**Stored Cross Site Scripting (XSS)**

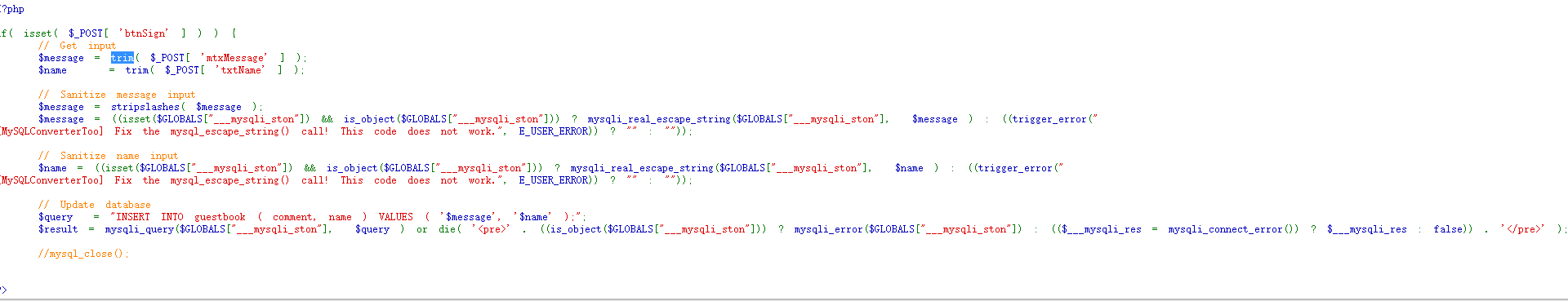
## 存储型XSS

存储型XSS又被称为持久性XSS，存储型XSS是最危险的一种跨站脚本。

存储型XSS被服务器端接收并存储，当用户访问该网页时，这段XSS代码被读出来响应给浏览器。

反射型XSS与DOM型XSS都必须依靠用户手动去触发，而存储型XSS却不需要。

# Level:Low



Low等级的源码

trim过滤了字符串首尾处的空白字符（或者其他字符）;

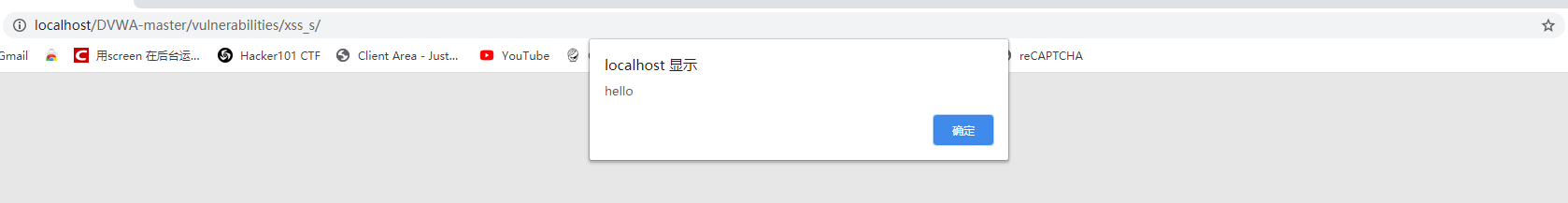
trigger\_errot用于这段代码出错会有特殊响应；

stripslashes 反引用一个字符串

mysqli\_real\_escape\_string转义字符串

这些源码中都没有对XSS有特定的防护过滤检查

在留言框中注入<script>alert(“hello”)</script>



# Level:Medium

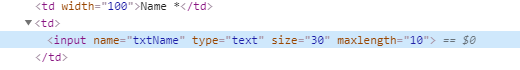


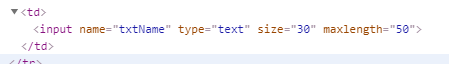
Medium等级的代码多出了

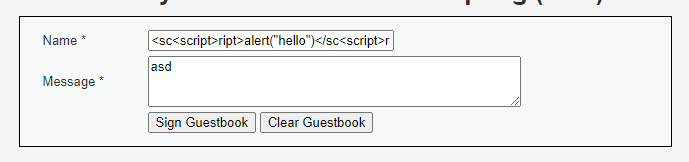
Strip\_tags 过滤HTML和PHP标签

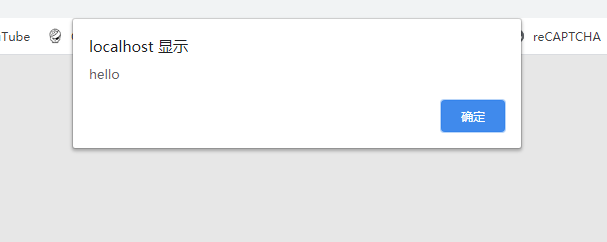
addslashes函数返回在预定义字符（单引号、双引号、反斜杠、NULL）之前添加反斜杠的字符串。

在message框中注入不了xss了，但是name标题并没有这个限制，可以通过修改前端的name标题的字数限制来进行注入,name标题只是简单的对<script>这个标签简单的过滤了，可以重叠写入<sc<script>ript>alert(“hello”)<sc<script>ript>









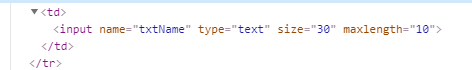
# Level:High



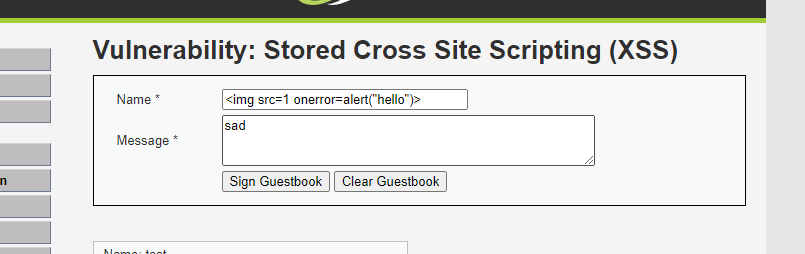
High等级的源码，给了name标题加强了对<script>的过滤，这个时候这个标签注入不了了

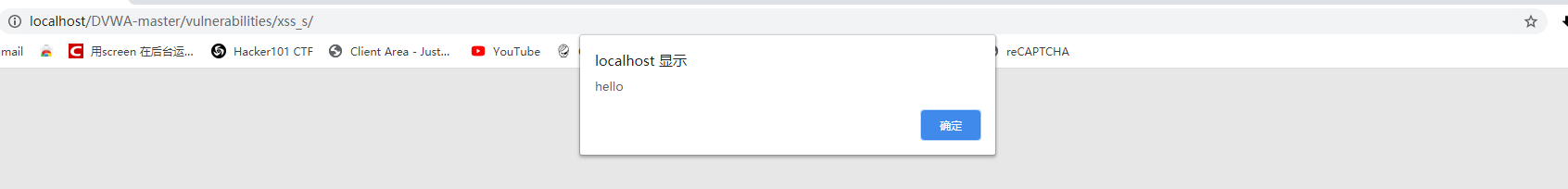
可以换img的onerror事件来进行注入

同样把标题的字数限制给改掉



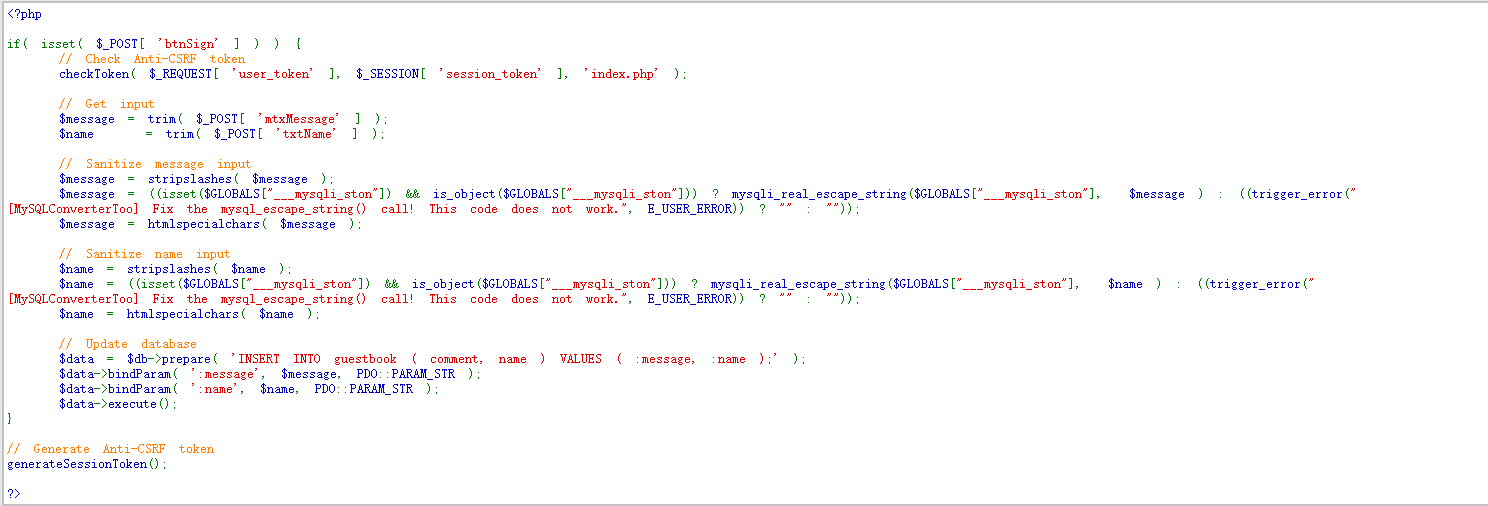






<img src=1 onerror=alert(“hello”)>

# Level:Impossible



Impossible等级中给message框和name标题框都给了htmlspecialchars函数

Htmlspecialchar这个函数会把特殊字符给html实体化