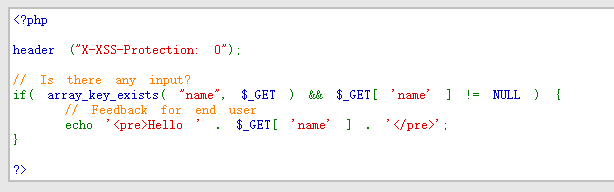
**Reflected Cross Site Scripting (XSS)**

# XSS(反射型攻击)

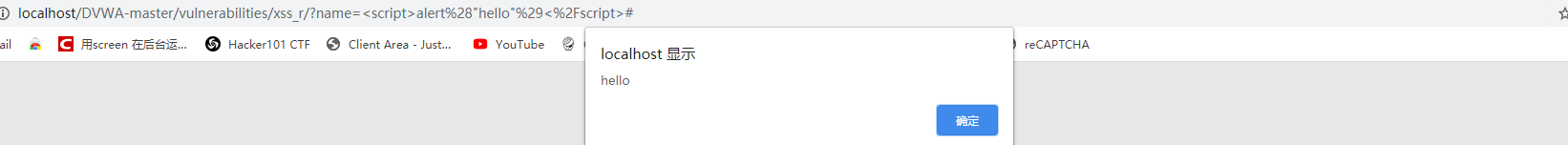
非持久型(反射型)跨站脚本漏洞是最基本的web漏洞。当web客户端提供数据时，就会出现这种漏洞，常见于HTTP查询参数(例如，HTML表单提交)，服务端脚本在没有正确过滤请求时，就立即解析并展示页面结果给用户。  
因为html文档是流式结构并且混合了控制状态，格式化，真实内容，结果页面中包含的任何未经验证的用户提交数据，如果没有正确的进行html编码，都有可能导致标签注入

# Level:Low

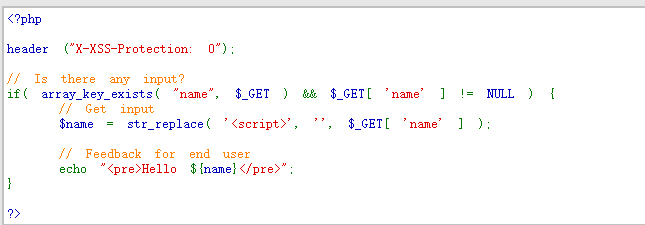


Low等级的源码意思是如果接收了name值的GET请求执行成功了就输出<pre>标签里的Hello和name值

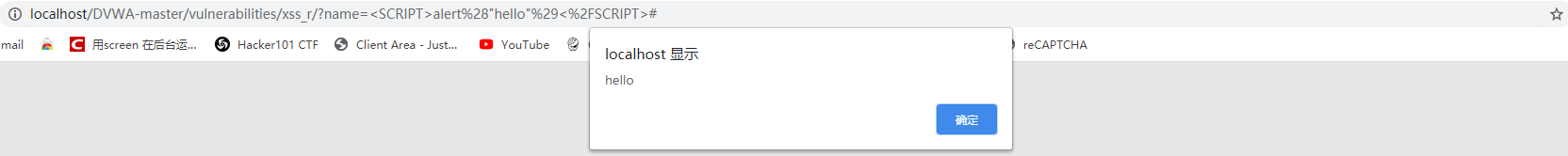
因为没有对javascript的代码标签进行过滤所以可以直接用<script>alert(“hello”)</script>进行注入



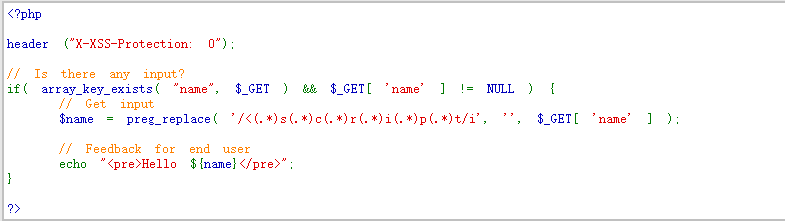
# Level:Medium



Medium等级的源码，这一次是对<script>这个标签进行了过滤，但是没有对大小写过滤，所以可以用大写来进行注入<SCRIPT>alert("hello")</SCRIPT>,



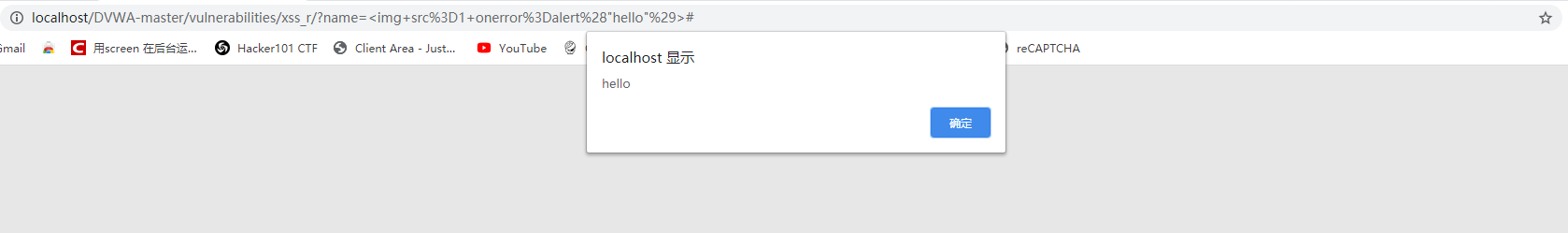
# Level:High



High等级采用了正则表达式的黑名单搜索匹配和</script>相关的字符串给过滤成空置

这次大小写和大小写混淆都不行了，所以换使用img的onerror事件，onerror事件是如果执行不成功就执行javascript

<img src=1 onerror=alert(‘hellp’)>



# Level:Impossible



Impossible等级的源码先判断name是否为空，来防范CSRF攻击不为空的话然后验证其token用htmlspecialchars把name值给HTML实体化了，防止注入HTML标签