漏洞演示平台之 XSS 篇

一.什么是 XSS

跨站脚本（cross site script）为了避免与样式 css 混淆，所以简称为 XSS。

XSS 是一种经常出现在 web 应用中的计算机安全漏洞，也是 web 中最主流的攻击方式。

XSS 是指恶意攻击者利用网站没有对用户提交数据进行转义处理或者过滤不足的缺点，进而添加一些代码，嵌入到 web 页面中去。使别的用户访问都会执行相应的嵌入代码。

从而盗取用户资料、利用用户身份进行某种动作或者对访问者进行病毒侵害的一种攻击方式。

二.XSS 攻击的危害

1、盗取各类用户帐号，如机器登录帐号、用户网银帐号、各类管理员帐号

2、控制企业数据，包括读取、篡改、添加、删除企业敏感数据的能力

3、盗窃企业重要的具有商业价值的资料

4、非法转账

5、强制发送电子邮件

6、网站挂马

7、控制受害者机器向其它网站发起攻击

三.XSS 的存在的主要原因

过于信任客户端提交的数据！对于用户数据过滤不完全甚至是完全不过滤！

四.设计目标

让使用者能去了解并且利用 XSS 漏洞，通过了解 XSS 的原理，掌握 XSS 的过滤与绕过技巧。XSS 有许多的利用方式，但只要能够进行最简单弹窗，那么其他所有方式几乎都是可行的，只需变换中间代码即可，故而在本作品中的输入栏输入 XSS 代码，只要能在该网页进行弹窗出'XSS'，即可算完成 XSS 攻击!

五.作品详解

1. xss-1.php

1.1 项目作用

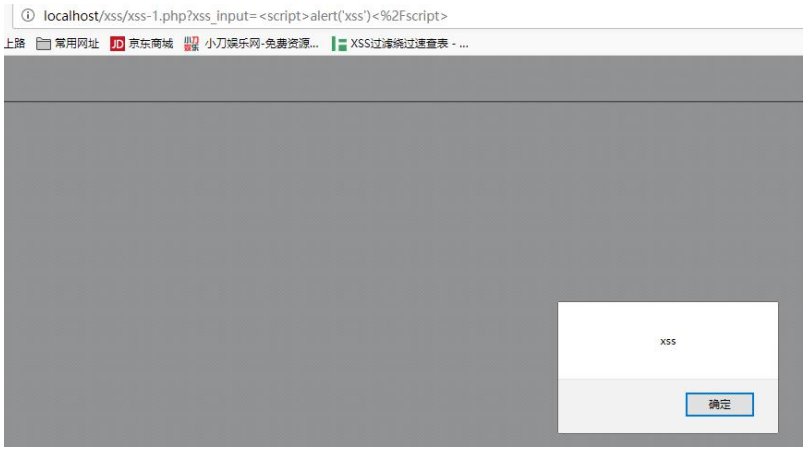
该项目的作用是接受用户输入的内容，在输入框下方进行显示。

1.2 xss 攻击方法

因为该项目并未对任何输入进行过滤，所以直接构造<script>标签进行攻击即可！

answer:<script>alert('xss')</script>

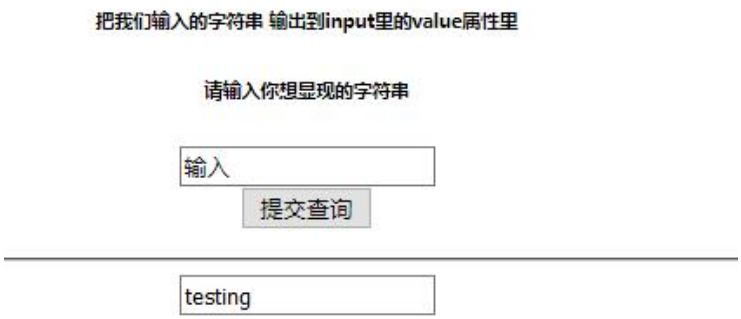
效果如图所示



xss-2.php

2.1 项目作用

该项目的作用是接受用户输入的内容，把我们输入的字符串输出到下方的输出的框中，考察的是标签中的 xss 攻击方法



2.2 xss 攻击方法

该输入是应用到标签<input>中，且并未进行任何过过滤操作，因此只需要闭合<input>标签，然和插入<script>标签以及代码即可。

answer: "><script>alert('xss')</script>

xss-3. php

3.1 项目作用

同 xss-1.php，接受用户输入的内容，在输入框下方进行显示。但该项目对于<script>标签进行了循环过滤，但大小写敏感。

所以当我们输入 <script>alert('xss')</script>时，会出现如下效果

3.2 攻击方法

虽然该项目循环过滤了<script>标签，但大小写敏感，而在 html 中对于<script>的大小写是不敏感的，所以只需将<script>标签中的任意

一个或几个字母用其大写替换即可进行绕过。

answer:<scRipt>alert(`xss`)</scRipt>

4. xss-4.php

4.1 项目作用

同 xss-1.php，接受用户输入的内容，在输入框下方进行显示。但该项目对于<script>标签进行了替换,但大小写不敏感,并且还过 滤了’与”。

所以当我们输入 <scRipt>alert(`xss`)</scRipt> 时，会出现以下效果

4.2 绕过方法

因为不不是对<script>标签进行循环过滤,所以只要我们输入的代码在被过滤一次后还能形成<script>标签，同时对于’ ” 的过滤可以使用`进行替换。

answer:<scr<script>ipt>alert(`xss`)</s</script>cript>

5. xss-5.php

5.1 项目作用

同 xss-1.php，接受用户输入的内容，在输入框下方进行显示。但该项目对于<script>标签进行了大小写不敏感的过滤，且过滤了’”、

5.2 攻击方法

先循环绕过<script>标签,因为过滤了’” `，所以如果想要弹出字符则可以使用 String.fromCharCode 函数即可进行输出

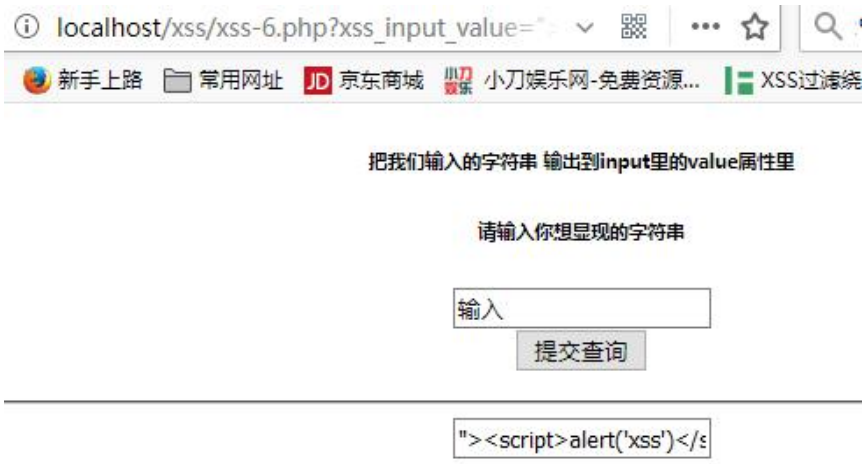
answer:<scr<script>ipt>alert(String.fromCharCode(88,83,83))</s</script>cript>

6. xss-6.php

6.1 项目作用

把我们输入的字符串 输出到 input 里的 value 属性里,并且对”进行了过滤，对<与>进行了转义。

所以在输入 "><script>alert('xss')</script> 时，情况如下



6.2 攻击方法

因为输入会到<input>标签内，并且并没有对’进行过滤，所以可以使用 onmouseover 事件进行绕过，当鼠标放置在输出栏中是就 会进行 xss 弹窗。

answer:’’ onmouseover=alert(’xss’)

7. xss-7.php

7.1 项目作用

使用 js 获取表单输入，用户输入为一张图片的路径与图片名称，在输入下方显示该图片

如输入当前目录下的 1.jpg

7.2 攻击方法

因为会输出图片，所以输入的内容必然会放置在<img>标签内，故而可以使用<img>标签的 onerror 事件进行 xss 弹窗

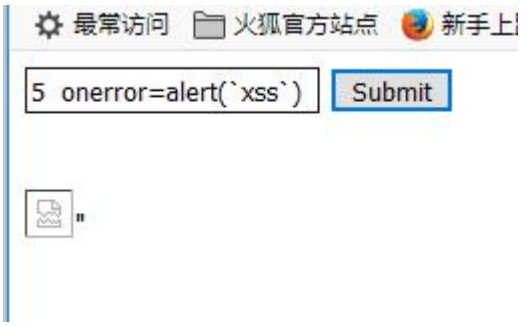
answer: 5 onerror=alert(`xss`)

8. xss-8.php

8.1 项目作用

使用 js 获取表单输入，用户输入为一张图片的路径与图片名称，在输入下方显示该图片，同时对 alert 关键字进行了过滤

此时输入 5 onerror=alert(`xss`) 效果如下



8.2 攻击方法

可以对 alert 进行构造，因为不是循环过滤

answer: 5 onerror=alealertrt(`xss`)

9. xss-9.php

9.1 项目作用

使用 js 获取表单输入，用户输入为一张图片的路径与图片名称，在输入下方显示该图片，同时对 alert 关键字进行了循环过滤

此时在输入 5 onerror=alealertrt(`xss`) 时效果如下

9.2 攻击方法

可以对 alert 进行编码从而绕过过滤

answer:5 onerror =\u0061\u006c\u0065\u0072\u0074(`xss`)

10.xss-impossible.php

该项目是’不可能达成任务’，对于<script>标签进行了循环过滤，同时对>〈进行了 html 转义，对于’”` 进行了过滤，该项 目的绕过方法留给使用者自行挑战钻研!