

Web 系统测试

3.6 Web安全测试——跨站脚本（XSS）漏洞

目 录

➤什么是XSS

➤XSS原理解析

➤怎样测试XSS漏洞

什么是XSS

➤XSS又叫CSS（Cross Site Scripting），即跨站脚本攻击，指攻击者在网页中嵌入客户端脚本，通常是JavaScript编写的恶意代码，当用户使用浏览器被嵌入恶意代码的网页时，恶意代码将会会在用户的浏览器上执行

➤XSS可以做什么

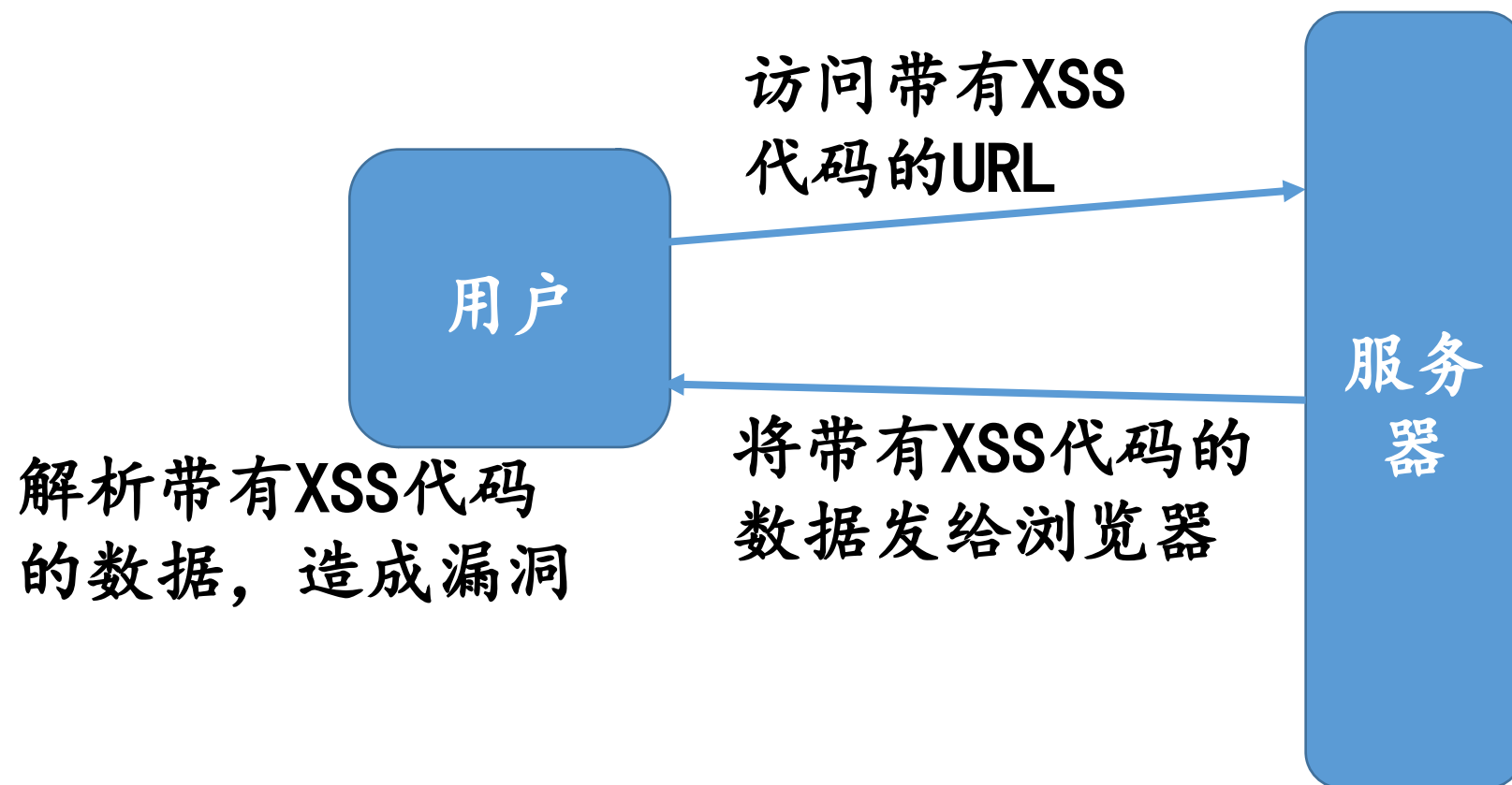
- 获取用户的Cookie
- 改变网页内容
- URL调转
-
- JavaScript能做到什么效果，XSS的威力就有多大

➤反射型XSS

➤存储型XSS

➤DOM XSS

反射型XSS



➤这个过程像一次反射，所以称为反射型XSS

```
<?php
```

```
    $username = $_GET[ 'username' ];
```

```
    echo $username;
```

```
?>
```

➤如果用户提交xss.php?username = HIM

- 程序输出HIM

➤如果用户输入username = <script>XSS 恶意代码</script>

- 造成反射型XSS漏洞

➤什么是存储型XSS

- 当用户提交一段XSS代码后，被服务器端接收并存储，当攻击者再次访问某个页面时，这段XSS代码被程序读出来响应给浏览器，造成XSS跨站攻击

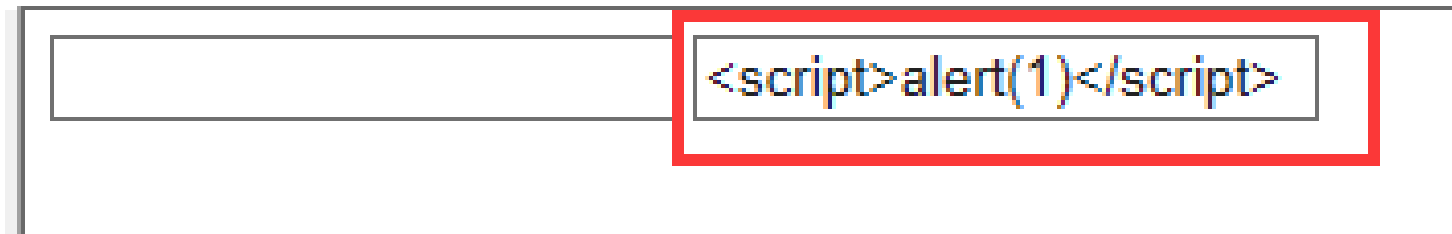
➤什么情况容易出现存储型XSS

- 运行用户存储数据的Web应用程序

➤找输入点与输出点：

- 将输出内容写在value中

`<input type = “text” name = “content”value =
“<script>alert(1)</script>” />`



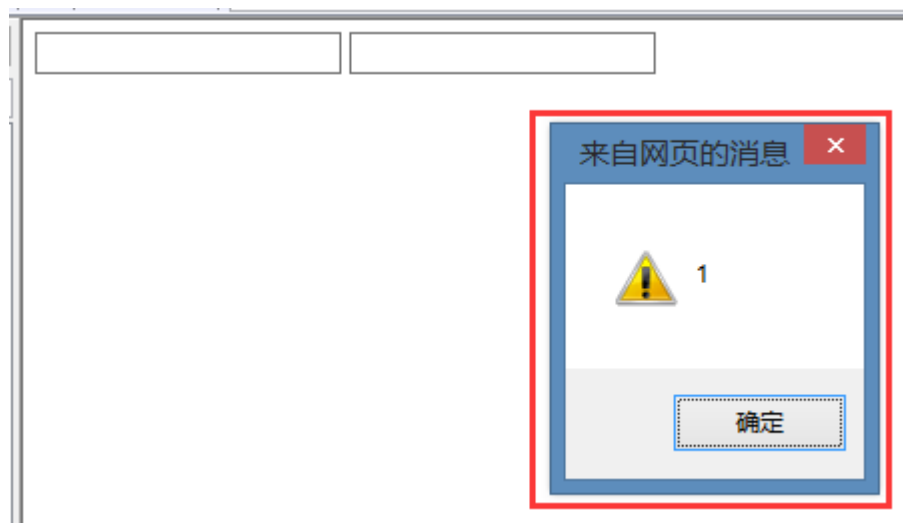
The diagram shows a text input field. A red rectangular box highlights the right portion of the field, which contains the text `<script>alert(1)</script>`. This illustrates how the malicious script is stored in the value attribute of the input field.

不能被执行

- 闭合input标签，使输出内容不在value属性中

`<input type = “text” name = “content”value = “ ”/>`

`<script>alert(1)</script>” />`



➤在网站输入框中输入

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

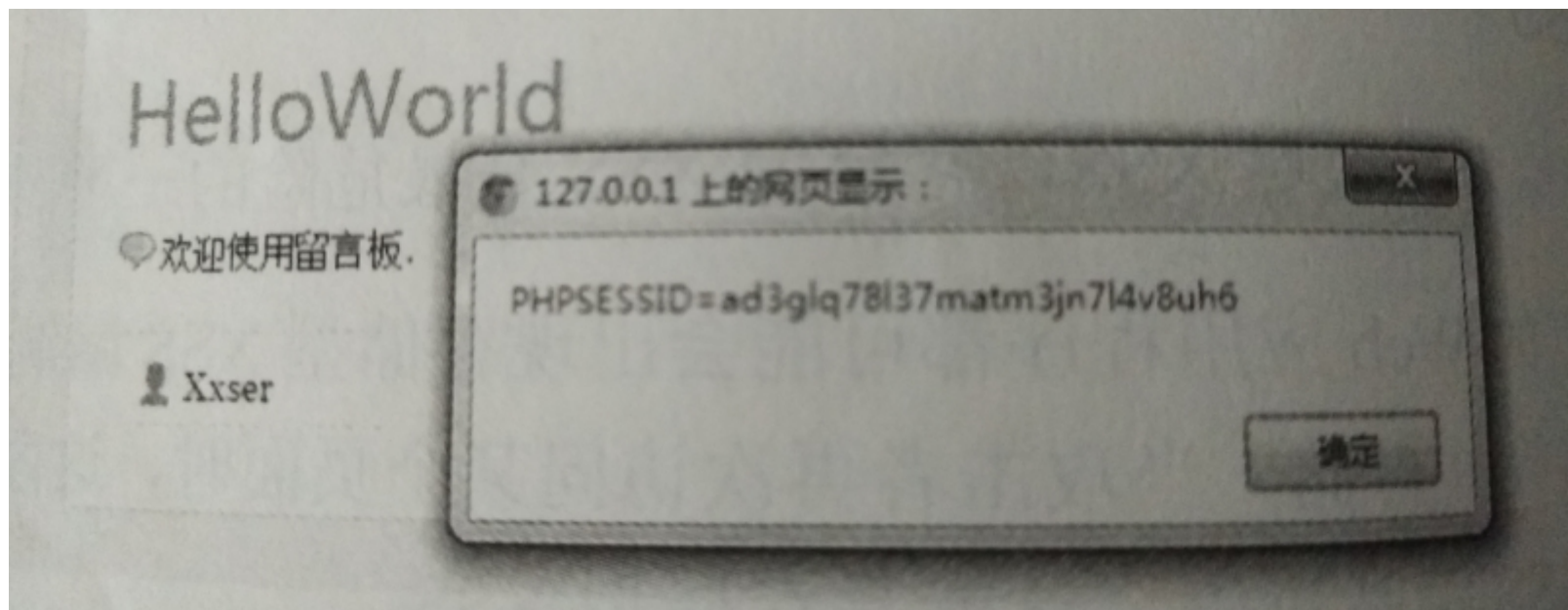
//普通注入

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

//闭合标签注入

●`</textarea"><script>alert(document.cookie)</script>`

//闭合标签注入



➤DOM : Document Object Model

➤DOM XSS

- 使用DOM可以允许程序和脚本动态地访问和更新文档的内容、结构和样式

```
<script>
```

```
    var tmp = document.URL;           //获取url
```

```
    var index = document.URL.indexOf("content=") +  
4;
```

```
    var par = temp.substring(index);
```

```
    document.write(decodeURI(par));    //输入获取内容
```

```
</script>
```

如果输入的内容中包含 `<script>alert(/xss)</script>`就会产生XSS漏洞

➤检测方式

- 手工检测
- 自动检测

➤手工检测

- 输入一些敏感字符，如“<、>、’、（）”，提交后查看HTML源代码，看这些是否被转义

➤全自动检测XSS

- 扫描工具

➤什么是XSS

➤XSS原理解析

➤怎样测试XSS漏洞

Question



XSS入门与介绍

XSS的危害

- 盗取各类用户账号，如机器登录账号、用户网银账号、各类管理员账号
- 窃取数据
- 非法转账
- 挂马
- ...



XSS的分类

反射型XSS

```
http://tdf.qq.com/mobile/index2.html?name=<a  
href="http://www.fooying.com">  
点击抽奖  
</a>&type=share&from=timeline&isappinstalled=1
```





XSS的分类

DOM型

其实DOM型也属于反射型的一种，不过比较特殊，所以一般也当做一种单独类

