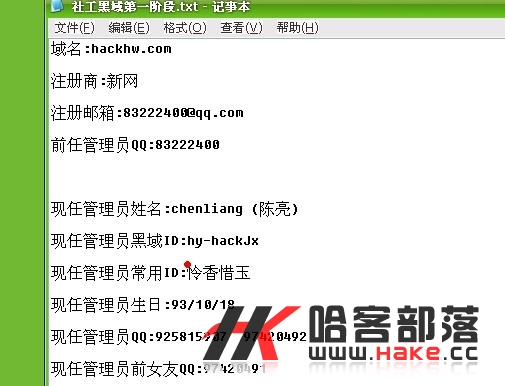
图/文

作者:小3鸡

本文出了不准对任何站长，只是说明，没任何站点是安全的

前几天被一个大黑阔站没事骂了一句，然后说，我的站你能日的下吗？还带了一句，我的站都没人日的下，这下好，悲剧了，我也不知道说啥了，就默默跑去看了。

一开始一个朋友貌似射到他一些资料了，不过资料让我很奇怪。其实就误导了我



当时我觉得悲剧了，这样的资料算神马社工哇。。 后来就不管了。自己跑去社了一天多，也只有一点点消息，不知道从哪冒出一个密码，特别悲剧，社的资料里，有个密码。可能是朋友社的，



这密码好经典，不知道咋说好，是管理2B还是啥的。直接登陆，居然进去了。！~！@

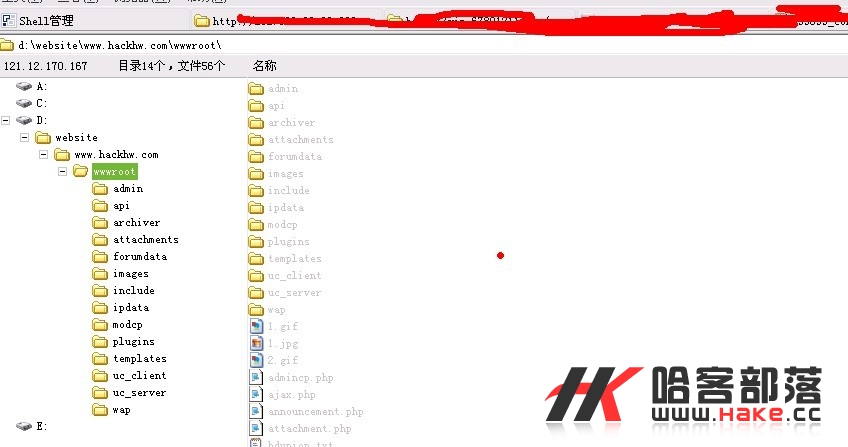
这后果严重了，连支持宝密码都一样。

进了他的后台，。是DZ 7.0的，百度多的是办法。随便找个方法

1.Ucenter IP插入一句话：hake\\');eval($\_POST[hake])?>;//

2. 然后返回刚才插入地方，随便替换几个字母  
  
3.连接文件是根目录下的 config.inc.php  
  
<http://localhost/dz/config.inc.php>成功插入

关于DZ后台拿SHELL的方法。  
这是关于 7.0至 7.3的方法.然后果断连接SHELL



拿到SHELL。这下他很悲剧，反正SHELL对我们没啥重要，拿服务器。

查看了一下配置文件，不是 ROOT。只能去找，权限大的去了。悲剧。翻完所有目录。找到 ROOT，果断下载DATA目录的文件，获取密码。

这三个文件，，然后就可以获取的ROOT加密文了，之后我们自己去解文明，至于人品，这就得看你自己了！

user.MYD

user.MYI user.frm



人品太好，解除来了。

123xxx123  
密码。

Root  
用户，

提权去，UDF

上传UDF。然后输入账号密码，提权的时候居然提示了



悲剧，无法导入？？？啥情况？ 回头检查了一下，

这有个详细方法。我们继续说我们下面的内容

PS:

---------------------------------------------

<http://www.hake.cc/forum.php?mod=viewthread&tid=4797&extra=page%3D2>

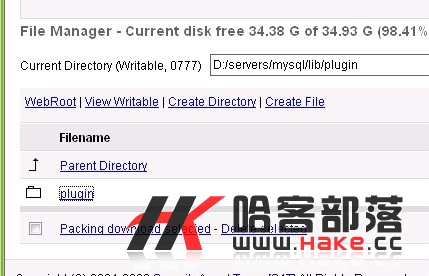
这有MYSQL 5.1提权方式。大家去看看吧。

-------------------------------------------

用大马去连接才知道是MYSQL 5.1的。MYSQL5.0与5.1提权方法是不一样的。



需要写入DATA目录。至于什么问题，这就得具体情况处理了



利用命令建立了一个目录 。。。然后进行提权看看

果断提权成功



至于你们想干嘛，我看你们知道的。。必须，黑阔都说过没人能格我盘，但我没那么贱。至于你觉得你牛B，我没话可说。果断服务器图  
 

大家别笑，我不想日他。但他做人很贱，很让人觉得恶心。还来一句，都没人能日我的站。

做人不能这么悲剧

好了。文章到这，果断挂首页，提醒黑客大站长，你的牛B站果断被日