道用什么方法，我不想。期间又想到利用搜狗输入法提权（我曾经成功了一次），但是没有搜狗，ser-u也没找到目录，思路一度停滞。我心想，我还就死磕mysql了，又在网上到处找，这样时间过去了2天，没有斩获。又在shell中翻看，终于找到了一个比较鸡肋的地方flashfXP，试试吧。下载quick.dat到本地放入fxp目录中



开始看历史连接记录，有一定可能拿到管理员用户密码，看到有 7 8 个历史连接记录，其中只有一个连接成功，利用星号密码查看器，顺利找到用户名和密码看目录也和我shell目录一样以为拿下服务器。

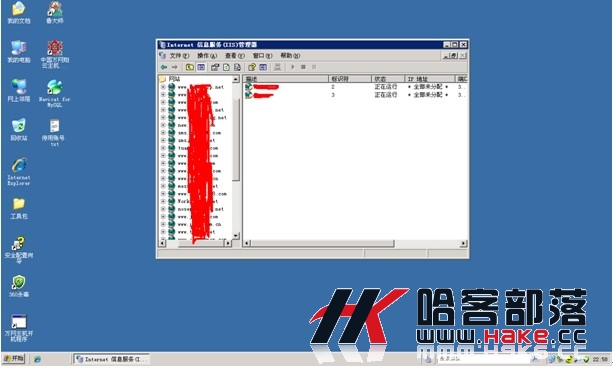


看了下端口改成了300xx，用这个ip连接，登陆失败。我又在fxp中找我自己的shell 这一找发现问题了，这个可能是原来这个网站的旧版，刚由于粗心错以为是现在网站，思路又一次中断。我想既然有这个，管理员肯定还会上这个网站去上传文件，等吧。运气这次可能眷顾了我，没过2天，我再次下载quick.dat在本地实验，发现了另一个ip。



这次仔细找了下我的shell，发现确实是现在的站点，利用星号继续查看账号密码。端口已经是300xx，当然现在只能看管理的习惯了，如果是管理员账号，那么我们成功。我再shell里面net user了一下 发现管理组就有这个账号，哈哈哈哈。立即连接，成功。自此服务器沦陷。





只是自己最后运气好，才能这么快拿下这个服务器，好了。文章到此结束，此文章只是技术交流，第一次写这种文章，写的不好，各种大牛勿笑，小弟拜谢