今天无聊时看到一山寨华夏黑客基地



2011-6-17 11:35 上传

[**下载附件** (53.27 KB)](http://wwww.hake.cc/forum.php?mod=attachment&aid=MjA1MnwxM2IxMmVlNHwxMzE5NzE1NTcwfDgxNTI%3D&nothumb=yes)

很牛啊

就对他进行了检测

老规矩

旁站



好像很远

找到目标站



(PS 这个站是个假的教育教)

ASP的我比较拿手

测试下后台还是存在的

这就不接图了

大家都明白

看了下站点有没有猪肉点 还是有



但被防注入了

听朋友说这类大多都可以COOKISS

RP还真好真存在

顺利拿到管理员帐号密码 进后台

大家都会 不会的百度大嫂查查



看到有备份

这下拿webshell 但是备份成功没大马

6.jpg

我就想了难道文件夹权限做了处理

我能不能重新换个目录呢

回到网站配置 上传目录设置admin

再次上传

备份

还是不行

突然鼠标查看了下上传文件管理

晕

他全部显成了ASP文件



这里面不是有问题

刚才是UploadFiles 换了个admin就爆出了ASP文件

看到那个admin0刚才用../admin0

备份的文件 难道这里面有什么不为人知的漏洞

说做就做

再次备份文件../asp.asp

提示成功 回到上传文件管理发理文件出现了

8.jpg

打开一看是数据库

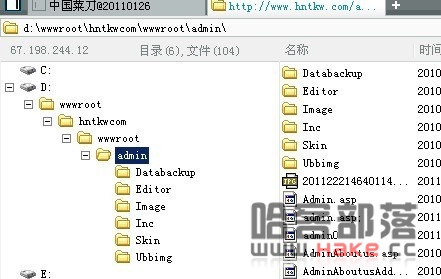
哈哈

这就好办了

随便找个地方写入一句话

再次备份数据库到../asp.asp

菜刀连接成功拿到webshell



文章到此也就完毕了

我是小菜

希望各位大牛不要见笑

PS；主要在于这站有一个上传配置文件不明爆出数据全文件