



3.3-XSS漏洞

无涯老师

： 上一节内容回顾

- 1、DNSLog注入
- 2、SQL注入的防御
- 3、WAF类型及安装
- 4、WAF绕过思路

课程大纲

- 1、无状态的HTTP
- 2、Cookie和Session
- 3、什么是XSS
- 4、XSS的防御



01

无状态的HTTP

记住我，记住了什么？

登录

[没有帐号？ 点此注册](#)

☐ 记住我

[短信验证登录](#)

登录

[已有帐号，忘记密码？](#)

 使用 OSChina 帐号登录

其他方式登录



HTTP请求方式



HTTP请求方式

归类	方法	作用
常用	GET	请求从服务器获取资源
	HEAD	类似于 GET 请求，只不过不会返回实体数据，只获取报头
	POST	向服务器提交数据
	PUT	替换服务器的内容
不常用	DELETE	请求服务器删除指定的资源
	TRACE	对链路进行测试或诊断
	OPTIONS	列出可对资源实行的操作方法，Allow 字段里返回
	CONNECT	要求服务器和另一台服务器建立连接，充当代理
扩展		MKCOL、COPY、MOVE、LOCK、UNLOCK、PATCH

HTTP请求格式



HTTP响应格式

协议、版本 状态码、描述

响应头

```
HTTP 1.1 200 OK
Server: Nginx 1.18
Content-Type: application/json
Transfer-Encoding: chunked
Date: Fri, 14 May 2021 14:48:22 GMT
```

wuya

响应体

```
{"password":"123456","userName":"wuya","birthday":null,
"salary":0,"realName":"wuyan zu","userId":"1000","dept":"teach"}
```

HTTP特点

- 请求应答模式
- 灵活可扩展
- 可靠传输
- 无状态 stateless

无状态的影响

现实：每个请求都是独立的
需求：保持会话



02

Cookie和Session

cookie内容

key/value 格式, 例如:

name=wuya

id=99

islogin=1

cookie怎么产生



第一次访问

→
wuya
←
BAIDUID=114BD4F4184058F7345B227D267D88CE:FG=1;
expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647;
path=/; domain=.baidu.com



wuya

之后的访问



BAIDUID=114BD4F4184058F7345B227D267D88CE:FG=1
→
wuya
←



Cookie格式

Set-Cookie: 第一次访问，服务器响应给客户端

Cookie: 之后的访问，客户端发送给服务器

⋮ set cookie格式 (一个cookie)

MIME	描述
name=value	cookie的键值对 (必需)
expires	cookie的过期时间
max-age	cookie多久过期 (单位是秒)
domain	cookie对哪个域名生效
path	cookie匹配的路径
secure	只有HTTPS连接, 才发送cookie到服务器
httponly	不允许通过脚本document.cookie去更改这个值

Cookie特点

- 1、明文
- 2、可修改
- 3、大小受限（视浏览器而定）

Cookie的用途

- 1、记住登录状态
- 2、跟踪用户行为

Cookie允许

您的追踪器设置

我们使用cookie和相似的方法来识别访问者和记住偏好设置。我们也用它们来衡量效果和网站流量分析。

选择“接受”，您同意我们和受信的第三方来使用这些方式。

更多内容或者随时地变更您的同意选择，请点击我们的 [cookie策略](#)。

接受全部和访问网站

管理您的追踪器设置

This website uses cookies to manage authentication, for analytics, and other functions. [Privacy_policy](#).

Got it!

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Necessary



Preferences



Statistics



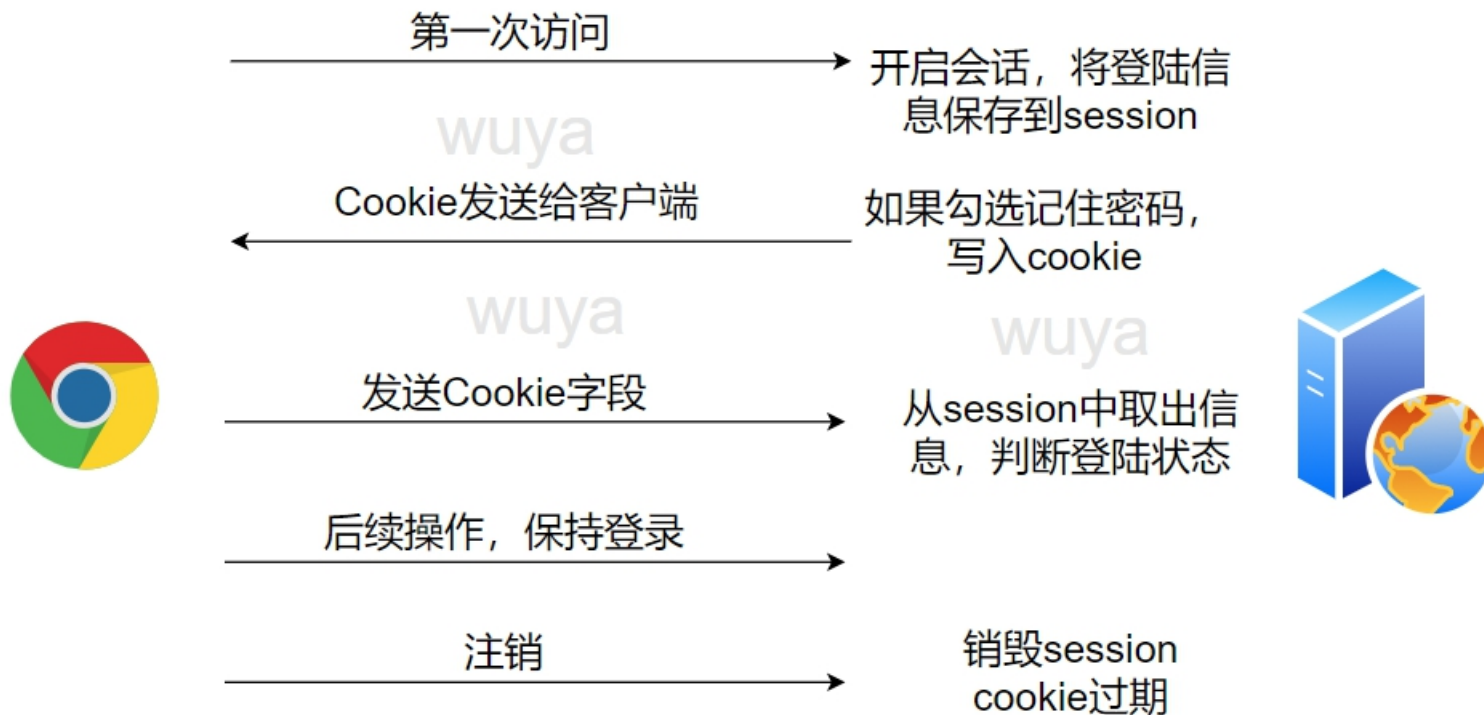
Marketing

Settings



Accept

session创建、校验、销毁



cookie和session

COOKIE内容:
BAIDUID=114BD4F4184058F7345B227D267D88CE:FG=1;
expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com



Cookie
保存在客户端



COOKIE内容:
PHPSESSID=7gn38vij5ucr8cpkbu2q4aus7d



Session
保存在服务端



SESSION内容:
BAIDUID=114BD4F4184058F7345B227D267D88CE:FG=1;
expires=Thu, 31-Dec-37 23:55:55 GMT; max-age=2147483647; path=/; domain=.baidu.com



直接利用Cookie登录

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无				
Cookie	项目过滤器			
http://localhost	名称	值	Domain	Path
Indexed DB	PHPSESSID	m7uhbbo9l6rdos9abrp6t1p331	localhost	/

问题

如何远程获取到其他用户的cookie?

JavaScript语法

获取: `document.cookie;`

设置: `document.cookie="username=wuya";`

修改:

删除:



03

什么是XSS

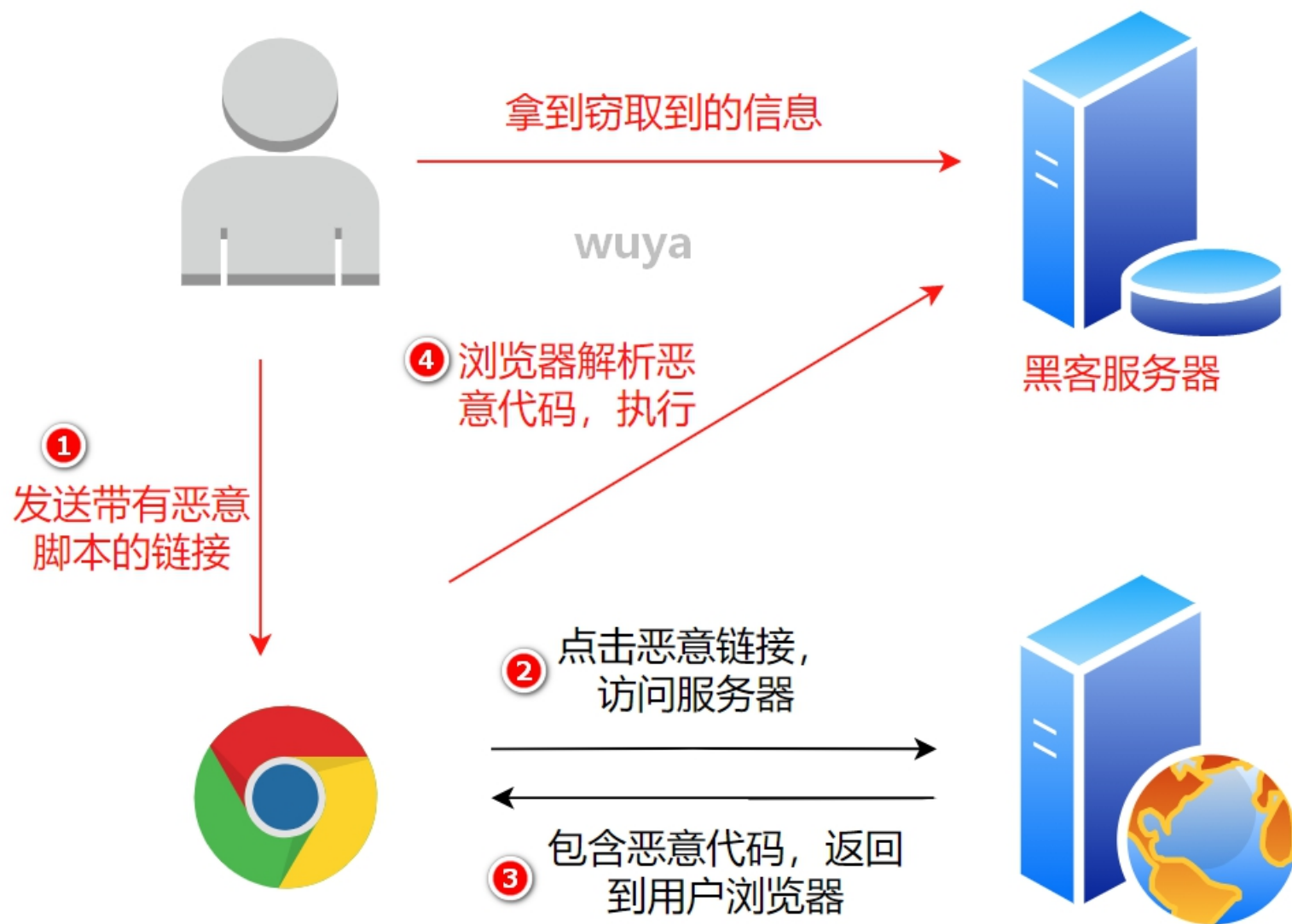
⋮ XSS : Cross Site Script

恶意攻击者利用web页面的漏洞，插入一些恶意代码，当用户访问页面的时候，代码就会执行，这个时候就达到了攻击的目的。

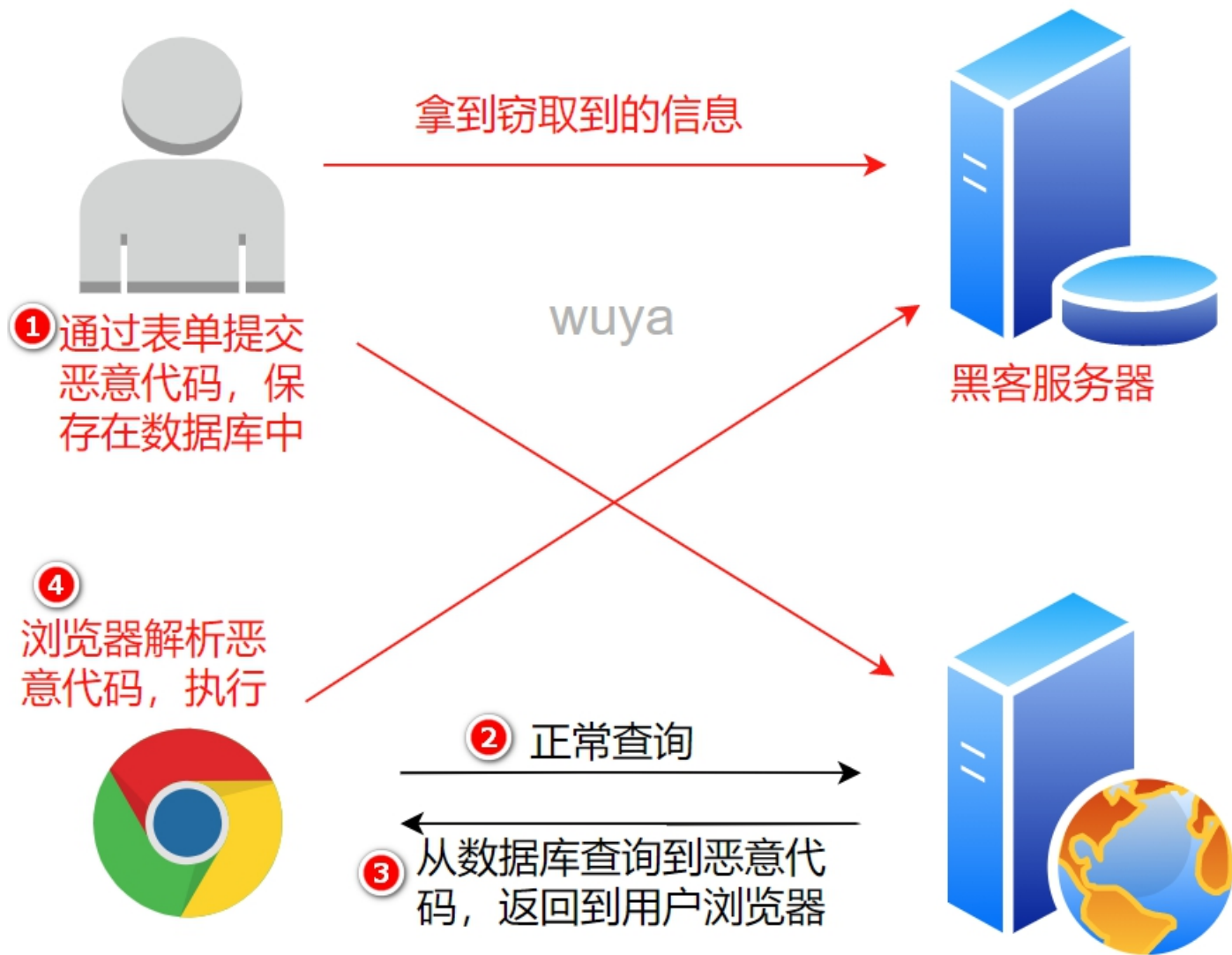
JavaScript、Java、VBScript、ActiveX、Flash

反射型，存储型

反射型XSS



存储型XSS



⋮ XSS的危害

- 1、冒充身份
- 2、刷点击
- 3、弹广告
- 4、传播蠕虫病毒



04 XSS的防禦

⋮ XSS的防御

过滤输入
处理输出
WAF



Thank you for watching

无涯老师