《漏洞利用及渗透测试基础》实验报告

姓名： 张丛 学号：2113662 班级：信安一班

**实验名称：**

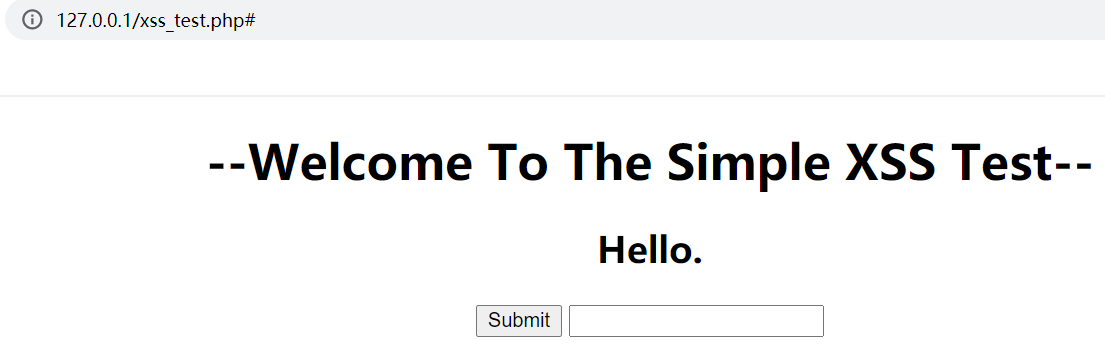
跨站脚本攻击

**实验要求：**

复现课本第十一章实验三，通过img和script两种方式实现跨站脚本攻击，可尝试撰写更安全的过滤程序。

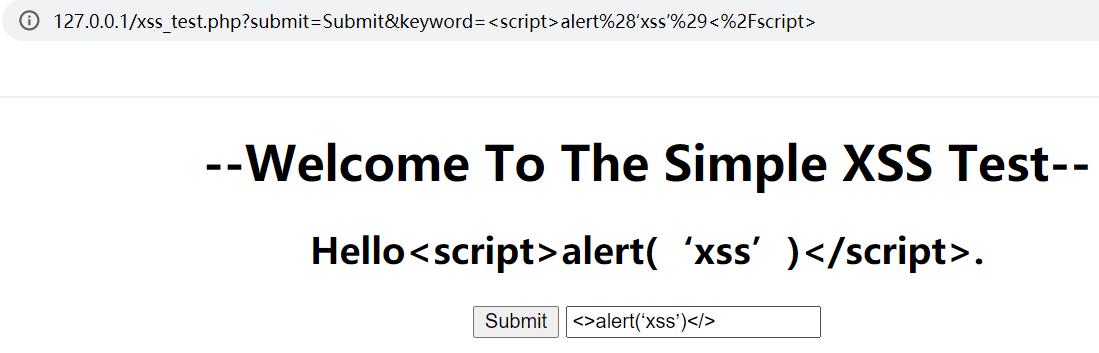
**实验过程：**

1.搭建xss\_test.php网页。



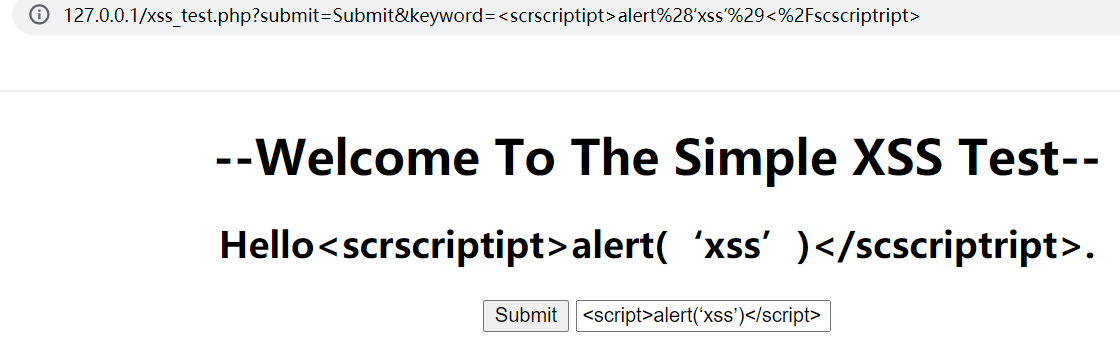
1. 使用script标签的脚本构造方法进行测试：

i）输入测试XSS脚本一<script>alert(‘xss’)</script>：



可以看到Hello后面出现了输入的内容，并且文本框中的回显过滤了script关键字

ii）输入测试XSS脚本二<scrscriptipt>alert(‘xss’)</scscriptript>：



黑盒测试情况下，并不能看到全部代码的整个逻辑，所以无法判断问题到底出在哪里。

iii）从源代码片段中分析问题。

①右击页面查看网页源代码：



从第5行可以看出，如果可以成功执行alert函数，页面将会弹出一个确认框，显示Congratulations~，也就是XSS成功攻击的标志；

接着查看第16行的<input>标签，唯一能输入且有可能控制的地方，通过分析可知，虽然成功插入了<script></script>标签，但是并没有跳出<input>标签，使得脚本仅可以回显而不能利用。

②设法将<input>标签闭合，

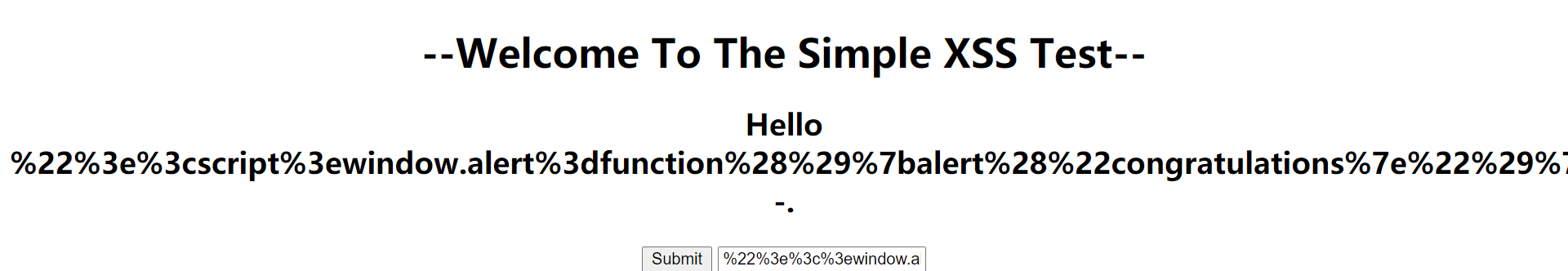
构造脚本”><scrscriptipt>alert(‘xss’)</scscriptript><!—

但仍然没有弹出确认对话框：

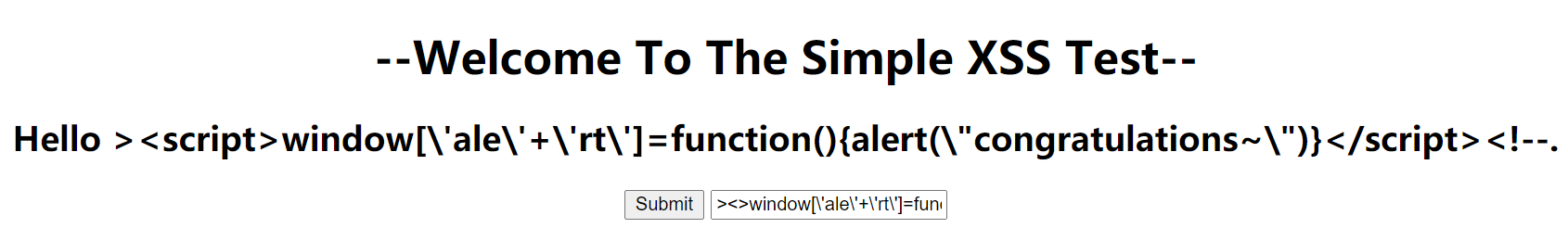


在尝试使用URL编码和特殊字符的脚本构造方式后仍然没有触发alert函数：

输入%22%3E%3Cscript%3Ewindow.alert%3Dfunction%28%29%7Balert%28%22Congratulation s%7E%22%29%7D%3C/script%3E%3C!—脚本：

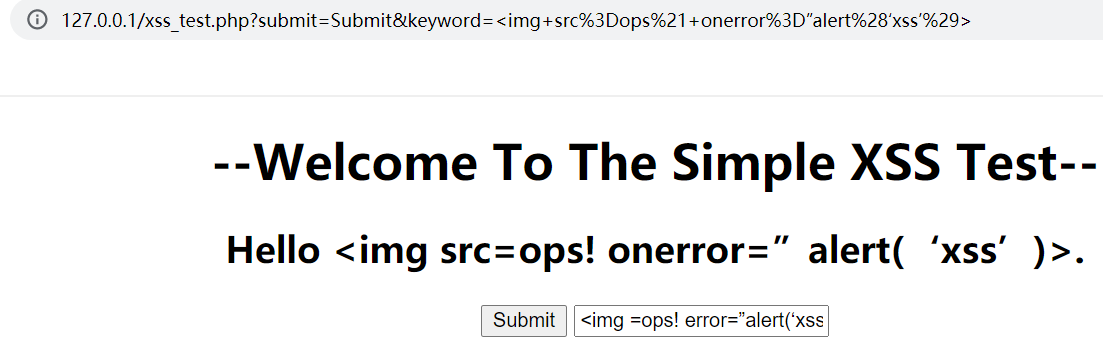


输入><scRipT>window['ale'+'rt']=function(){alert("Congratulations~")}</scRipT><!—脚本：



1. 使用img标签的脚本构造方法

i）输入测试脚本<img src=ops! onerror=”alert(‘xss’)>

过滤后的结果为：  


可以看到src和on被过滤掉了；

<img>标签是用来定义HTML中的图像，src一般是图像的来源，onerror事件会在文档或图像加载过程中发生错误时被触发，也就是当img加载一个错误的图像来源ops!时，会触发onerror事件，从而执行alert函数。

**心得体会：**

在这次实验中，我们学习了XSS攻击的基本实现方式：黑客将恶意脚本代码注入到网站输入框等可输入文字的位置之后，当其他用户访问该网页时，这段脚本代码将在用户的浏览器中自动执行。而这可能会对用户的隐私、网站的数据安全以及功能造成不可逆的破坏性影响。

因此，在进行WEB开发时，特别是在处理用户可输入的内容时，我们要做好输入验证与过滤工作，以避免XSS攻击的发生。对用户的输入进行特殊处理可以有效提高Web应用程序的安全性，保护用户的个人信息不被黑客利用，以及避免对整个网站的损害。