《漏洞利用及渗透测试基础》实验报告

姓名： 许健 学号：2013018 班级：信安班

**实验名称：**

跨站脚本攻击

**实验要求：**

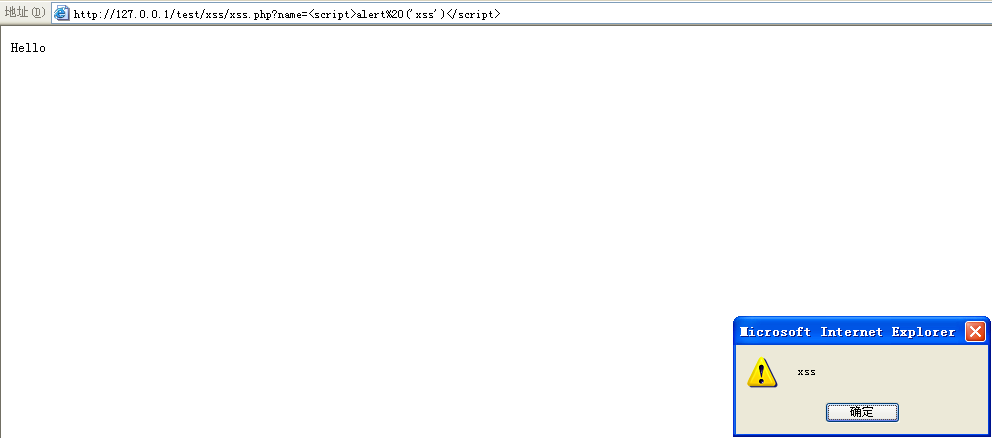
复现课本第十一章实验三，通过img和script两类方式实现跨站脚本攻击，撰写实验报告。有能力者，可以自己撰写更安全的过滤程序。

**实验过程：**

1. **复现反射式跨站脚本**

|  |
| --- |
| //一个简单的存在漏洞的php脚本  <?php  if(!array\_key\_exists ("name", $\_GET) || $\_GET['name'] == NULL || $\_GET['name'] == '')  {  $isempty = true;  } else {  echo '<pre>';  echo 'Hello ' . $\_GET['name'];  echo '</pre>';  }  ?>  //这个php页面将传入的参数name未经过有效性检验而**直接写入到响应结果中** |

将恶意脚本附加到URL地址的参数中：



1. **复现script持久式跨站脚本攻击**

存储式XSS与反射式XSS类似的地方在于，会在Web应用程序的网页中显示**未经编码**的攻击者脚本。

**从黑盒测试的角度实现跨站脚本攻击**

1. 输入最简单的XSS脚本：<script>alert('xss')</script>



php服务器自动会对输入的双引号等进行转义，以预防用户构造特殊输入进行攻击，将其关闭：



1. 发现关键字script被过滤了，尝试双写关键字绕过过滤



脚本代码还是未执行，这时候右键显示源码分析出问题的地方

发现没有跳出input的标签，所以无法利用

1. 重新编写代码，闭合input标签

"><scrscriptipt>alert('XSS')</scscriptript><!—

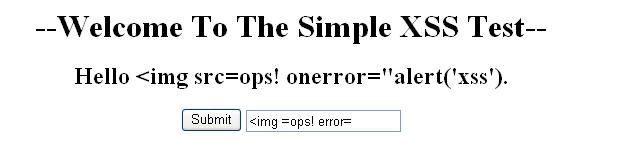


能看到恶意脚本成功执行，完成我们预期的效果。

1. **尝试img跨站脚本攻击**

根据之前相同的思路，构造脚本代码：

<img src=ops! onerror="alert('XSS')



发现关键字src和on被过滤了，尝试双写关键字绕过过滤，并闭合input标签



攻击成功！