细心决定成败

今天和情书聊了会天

三句不离老本行；我XXOO 丢了几个单子来说要我玩玩

看了下他的站没办法弄

旁站吧

就是了今天的文章了

找到了入手点

<http://www.xxxxx.com/shownews.asp?id=145> 提交单引号

郁闷出现



大家都懂得 注入中转嘛

很快拿到帐号密码 这点我还是分开猜出来机子太卡了跑不起来我XX他OO



进后台了精良？靠

以为用以前的方法 上传那修改下上传路径把UploadFiles  
换成admin能爆出admin文件下的所有文件

一看我郁闷



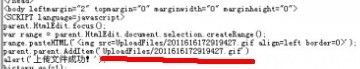
灰屏的没法写（注：有要那个修改上传地址拿webshell的我过会传上来）

不管多说先找上传吧

得到地上传的地址

有明小子试了下

郁闷没用



奶奶的

先把上传的看能备份不试试



MDB靠

丢一边去

。。。。。。。。。。。。。。。。。。。。。

省略N字

最后还是搞下来了

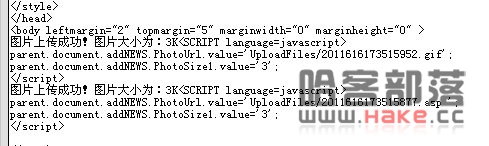
还是上传

在添加公司型像里面发现也有上传不知道是不是和刚才的那个上传

一样呢

报着试试的态度抓包上传了下

HOHO



可爱的ASP

马上连接看看



太可爱了

好了这算是拿到webshell了吧

呵呵

在看看网站情况去

正准备册马时发现



饿

不是刚才我们备份的嘛

我XXOO的

难道那个备份的MDB是假的

试着看看

还真是

好了就写到这

第一次弄这个语言水平就只有这样

我在这总结下

1：明小子上传不成功多换几个上传抓包试试有可能就会成功的哦

2：备份成功了显示MDB结尾的试试把MDB去掉连接试试（PS：数据默认加的MDB）

以上的是良精的系统，我拿过很多都是多找上传能拿到，但备份提示有MDB但真实却没有MDB尾的第一次看到难道是最新才有这种情况？有的跟我说下

谢谢