图/文

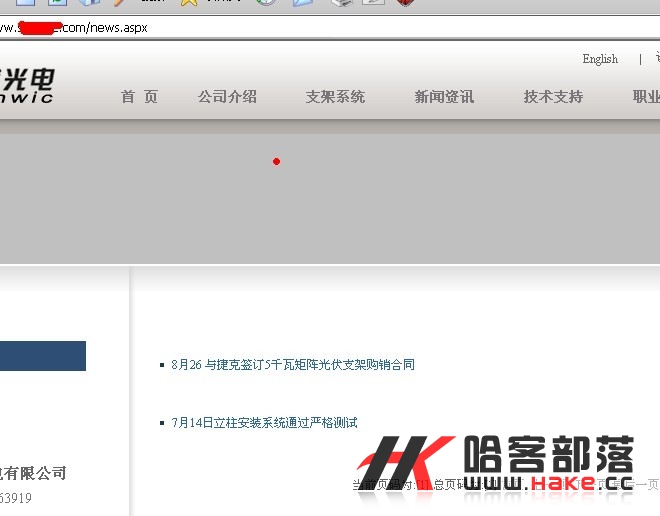
作者:人生

   这是我遇到的一个站，把经验分享给大家把

    好了。下面是内容

  目标是: [www.stanxxxx.com](http://www.stanxxxx.com/)

      站点是aspx的



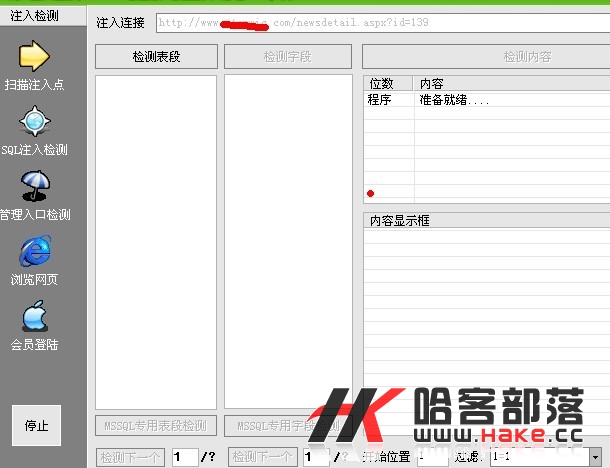
   存在注入点，



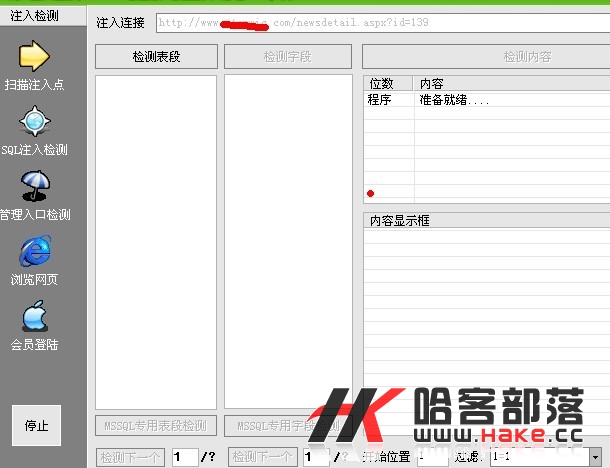
经过分析，该站是ACCESS。我们先注入一下跑一下表吧，如果猜不到表我们用工具跑



但在猜表的时候 没有admin 也没有常见的表类型，就靠工具跑一下



因为有时候很多表我们是不知道的，就靠工具跑一下吧，这时候手工会死人的



跑完了，什么表都没有。。。。这下纳闷了。跑去找T00LS 某大牛咨询一下。。。也没得出任何结果，，，就跑去睡觉了。。

  第二天起来的时候，回头看看这个站，发现一个很强大的结果。。

回头继续看那个注入点忽然发现如下



发现一行语句

是查询文章的 表名也发现了  
j1\_Refer 这给我们很大的提示啊。然后想到这样会不会以j1开头

然后后面是其他表明呢？ 就试了一下，结果得出，完全是意料之内的。。



J1\_User J1\_SYSTEM 测试发现这几个表。



结果，想继续猜下去，这回又给我出了一个难题，，结果猜了N久就得到密码而已。这下让我很是头疼。。。



用户表也没猜到。。。  这下想起来的更悲剧，，，，连后台也没找到。。。。汗了。这下思路完全死在这里了

  忽然联想到这回不回与这表名有关呢。。。 就胡乱想。胡乱试。。。。

10分钟过去了。。。。20分钟过去了。。。。。。1小时过去了。。。。。。。啊啊啊

不知道咋输入了 j1\_login.aspx



强大的后台居然出现在了我们眼前。。。。好悲哀。这什么鸟系统。。。

就测试了一下’or’=’or’ 和 “or”=”or” 因为是习惯。就随手试了一下

没想到’or’=’or’ 竟然进了后台。。。



靠，哪我猜不到用户表算什么鸟毛啊。。理个操啊。。。浪费哥一天时间不说，结果到最后这套程序完全只靠一个编辑器。连个上传都没有。。。

忽然想起登陆界面有个公司，就尝试找哪公司的人，想从哪里得到这套系统来研究



直接打开是一个建设网站公司

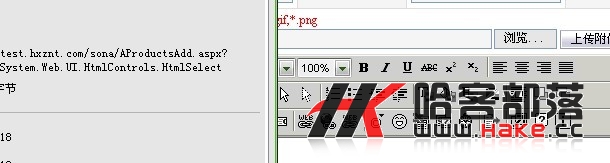


然后去骗了一下客服

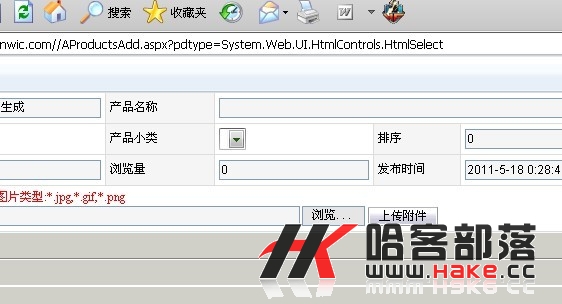


给了一摸一样的程序。进去看看。后台我们也知道了。

进去结果发现一个上传。但另一套程序上面没有。



结果测试一下，一摸一样



但是到了最后还是以失败告终。。。。。。

好了。本文章讲的是经验至于SHELL拿不拿到就是另一回事了。重说完了。

大牛勿笑，小菜只是路过。。。。