夏令营集训4----WEB前端安全-XSS与CSRF

原创

MIGENGKING 于 2019-07-20 16:17:12 发布 118 收藏

什么是前端、后端？

前端：
即网站前台部分，运行在PC端，移动端等浏览器上展现给用户浏览的网页
后端：
更多的是与数据库进行交互以处理相应的业务逻辑。需要考虑的是如何实现功能、数据的存取、平台的稳定性与性能等

前端与后端的联系：

前端的三个核心技术：
一HTML： 超文本标记语言 (Hyper Text Markup Language)，用来显示文字、图片等内容

二CSS:层叠样式表 (Cascading Style Sheet)，可以使人更能有效地控制网页外观

三JavaScript：面向对象的动态类型的客户端脚本语言，用来给HTML网页增加动态功能。

HTML基本语法

1 HTML是一种标记语言，HTML 标记标签通常被称为 HTML 标签
2 HTML 标签是由尖括号包围的关键词，比如
3 HTML 标签通常是成对出现的，比如 **和**
4 标签对中的第一个标签是开始标签，第二个标签是结束标签
5 开始和结束标签也被称为开放标签和闭合标签

实例：

```
<!DOCTYPE html> <!-- 声明这是HTML5文档 -->
<html> <!-- HTML有两部分组成，head部分与body部分 -->
        <head>
                <meta charset="utf-8"> <!-- 指定编码方式 -->
                <title>我是文章标题</title>
        </head>
        <body>
                <h2>我是2号标题</h2>
                <input type='text' name='input' placeholder="我是文本输入框">
                <input type='submit' value='我是确定按钮'>
        </body>
</html>
```


CSS基本语法

1 CSS可以嵌套在HTML中，也可移出 HTML 文档，移入一个独立的样式表。
2 CSS 规则由两个主要的部分构成：选择器，以及一条或多条声明。

```
<!DOCTYPE html>
<html>
        <head>
                <meta charset="utf-8">
                <title>我是文章标题</title>
                <style type="text/css">
                        /* 设置CSS样式 */
                        h2 {
                                color:red; font-size: 14px;
                        }
                </style>
        </head>
        <body>
                <h2>我是2号标题</h2>
                <input type='text' name='input' placeholder="我是文本输入框">
                <input type='submit' value='我是确定按钮'>
        </body>
</html>
```


JavaScript基本语法

在 HTML 中，JavaScript 代码必须位于 标签之间。

```
<!DOCTYPE html>
<html>
	<head>
		<meta charset="utf-8">
		<title>我是文章标题</title>
		<script type="text/javascript">
			//弹窗
			alert('hello world');
		</script>

	</head>
	<body>
		<h2>我是2号标题</h2>
		<input type='text' name='input' placeholder="我是文本输入框">
		<input type='submit' value='我是确定按钮'>
	</body>
</html>
```


浏览器的两个功能

1.查看页面源代码：查看被浏览器解析后的HTML源码

2.查看元素/检查：
Elements(元素)选项可以查看被浏览器解析前的页面源码，并可以更改源码；
Console(控制台)选项可以调试页面的JavaScript代码

打开网页，鼠标右键即可找到这两个选项

什么是XSS？

1、XSS(Cross Site Script)，即跨站脚本攻击，本来缩写是CSS，但是为了和层叠样式表(Cascading Style Sheet ,CSS)有所区别，所以在安全领域叫做“XSS”

2、XSS攻击通常指黑客通过“HTML”注入篡改了网页，插入了恶意的脚本，从而在浏览网页时，控制用户浏览器的一种攻击

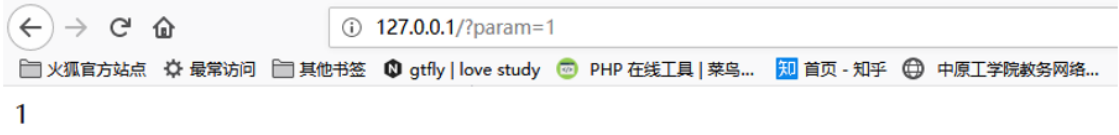
3、XSS长期以来被列为客户端Web安全中的头号大敌。因为XSS破坏力强大，且产生的场景复杂；针对各种不同场景产生的XSS，需要区分情景对待

实例在low等级下的
题目一：

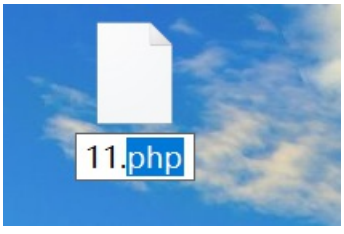
后端代码为：

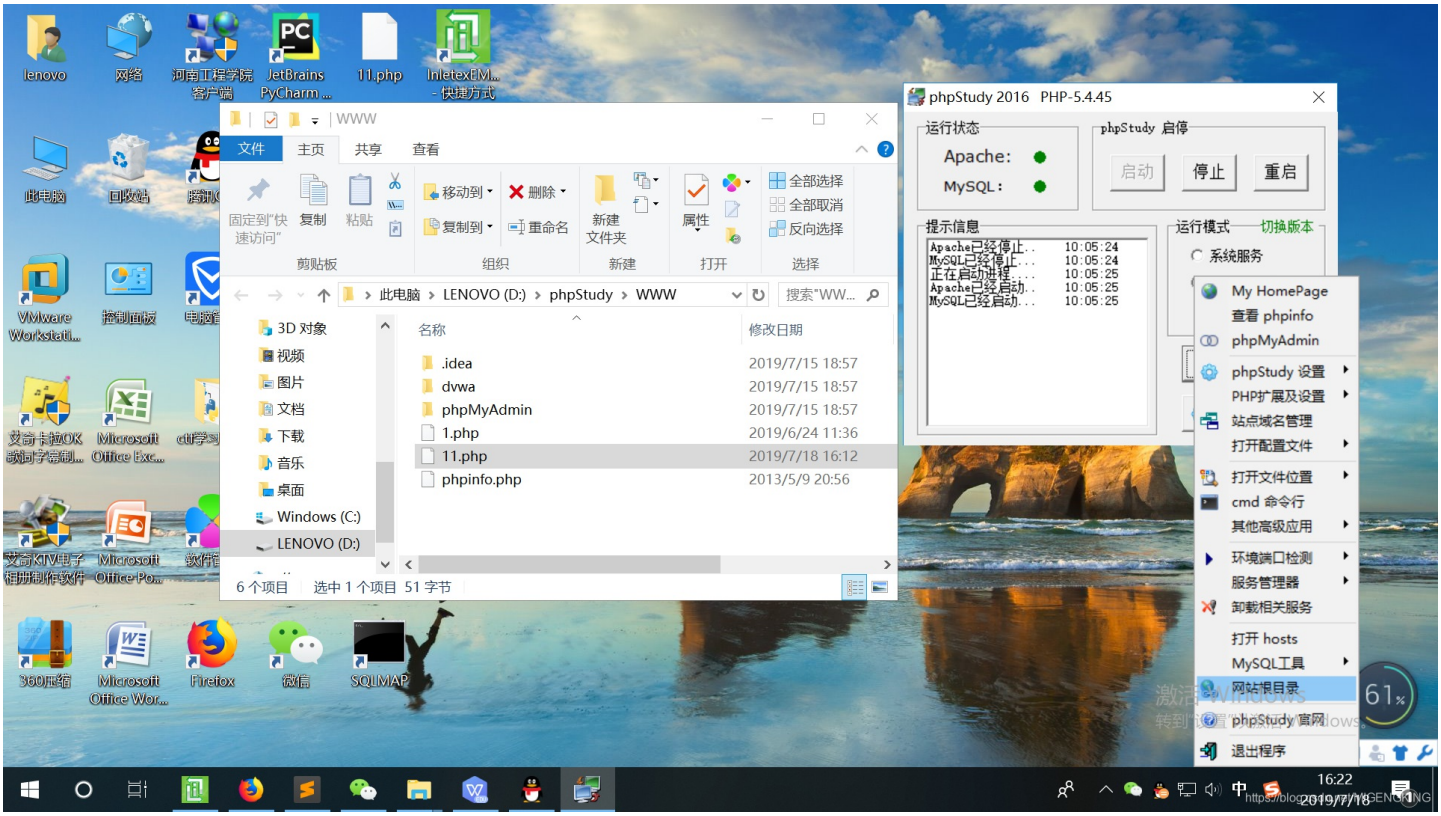
```
<?php

$input = $_GET['param'];
echo $input;
?>
```

意思就是接受参数param，并将其值输出到页面

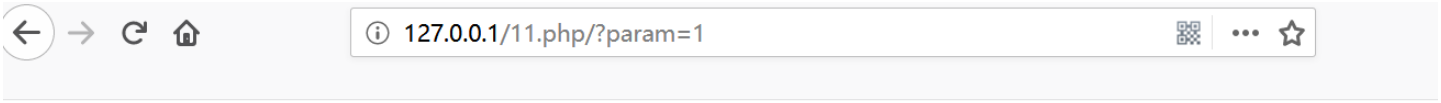


解题思路：先把代码保存为后缀为.php的文件，然后把文件放进phpstudy软件的根目录下





然后去浏览器上打开

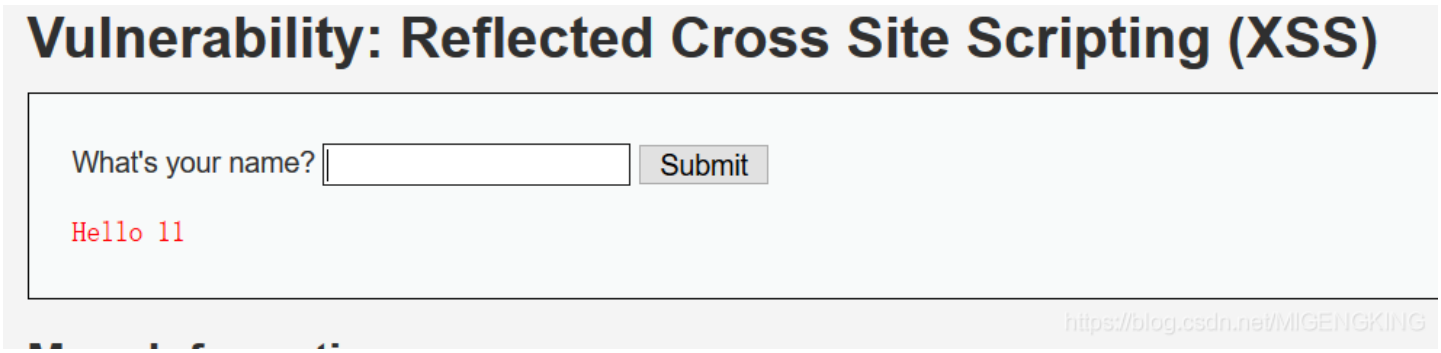


1

可以看到，代码直接引用了name参数（需要看代码），并没有任何的过滤与检查，存在明显的XSS漏洞。

题目二（DVWA在线平台： http://43.247.91.228:81）：

题目出现一个框，然后你在框里面输入什么它就会输出什么，这样的题目你首先想到时候有XCC漏洞



如果提交如下一段JavaScript代码：

```
<script>alert(1)</script>
```

可以发现，，成功弹框：

题目:

XSS挑战http://xss.tesla-space.com/

辅助理解：

Writeup：https://blog.csdn.net/qq_42357070/article/details/83818283

xss.tesla-space.com/level1.php?name=test

欢迎来到level1

欢迎用户test

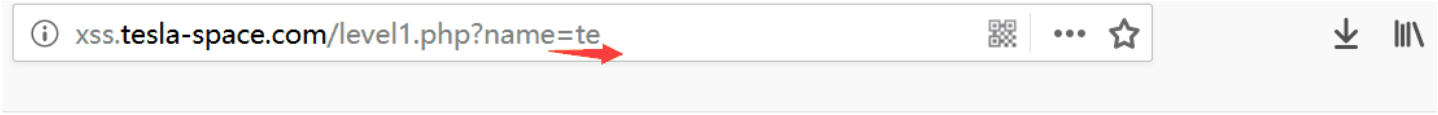
payload的长度:4

`

xss.tesla-space.com/level1.php?name=tes

欢迎用户tes

payload的长度:3



欢迎来到level1

欢迎用户te

payload的长度:2

很明显，当我们已修改URL上name的数据，图片里面的数据也会随着改变这是XCC漏洞的特征，如果提交如下一段JavaScript代码：

```
<script>alert(1)</script>
```

可以发现，这段代码在当前页面执行了；如果用户的输入提交后触发了弹窗，那么就说明存在XSS

什么是DOM?

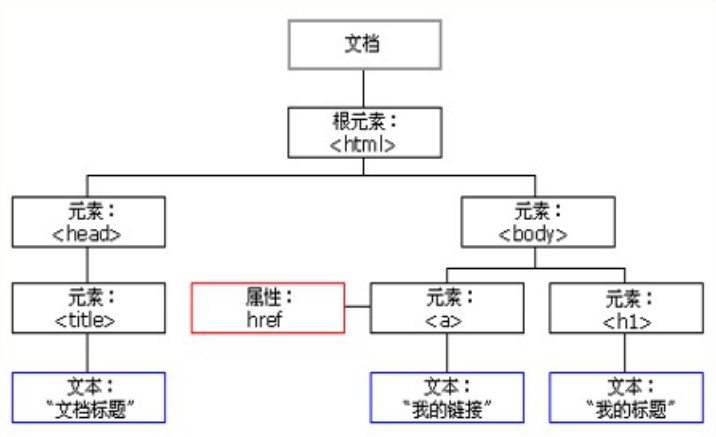
根据W3C的HTML、DOM标准文档中所有的内容都是节点;

1、整个文档是一个文档节点
2、每个HTML元素是元素节点
3、HTML元素内的文本是文本节点
4、每个HTML属性是属性节点
5、注释是注释节点

HTML DOM 节点树

HTML DOM 将 HTML 文档视作树结构。这种结构被称为**节点树**:

HTML DOM Tree 实例



通过 HTML DOM，树中的所有节点均可通过 JavaScript 进行访问。所有 HTML 元素（节点）均可被修改，也可以创建或删除节点。

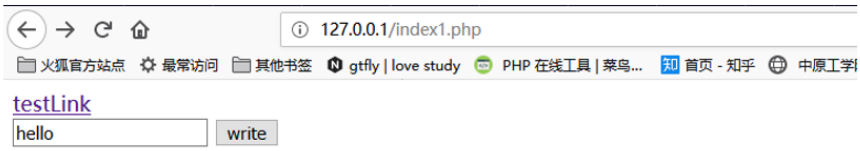
实例：

代码：

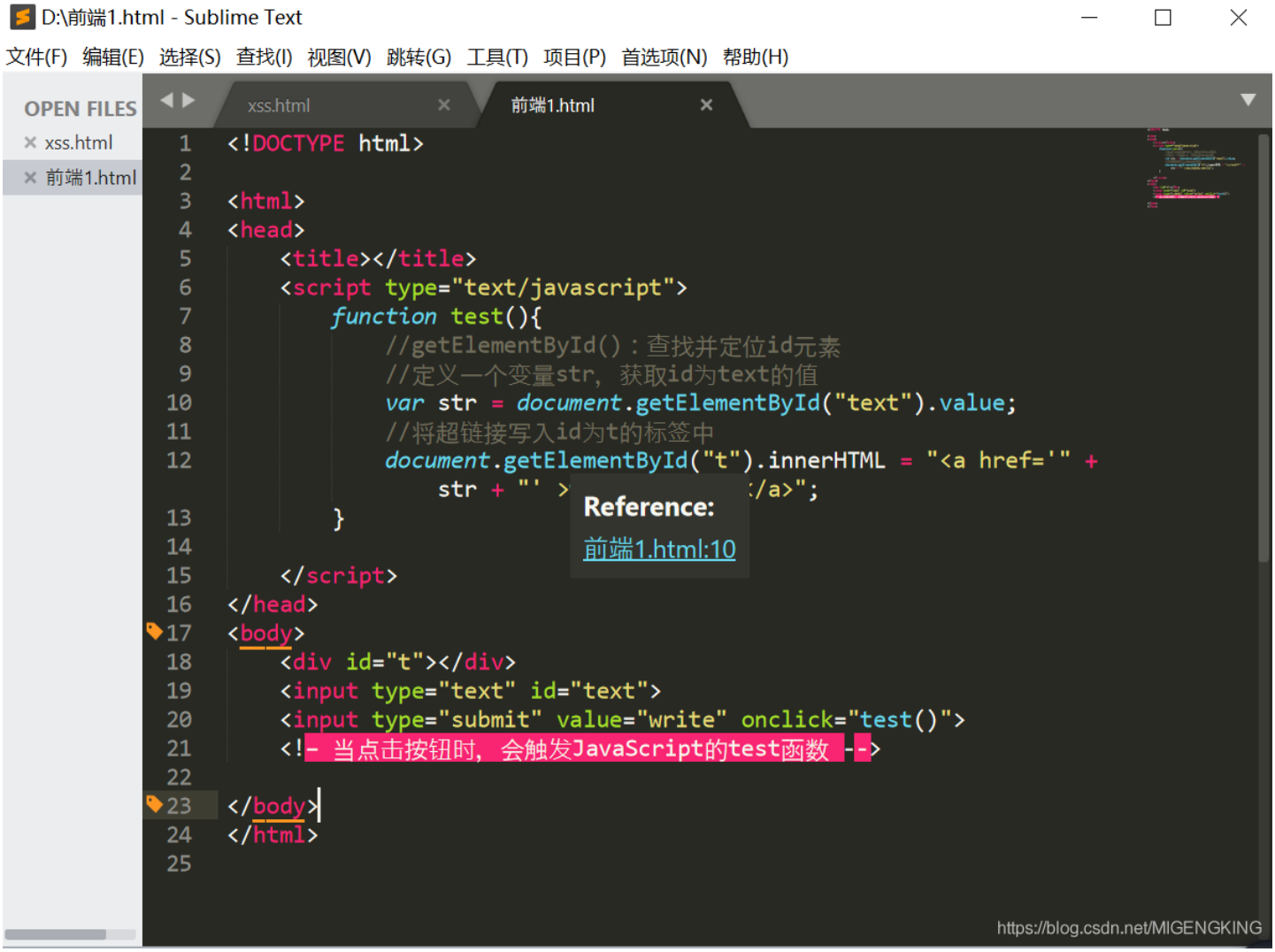
```
<!DOCTYPE html>

<html>
<head>
	<title></title>
	<script type="text/javascript">
		function test(){
			//getElementById()：查找并定位id元素
			//定义一个变量str，获取id为text的值
			var str = document.getElementById("text").value;
			//将超链接写入id为t的标签中
			document.getElementById("t").innerHTML = "<a href='" + str + "' >testLink</a>";
		}

	</script>
</head>
<body>
	<div id="t"></div>
	<input type="text" id="text">
	<input type="submit" value="write" onclick="test()"> <!– 当点击按钮时，会触发JavaScript的test函数 -->
</body>
</html>
```


举个DOM Based XSS的栗子

当输入内容点击“write”按钮后，会在当前页面插入一个超链接，其地址为文本框内容

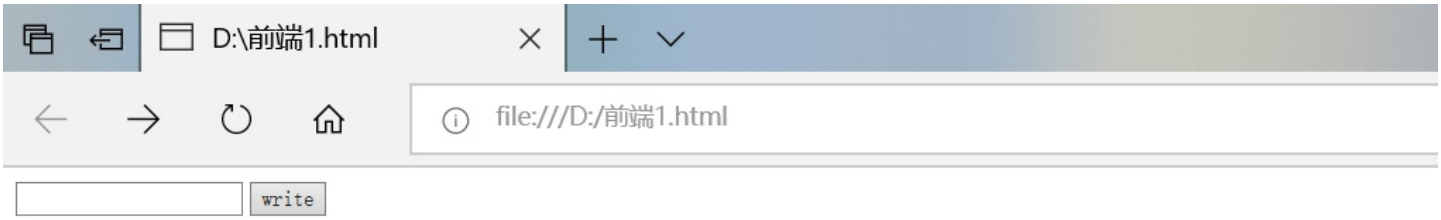


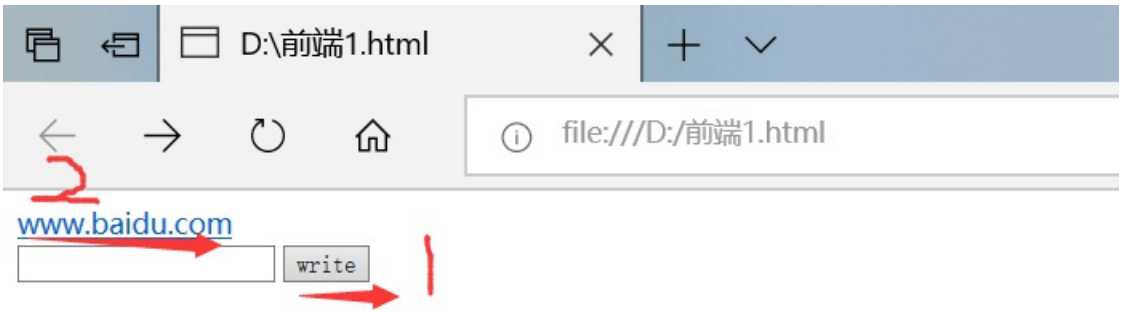
然后把网页代码放进sublime text里面保存为html文件




```
<!DOCTYPE html>

<html>
<head>
    <title></title>
    <script type="text/javascript">
        function test(){
            //getElementById()：查找并定位id元素
            //定义一个变量str，获取id为text的值
            var str = document.getElementById("text").value;
            //将超链接写入id为t的标签中
            document.getElementById("t").innerHTML = "<a href='" +
                str + "' >
        }

    </script>
</head>
<body>
    <div id="t"></div>
    <input type="text" id="text">
    <input type="submit" value="write" onclick="test()">
    <!- 当点击按钮时，会触发JavaScript的test函数 -->

</body>
</html>
```

放进sublime text软件中的代码要注意中英文符号(“)要改为英文的"
保存为html后缀的文件然后打开文件，直接会跳转到浏览器





一按write，就会跳出www.baidu.com,因为代码上有跳转的参量

XSS到底能干吗？

XSS并不等同于弹窗，上述例子只是为了检测是否存在XSS

常见危害：

1、劫持用户会话
2、盗取cookie
3、钓鱼欺骗
4、强制弹出广告
5、提升用户权限
6、传播跨站脚本蠕虫
……

XSS测试平台：http://www.l31.cc/index.php

CSRF简介

CSRF，Cross Site Request Forgery，即跨站点请求伪造

它是一种常见的Web攻击，也是Web安全中最容易被忽略的一种攻击方式

它与XSS非常不同，XSS利用站点内的信任用户，而CSRF则通过伪装成受信任用户的请求来利用受信任的网站。

一般攻击方式为攻击者诱使用户访问了一个页面，就以该用户身份在第三方站点里执行了一次操作

DVWA在线平台： http://43.247.91.228:81/

短网址生成工具：
http://suo.sheng2019.cn/?pid=2&zzj02&renqun_youhua=737067