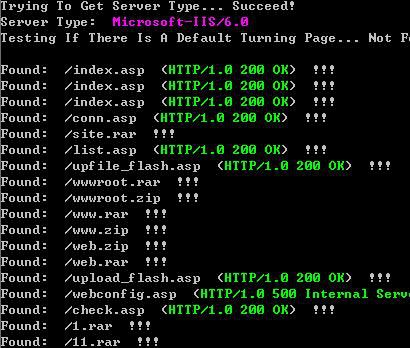
[)](http://www.cqzh.cn/post/IIS%E7%9A%84%E7%95%B8%E5%BD%A2%E6%96%87%E4%BB%B6%E6%BC%8F%E6%B4%9E.html)

**分类:**[**转载文章**](http://www.cqzh.cn/catalog.asp?cate=9) **| 评论:1 | 浏览:141**

**另类拿SHELL方法(IIS的畸形文件漏洞)**

作者：杀虫剂   
出处：BHST安全小组

很多人知道也有很多人不知道科普知识，以下地址已做处理，话说在拿一个站SHELL提权，首先用WWWSCAN扫描敏感信息如后台，数据库，网站备份等信息不多还好扫到了个上传页面！看看能不能利用



打开http://www.fuckyou.com/upload\_flash.asp出现一个上传页面，先上传个JPG图片测试下



连图片都不能上传，没这个道理啊.继续打开刚才的上传页面点右键查看源文件。来到上传模块这行

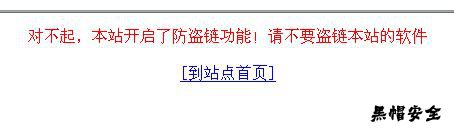
name="filelx" value="">可以看到这里为空没有上传格式，我们把它补上，地址也修复顺便利用IIS的畸形文件漏洞上传木马，最终修改如下



把修改好的页面保存为HTM或者HTML格式在本地，由于网站没对外数据进行验证上传一个JPG格式的ASP小马成功



本以为这样就完了，输入小马路径；提示本站开启了防盗链功能！请不要盗链本站的软件



问了下BHST里的人，有人给出了解决方法：清空IE输入

javascript:document.write("<a href='http://www.fuckyou.com/a.asp;120105413464824237.jpg'>fuck</a>")

页面会显示一个fuck字样，点fuck进入我们小马页面



逍遥复仇：又是一篇技巧类文章，我不明白一点，既然没有上传格式，直接添加asp后缀上传马不行吗？

看过以上内容后再看本博客的这篇《[一上传漏洞的探讨结果](http://www.cqzh.cn/post/193.html)》灵活灵用，下次碰见就可以搞定了！