《漏洞利用及渗透测试基础》实验报告

姓名：沙璇 学号：1911562 班级：信息安全

**实验名称：**

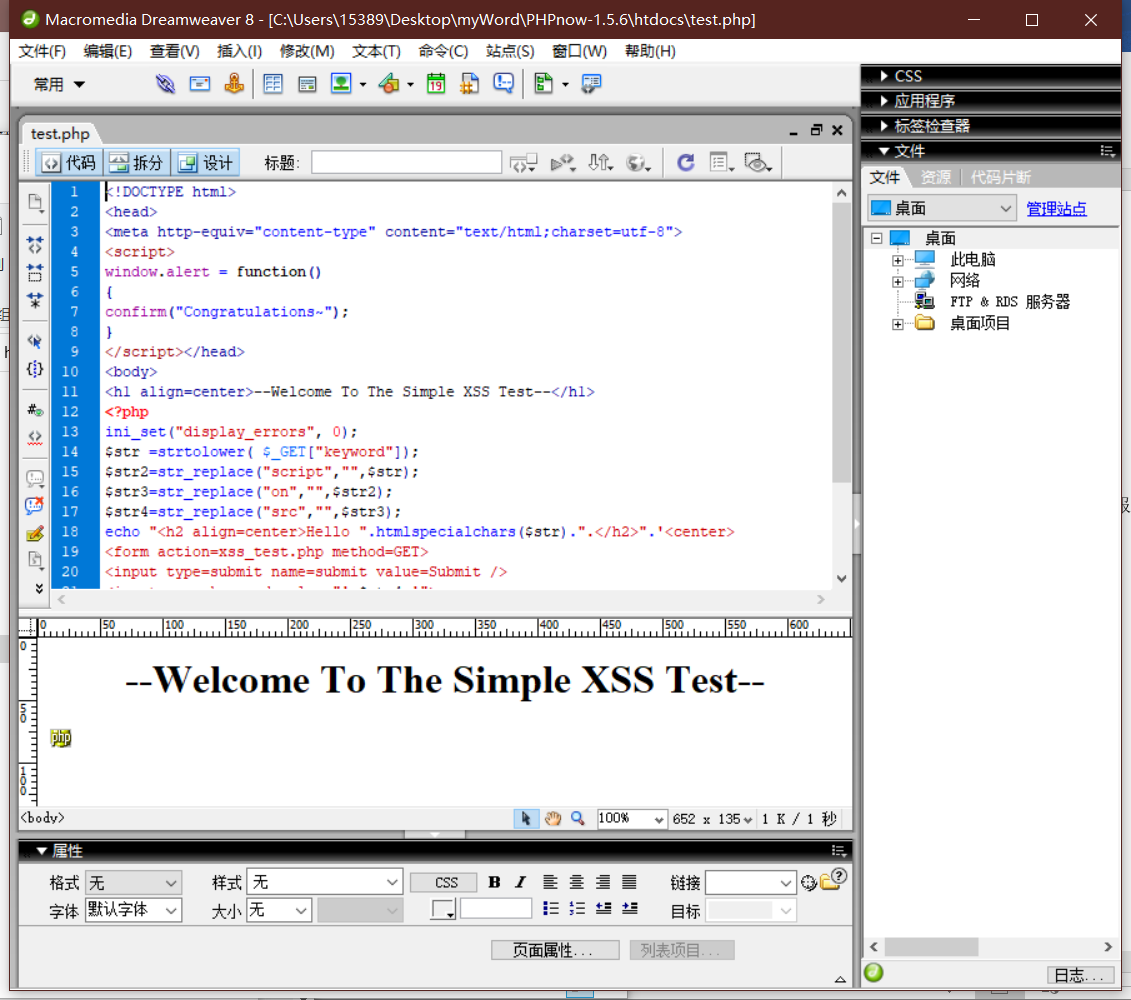
跨站脚本攻击

**实验要求：**

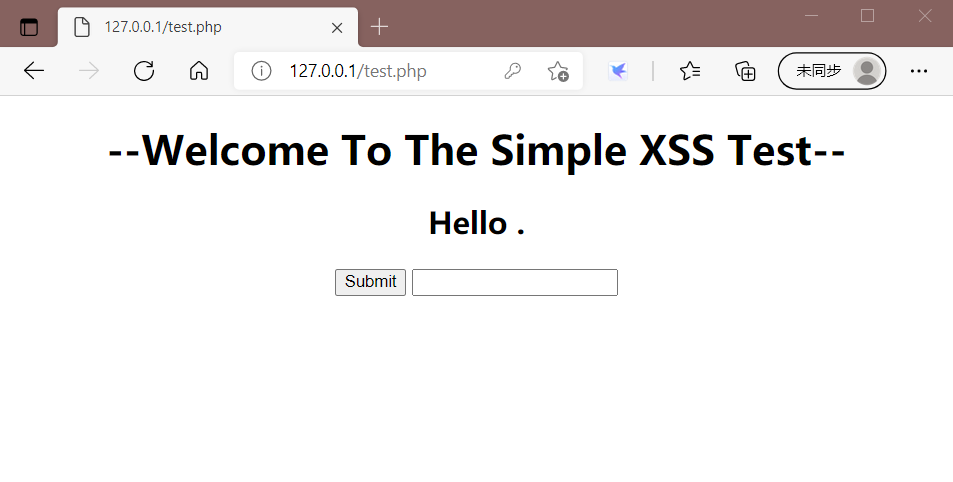
复现课本第十一章的实验三，通过img和script两类方式实现跨站脚本攻击，撰写实验报告。有能力者，可以自己撰写更安全的过滤程序。

**实验过程：**

①打开如下代码的php网页

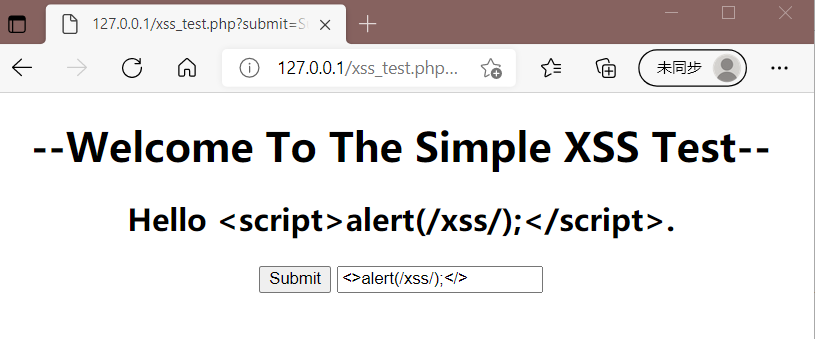


打开后：



②script方式：

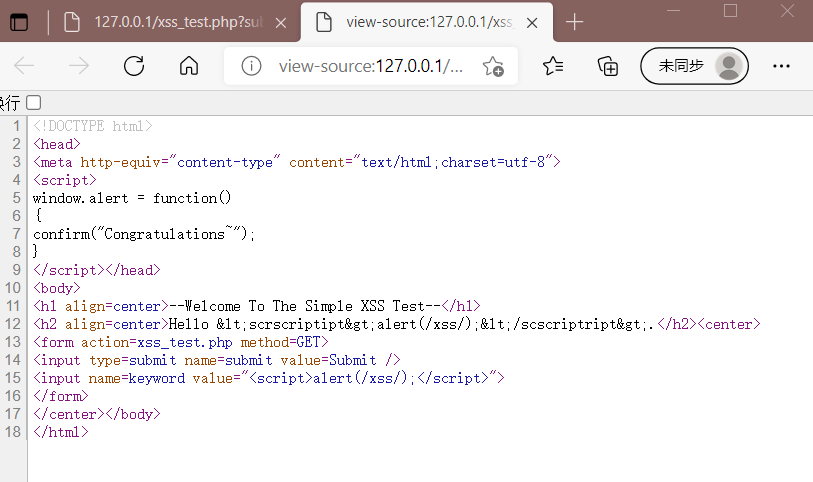
输入XSS脚本*<script>alert(/xss/);</script>*来进行测试，显示如下：



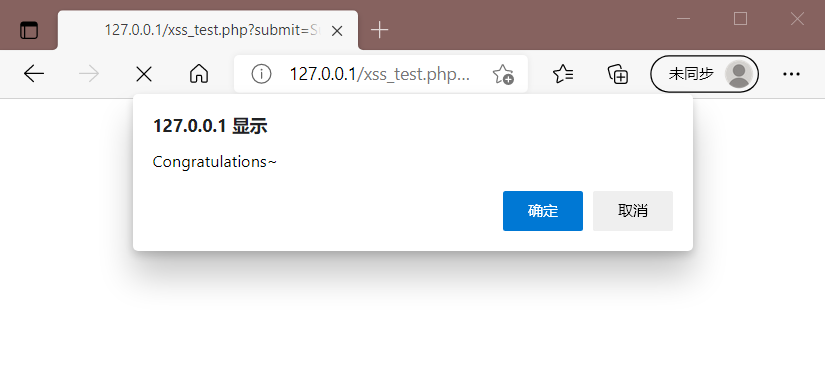
再次构造脚本*<scrscriptipt>alert(/xss/);</scscriptript>*测试，显示如下：



尝试从源码片段中分析问题。右键源码如下：

分析后构造如下脚本 *"><scrscriptipt>alert(/xss/);</scscriptript><!—*

弹处确认框，XSS 攻击成功。执行效果如下：



Img方式：分析同上。

构造如下脚本 *"><img ssrcrc=ops! oonnerror="alert('XSS')"><!—*

弹处确认框，XSS 攻击成功。执行效果如下：

**

**心得体会：**

通过本次实验，我了解了跨站脚本攻击，增强了实战能力。