图/文

转载请注明：哈客部落  
www.hake.cc

作者：人生

晚上刚睡。明天要出发去地方，刚好。遇到个站，全部都是 帝国系统，这让我情何以堪啊。悲剧死我了

目标.  
www.fuck.com

然后找几个旁边随便看看。怎么看都是一个系统。帝国啊帝国啊。。我日。然后发现一个是5.1的。



漏洞也补了。无语啊。反正没事做，找wwwscan去扫扫。很卡。扫了一会。貌似出现了一个bbs/data/dvbbs8.mdb

数据库啊，激动赶紧下载。然后打开 [www.fuck.com/bbs/](http://www.fuck.com/bbs/) 果断是dvbbs8.2 高兴啊。上传漏洞。

然后去解密码。后台账号密码都一样。果断进后台



然后去前台。找上传漏洞。悲剧发生了。

userspace.asp?sid=0&act=modifyset  
Dv\_plus/myspace/script/filemange.asp

全部删除，难道是精简版不成！我日，忽然想起。博客可以设置php 上传，高兴的又跑后台去翻。



神马情况！！！！博客都没有！！！坑爹啊！！！！

彻底崩溃…想了想思路。Bbs前台 后台密码一样。去帝国后台试试密码？

[www.fuck.com/e/admin/](http://www.fuck.com/e/admin/)



留意悲剧的发生！一个密码发生的血案。从此就悲剧



果断拿SHELL

摸索了几分钟。发现个方法

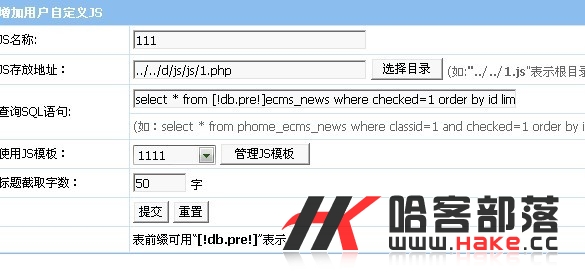
点击模板管理—管理JS模板---添加js模板



把PHP一句话写进去 然后



增加JS



内容如下。选择模板。重要的一点。Js存放地址改成1.php后戳。否则就是js.

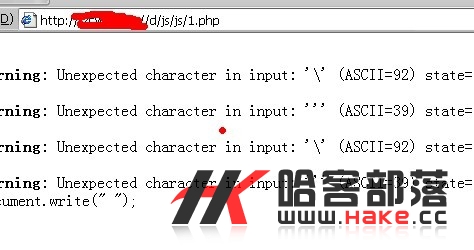
然后预览



之后地址是靠js.php直接调用。我们删去。



访问



报错了  然后连接  密码 c



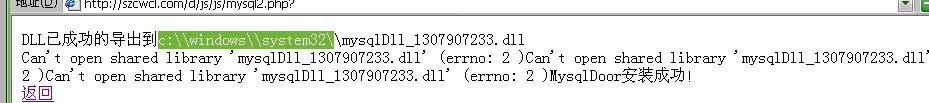
拿下SHELL。。

然后测试一下脚本。忽然发现他全部都支持。让我情何以堪啊

Aspx 直接列IIS 翻目录直接翻了ROOT



5.0 的mysql 提权方法就用udf



提示安装过。就代表有人来过了吧？



然后去看，确实。前三个月人家就来了一次

换了个免杀的 dll  
然后改函数，还是发现不行。之后连接了mysql才知道。



发现吭爹了。这是5.1版本的，。真折腾

再次去改udf 大马的代码。悲剧啊。改了路径。导出。就是写不进去。纳闷了。然后去建立个目录。有写入权限，然后尝试把朋友的dll上传。直接被杀。这下。搞懵我了。

之后发现被杀的.dll 叫朋友免杀。然后转换 16进制.导入

D:/MySQL/lib/plugin/

然后点一下提交



成功了。他成功了。我鸡冻了！！！！到这就不继续了。不喜欢破坏。最终，一个密码造成的血案哇

小菜出文章。大牛勿笑。有问题可以点出。但别指指点点！！