**声明：原创文章，转载请注明来自哈客部落(**[**www.hake.cc**](http://www.hake.cc/)**），违者必究！**  
  
**作者：残剑**

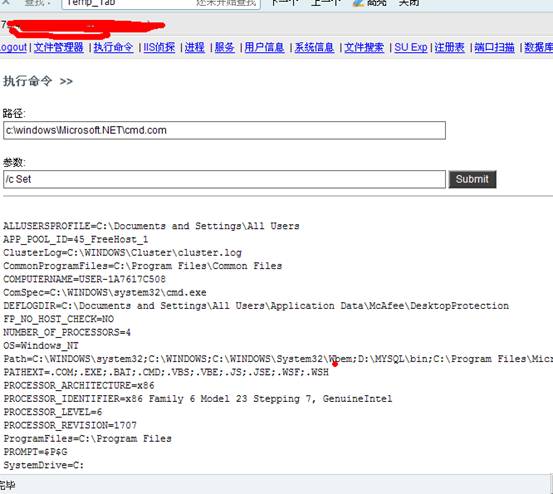
大家好,我是残剑。哈客今天就开放了,拿篇原创文章晒一下把

话说,今天检测一牛人的blog。Wp程序的,没0day,直接去旁把

看到一网站上有注册。登录后发现上传头像的地方可以突破直接上传php马，简单拿到一个旁站SHELL。支持.NET 支持PHP。权限挺大的,这权限是个好处，悲剧的是这是个星外。

不能列目录…更不能跨目录。。。。悲剧的要命



   
找到可读可写目录,上传了一个cmd执行  
 

从上面找到个MYSQL。目录。寻思着木有那么大权限访问吧？随手就尝试试试

天生就是个悲剧。居然能打开。你们懂的该干什么…

下载data/mysql 目录下的user.MYD user.MYI user.frm三个文件。

本地搭建mysql,寻找root帐密。这下好了,帐号找到了， 密码也解了

先想到的是UDF提权。大家都懂的。

居然有人来过了。还执行了。尝试去看了一下他的字段。是已经导出了的。但貌似执行不成功。就放弃了？不可能！

既然人家先来了。我们去了解是啥版本的数据库

用个PHP大马连接了一下

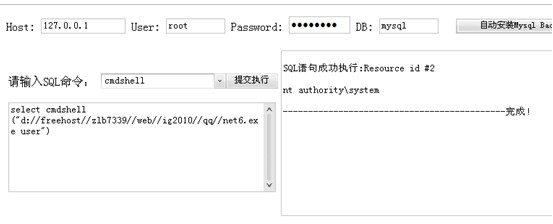
是 5.1 的。貌似mysql5.1的提权方法不一样

大家百度一下吧。我就不多说了。 需要找到当前的mysql目录 在lib/plugin  
目录下才才能执行函数

好。我们改一下导出目录。导到D:/mysql/lib/plugin

成功导出。看是否成功 执行一下函数看看



System 我想大家知道要杂做了。

服务器已经到手了。清理日志 走人

本文章只是总结经验，请大牛别笑