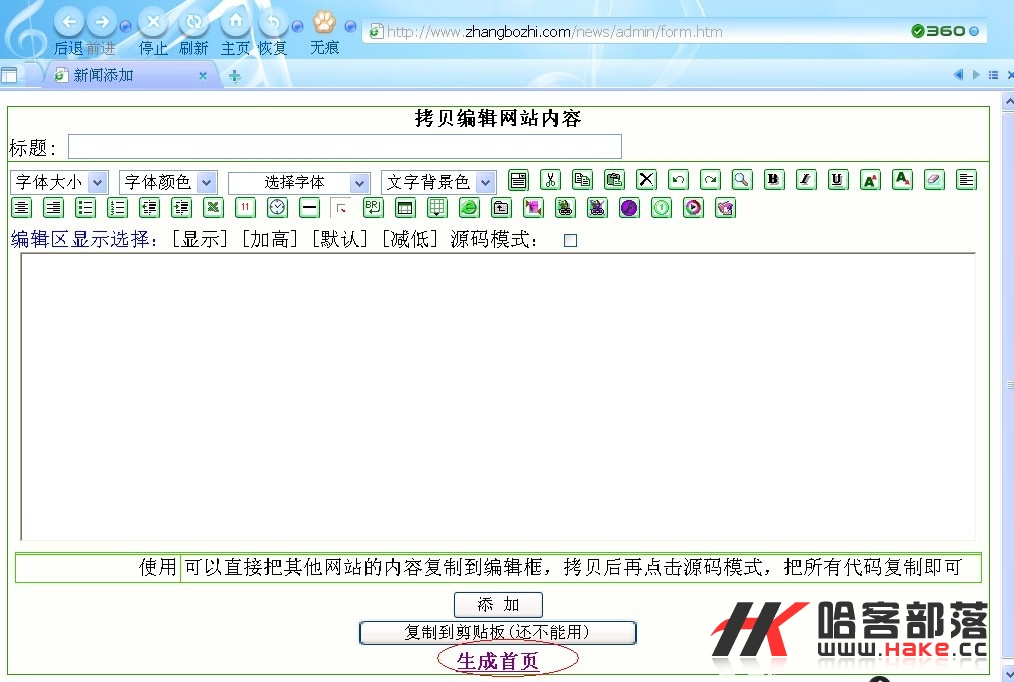
声明：原创文章，转载请注明来自哈客部落([www.hake.cc](http://www.hake.cc/)），违者必究！  
  
from: [www.hacke.cc](http://www.hacke.cc/)  
  
今天一时兴起,想太阳个明星的官网玩玩   
这不,心里一思量就想到了我们的柏芝姐姐从前,有一个美女....  吖的。跑题了,, 回来  
我们继续~~  
百度找到张柏芝的官网  
   
  
   
  
简略的踩点了一下。发现大部分都是html的静态页面,也没办法下手。看这外观又有点像某个cms的样子。  
随即想看看googlehack能不能找到后台地址。查出程序版本..好对症下药！  
   
看到了把，懂得人都知道这是目录遍历。同时还发现了网站有用aspx的语言程序。  
   
  
  
 

看到生成首页这边。脑子里突然想到一个思路。不是尘缘雅境有个版本可以在某个文件插入一句话。然后生成首页 用一句话连接的么。但是后来想了想,他生成首页后的文件不懂是哪个。况且还不一定插的进去.索性放弃这个思路了,

又看了一下其他的几个目录,观察了下目录中的文件。并没有发现有什么可以值得利用的、

没办法！旁吧,

旁之前。我随手查了一下服务器信息。居然是linux+apache。我刚开始看到目录遍历以为是iis的呢.  
 

（Ps:在后来的过程中我一直以为是iis6。解析漏洞搞了半天,一直不成功。后来想起来服务器用的是阿帕奇。唉！入侵中细心是件好事啊。不然会绕一个大弯子）

继续。

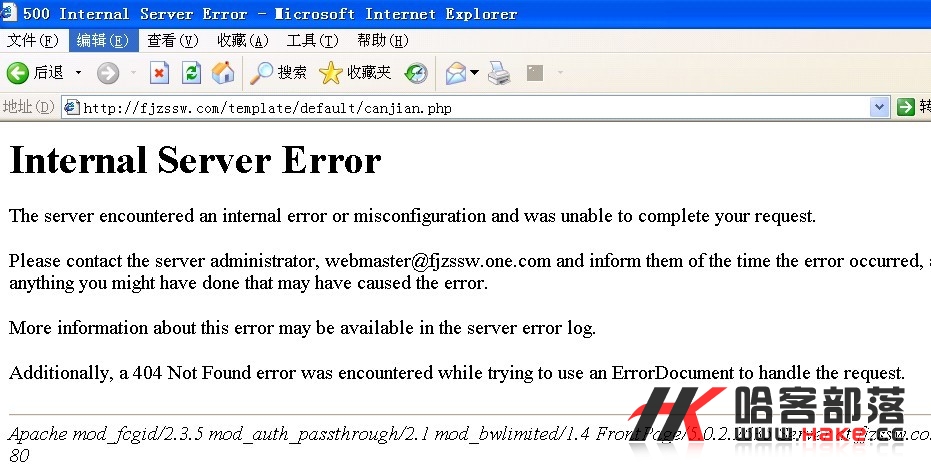
找到一个同服的站。Robots.txt查找敏感信息

Cmseasy2.0版本的。进入后台页面,尝试性的测试几个弱口令。没想到竟成功登录

接着在模仿管理-编辑当前模版-在模版中插入php一句话。在保存的同时抓包，把抓到的包\_left\_html改成cajjian.php。利用nc进行上传

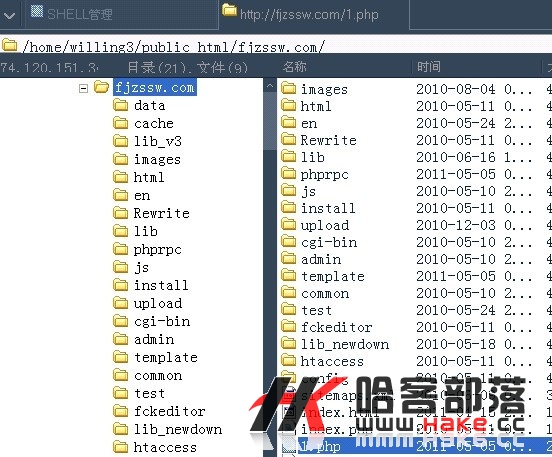
上传之后发现服务器显示500错误。

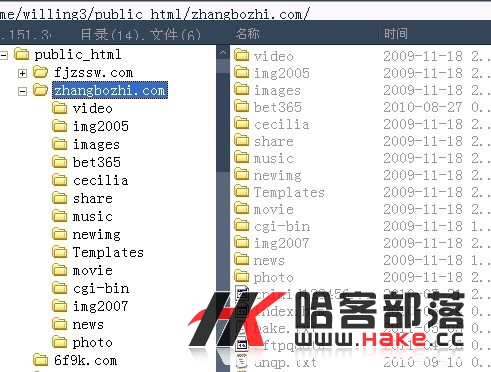
后来用1.Php;1.jpg，1.php;.jpg等各种后缀尝试上传。均宣告失败！接着又用了txt后缀上传,内容正常显示。心里思量着,马儿肯定是上传上去了，可能是服务器对上传的php文件进行了过滤。也可能是管理员对目录做了什么设置。索性更改了上传的目录,直接把马传到网站的根目录去。



用菜刀成功连接！



虽然是Linux系统,但是目录权限设置不当。直接跨目录。连提权都免了…



入侵过程中思路最重要。我发出过程是本着共享的精神,希望大家不要做任何破坏