图/文

作者:小辉

后台Union注入绕过验证

话说网上的关于UNION绕过后台验证的有很多，但大多是拿到源码的分析（教的是个思路..）

昨天朋友扔了个站，看了看，没啥利用，就旁一下吧，找了几个站，都没常用可以利用的，郁闷了，我难不成要去C，NO!好漫长….

找到一后台，输入默认密码，报错



看见了错误错 '80020009', asp程序中常见的BOF和EOF有一个为真，或记录集被删除，直接可以看出是可以直接后台绕过的,下面开始构造吧…

因为程序是会多内容框的长度做限制的，而IE是无法源代码的，拿出Opera浏览器，构造吧



将maxlength的长度改大点，应用修改，----------------------------------------------

说下UNION的语法吧，当以查询语句前为假的时候，就可以使用UION语句替换前面的查询（我是这样理解的，估计不专业）

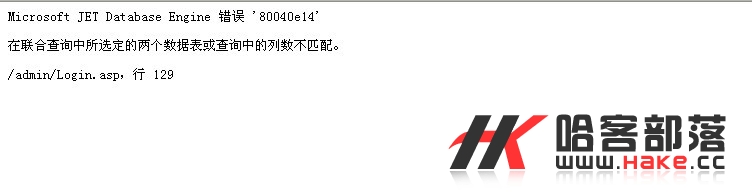
先构造个语句and 1=2 'union select 1,2,3 from admin where 'a'='a出错了，如下图;



看来是表不对啊，试了System,manage,web\_admin均没有结果啊，一样报错，突然想到用use试试！如下图：



哈哈，成功获得表名，下面猜有几个字段吧！如下语句：and 1=2 'union select 1,2,3,4,5 from use where 'a'='a



看来字段不对啊，杯具了，继续，将字段加到十几了，还报错，晕啊，突然想到自己烧饼了，呵呵，怎么就没想到小于5的字段个数呢，用到三的时候，哈哈，成功（and 1=2 'union select 1,2,3 from use where 'a'='a）

说是密码错误，就对了，

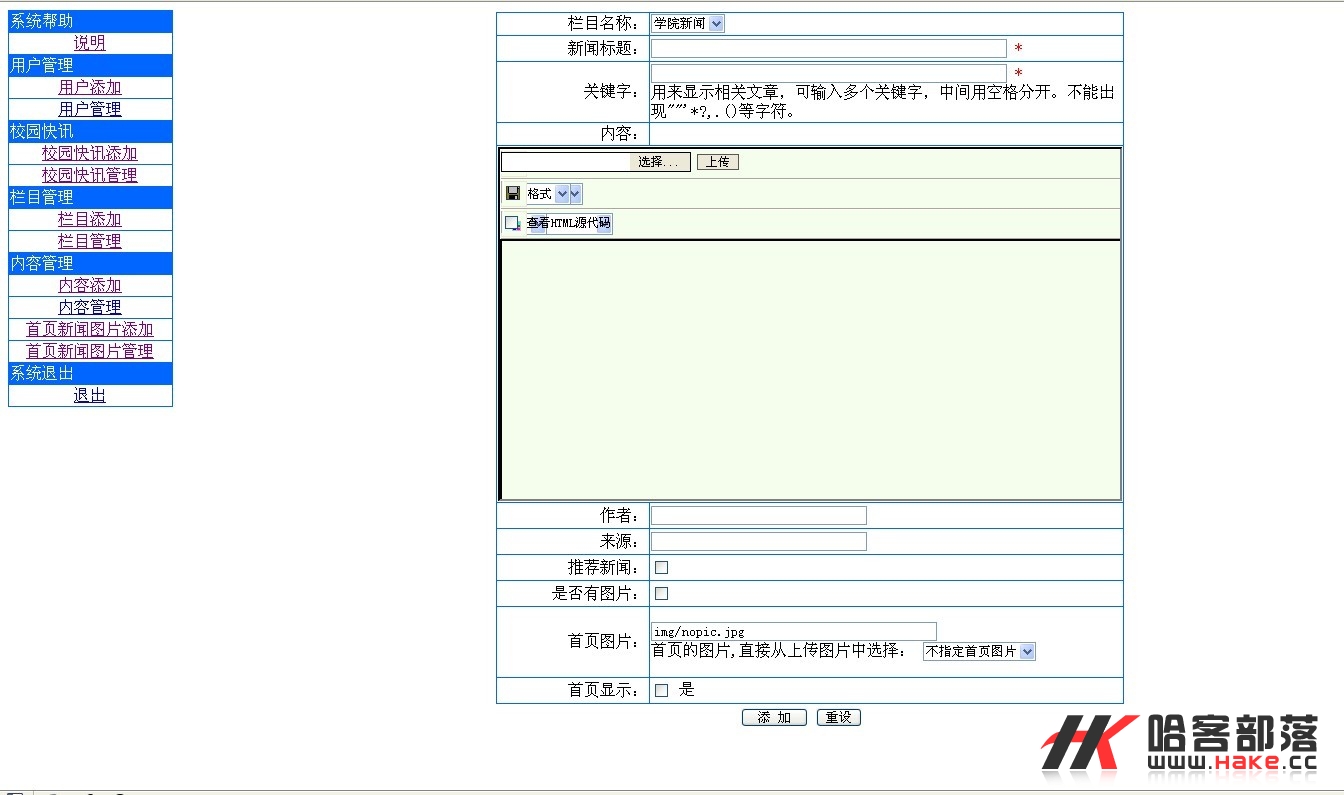
下面整理思路，既然是三个字段，第一个差不多是ID啥的，后面的就是用户密码了，构造语句：and 1=2 ‘union select 1,’admin’,’admin’ from use where ‘a’=’a 密码就输入admin

NND,还提示错误，晕，又一次烧饼，密码肯定是加密的了，继续

用户名输入: and 1=2 ‘union select 1,’admin’,’ 469e80d32c0559f8’ from use where ‘a’=’a

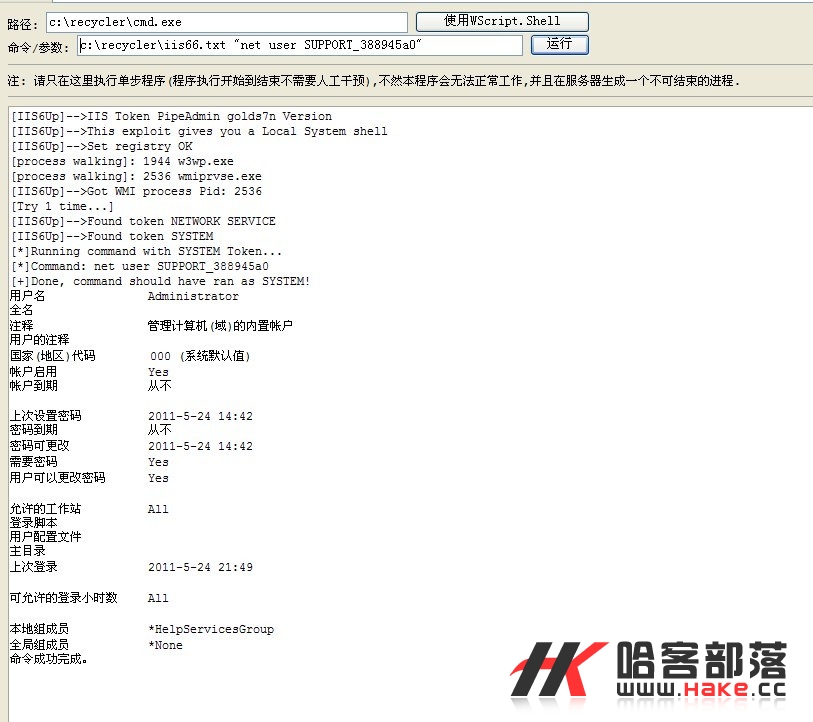
密码就输入:admin888(469e80d32c0559f8是对应的admin888的MD5)

试试吧………………..成功进入后台，如下图：



看着后台好杯具啊，话说我出道的时候美工也没这么差，哈哈，题外话啊，管他啥后台，能给我们SHELL的后台就是好的后台，呵呵（多希望你一进后台就会有一页面显示，“既然都来，就请黑阔们留下自己的马儿吧，我也在C盘回收站给你留下了可写可运行的目录，哈哈，玩笑了，继续）

下面拿SHELL的也就不说了，有上传，抓个包得到了SHELL。。



克隆个账号，搞定，服务器的页面也就不截了，是可以直接登录的。。。。。。

好了，这篇文章的关键是如何绕过后台，大牛勿笑（无视呵呵、、）