文章作者:lost  blog:lost.cq.cn  
尊重别人，尊重自己，请不要因为区区的一篇小文而践踏自己的人格，谢谢您们的支持、理解和合作！  
  
在我的印象里，社工就是忽悠人，有时候在你渗透的时候知道了管理密码。但是你不知道后台吖。没办法吧。  
  
你在怎么渗透也要找地方去上传webshell吧。  
  
我就碰到一次，管理忽悠我，忽悠了我3天。说到找后台，我给大家说说找后台的经验。  
  
就是上次渗透的时候管理密码都知道了。他网站有一个默认的后台admin.  
  
但是我知道的密码登陆不进去，头痛阿，那站必须拿下的，是一门户站。管理把我忽悠了。去注意那默认后台。  
  
我那两天以为是我爆出来的密码是其他站的，mysql5.0的数据库麻，直接爆出库来。我在数据库里转了两天。  
  
我把点仍朋友了。他说web分离，距我经验不可能分离的，我给他说还有一个后台他不相信。我说你没找到当然说没有。  
  
后来我找到了。我在网站首页查看图片，/Article/UploadFiles/200907/20090723201120157.jpg  
  
你可以去试下<http://lost.cq.cn/pass_admin/> 结果还真是后台。  
  
其实你开原在网站首页去查看原代码，查找下敏感的信息。也许那就是后台了。  
  
后台忽悠完了，我们回到主题，也是渗透一个大型门户站的时候，获得密码了，前提是没找到后台。  
  
权限不可以读写，mysql4.0,不是root，更不要去找phpmyadmin了。  
  
什么方法都使完了，没办法了。只有社工网站管理员了，  
  
最后在WEBSHELL上得到后台路径的。  
  
我直接把我的马给管理员，让他自己放上去 。  
  
我说他的站有漏洞，我写了一段修补。关键是看你对他了解多少。  
  
基本上我看下就知道他是用什么过滤方式来过滤，然后我会问他他的过滤文件是不是这样写的。  
  
然后我在说我已经得到他的账号密码了，告诉他我没有恶意的，只是安全检测。  
  
账号密码报给他了，他一看确实是，从心里上对我的防范就很淡薄了。  
  
然后接着攻心。故意问问过滤代码是不是他写的，接着问问他网站的一些情况。  
  
最后在说我是专业做安全维护的，如果以后有需要可以找我。顺便把价格也给报上，达到迷惑管理员的目的。  
  
走之前顺便问他会不会修复漏洞，一般都不是很清楚，即使他说会，你可以套出他是怎样修复的。  
  
社工的方法太多了　，前题你手里要有他的站点的一些隐蔽的信息。  
  
搞这个站的时候我都想过找个兼职妹去社工... 忽忽。。。。。。