### 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>

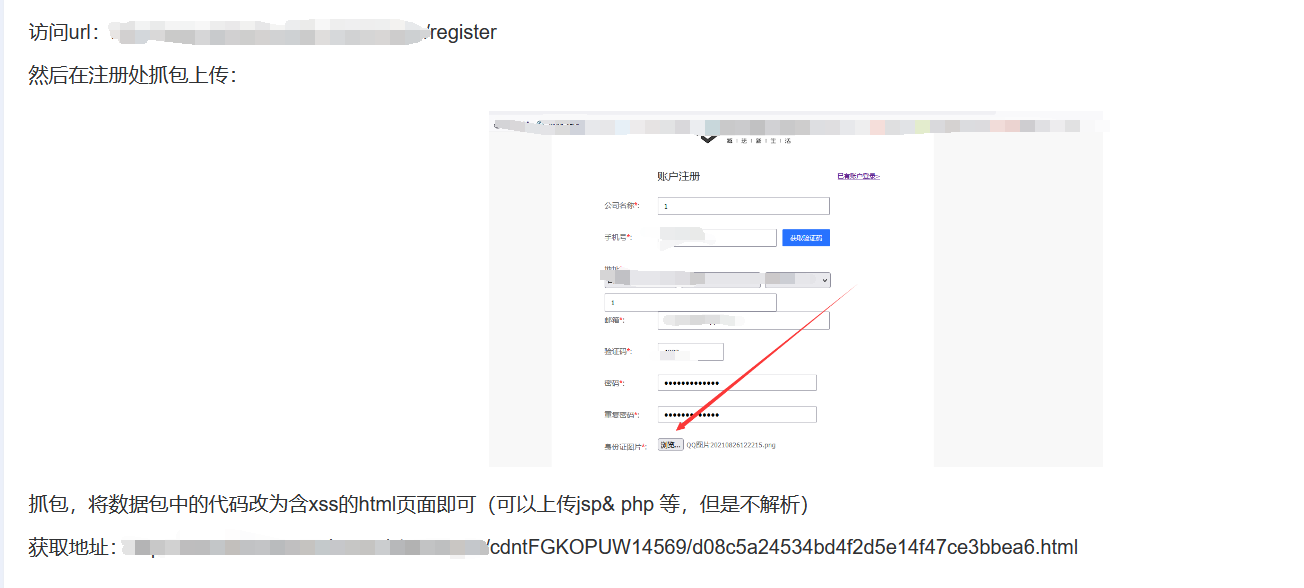
漏洞点及测试方法

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

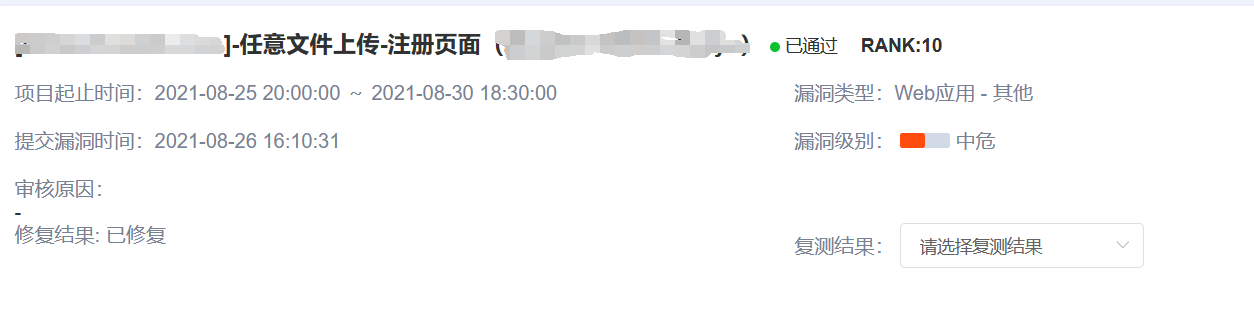
#### 0x03案例 ：

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）



同样的在页面找到文件上传的地方

