文件上传 html 嵌套 xss 语句

0x01 漏洞描述

在我们文件上传的时候很有很可能会遇见无法上传马子的情况，我相信很多人在这个时候都会直接不管这一个上传点，然后在企业 src 里面这样的上传点可以试试上传一个 html 文件配合 xss 语句，导致一个挂黑页弹窗的危害，在众测里面达到了中危的标准

0x02.漏洞测试工具：

Burp　html 配合 xss 语句的文件

```
<!DOCTYPE html>
<html>
    <head>
        <title></title>
        <meta charset="utf-8">
        <script type="text/javascript">
            alert("testxss");
        </script>
    </head>
    <body>


    </body>
</html>
```

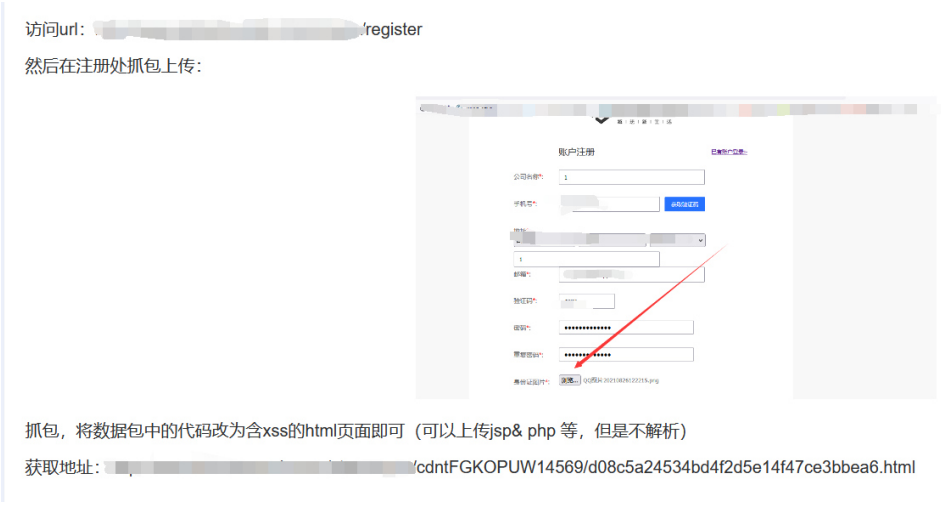
漏洞点及测试方法

漏洞点：存在文件上传的地方

测试方法： 在文件上传的时候上传 Html 嵌套 xss 语句

0x03 案例 ：

在某安的一次的众测活动中，看见一个营业职照的上传点，能上传马子但是不解析，于是随手改为 html 上传成功。赏金（800r)

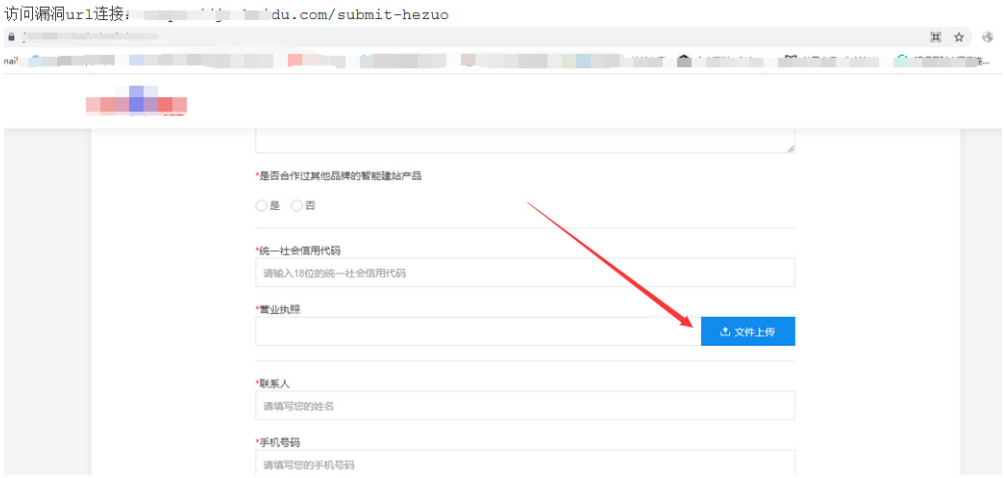


最终获取中危等级 800 元

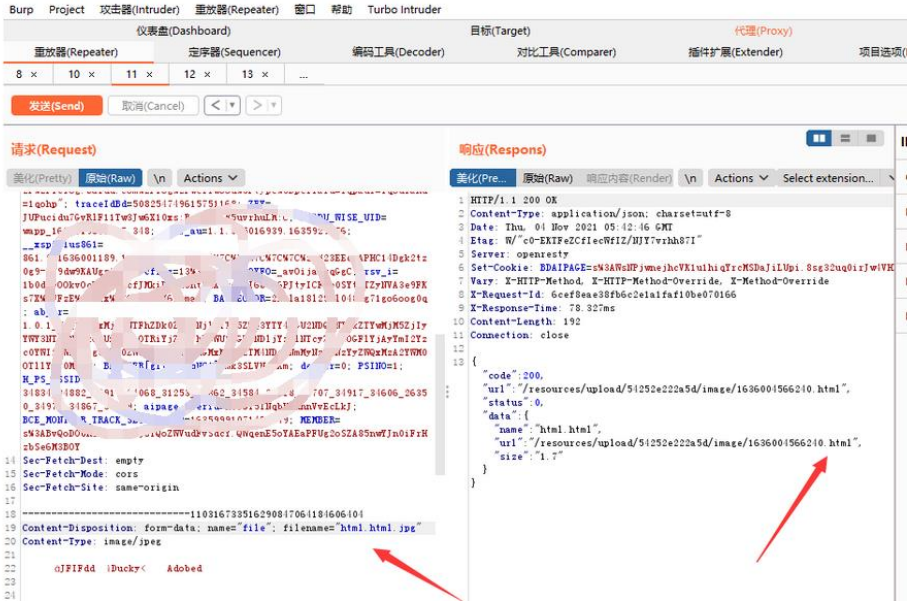
案例 2：某度的文件上传 xss（赏金 100r）

漏洞状态	待用户复查
漏洞ID	[redacted]
漏洞名称	【火线npctnzs8ba3b】百度[redacted]存在存储XSS
漏洞链接	[redacted]/submit-hezuo
参与活动	高校挑战赛 | 第三届百度大学生网络安全技能大赛
漏洞类型	应用漏洞 >> XSS跨站脚本漏洞
提交时间	2021-11-16 10:01:43
危害自评	中危
审核等级	中危
奖励安全币	20

同样的在页面找到文件上传的地方



2.将准备好的图片xss上传（此处绕过waf是图片头加.html.jpg即可绕过，大小写php，jsp可以绕过）



3.然后访问：https://[redacted]/upload/54252e222a5d/image/1636001837455.html