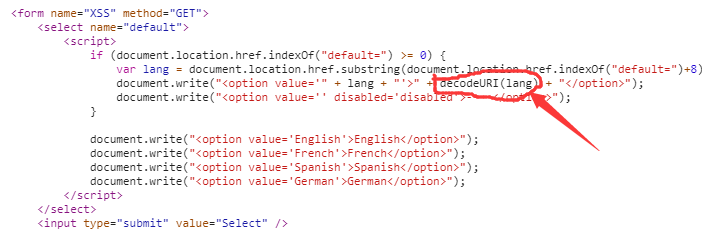
# XSS(DOM)

　　XSS（cross site scripting）跨站脚本为了不与网页中层叠样式表（css）混淆，故命名为xss。黑客将恶意代码嵌入网页中，当客户网文网页的时候，网页中的脚本会自动执行，从而达成黑客攻击的目的。DOM漏洞是基于文档对象模型Document Objeet Model，DOM)的一种漏洞。DOM是一个与平台、编程语言无关的接口，它允许程序或脚本动态地访问和更新文档内容、结构和样式，处理后的结果能够成为显示页面的一部分。DOM中有很多对象，其中一些是用户可以操纵的，如uRI，location，refelTer等。客户端的脚本程序可以通过DOM动态地检查和修改页面内容，它不依赖于提交数据到服务器端，而从客户端获得DOM中的数据在本地执行，如果DOM中的数据没有经过严格确认，就会产生DOM—based XSS漏洞。

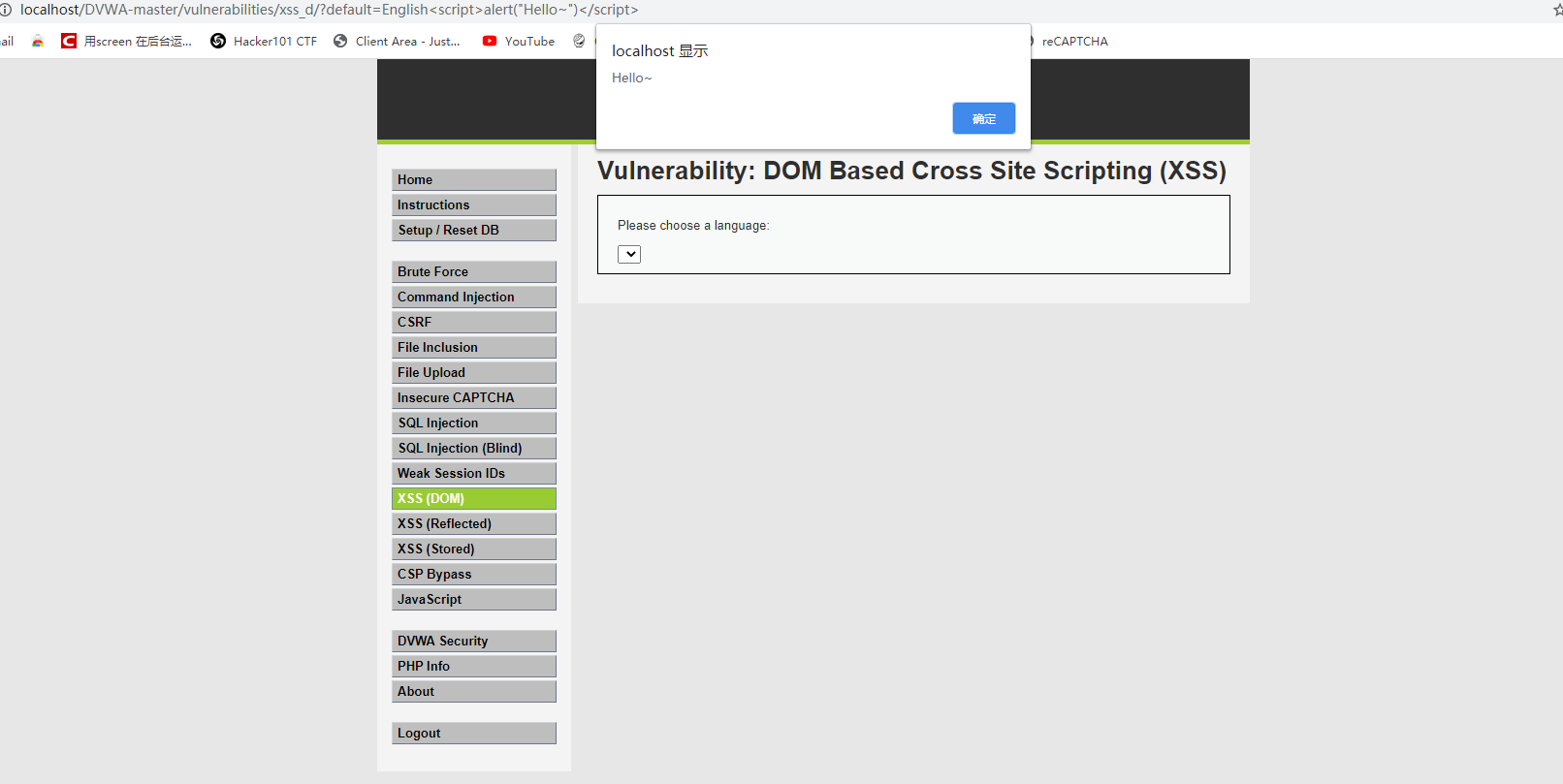
# Level:Low



可以在javascript代码可以再URL执行

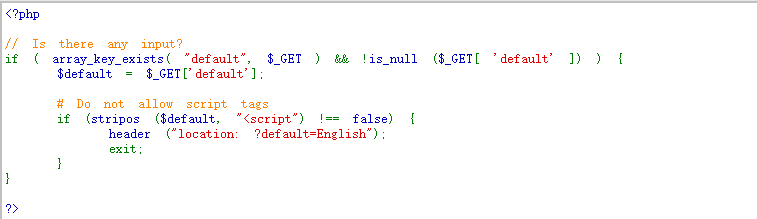


Low级别没有任何防护，所以可以尽情XSS

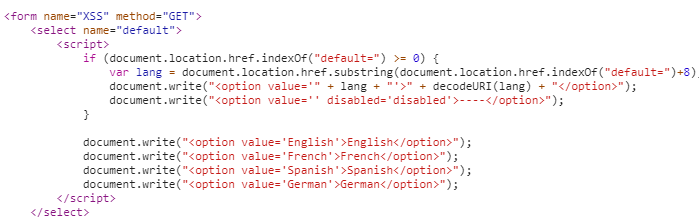


<script>alert(“Hello”)<script>

# Level:Medium

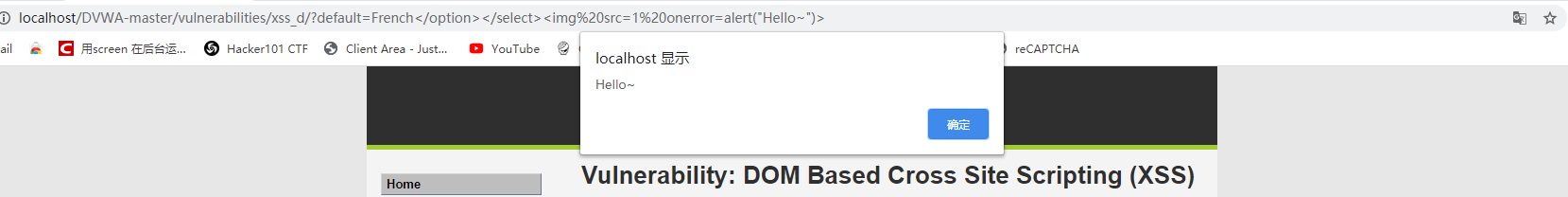


Medium级别的源码把</script>标签给过滤了



再根据这段JS闭合</option>和</select>这两个标签再用<img src=1 onerror=alert(“Hello”)>

插入，onerror事件是如果错误了就执行javascript



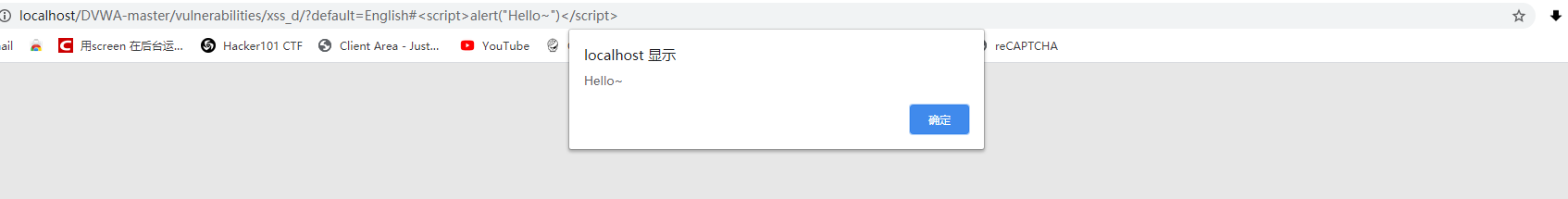
# Level:High



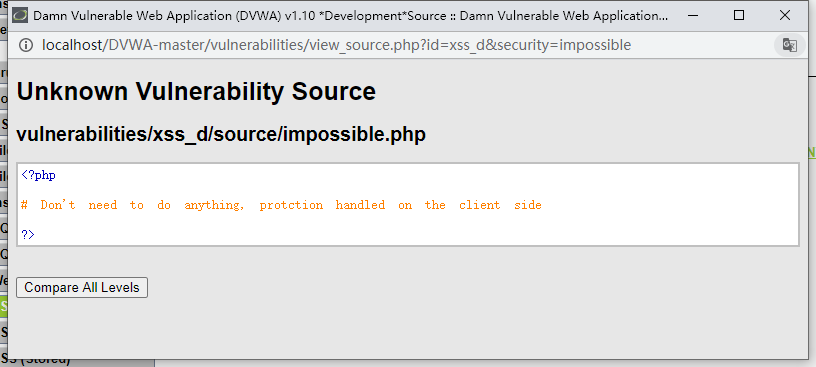
High级别的源码用了白名单，只有GET请求到的值default值是French、English、German、Spanish上传

这样可以用#注释掉一部分代码不会传到服务器，这样也符合白名单的要求了

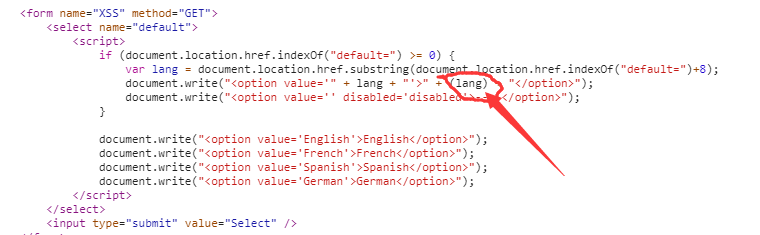
#<script>alert(“Hello”)</script>



# Level:Impossible



不需要再服务端做任何防护



网页源码变了,变成不可以在URL执行javascript