手把手带你掌握WS研发安全体系
——会话安全管理

讲 师： 孙 瑜

wondershare
万兴科技

课件信息

课件密级	内部	课件版本号	V1.0.0
课件使用频次	多次	课件类型	新课件
课件讲师	仅课件开发人		
面向对象	研发岗位员工		
年度内预计学习人数	100人		

信息保密要求

本文档所有信息属于公司**内部**文件，请严格保密

本文档可供公司内部人员查阅，禁止外传

请本文档查阅人员严格遵守以下规定：

- 未经许可，严禁向公司外部人员透露或发送本文档的任意内容。
- 如果您不是本文档的预期查阅人，请立即将此错误举报至万兴科技信息安全部门，并迅速永久性删除本文档。
- 如违反上述规定，将构成《万兴科技审计监察管理实施细则》规定的严重违反公司规章制度的行为，也构成违反《保密协议》相关保密义务的行为，公司有权对泄密人员作辞退处理。

wondershare
万兴科技

信息脱敏申明

本文档中涉及的敏感信息均已脱敏处理

请勿依据本文档决策

请本文档查阅人员注意：

- 未经许可，严禁向任何不相关人员透露或发送本文档的任意内容。
- 本文档中出现的各类信息均已经过抹除、模糊、混淆脱敏处理，不能作为推断公司情况的依据。
- 任何人员依据本文档所作出的决策或判断，均不可采信。
- 如因依据本文档进行决策而造成任何风险，由决策人自行承担一切责任，与万兴科技无关。

股票代码：300624.SZ

好好学习 天天向上

自觉遵守学习纪律，从我做起

勤学习

勤思考

勤实践

CONTENTS

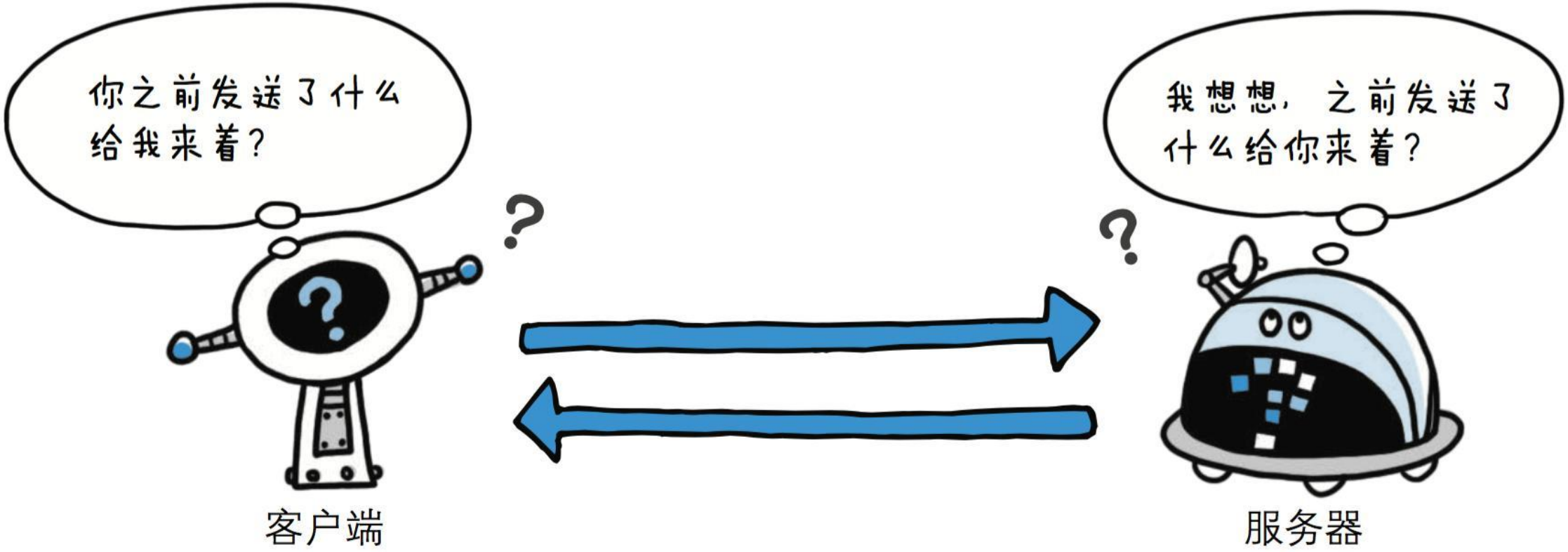
01

会话的产生

- ✓ 互联网没有“记忆”

什么是会话？

互联网没有“记忆”！



图：HTTP 协议自身不具备保存之前发送过的请求或响应的功能

什么是会话？

客户端

服务器

① 发送已登录信息（用户ID，密码）

向用户发放Session ID，记录认证状态

② 发送包含Session ID的Cookie
Set-Cookie: **PHPSESSID=028a8c...;**

③ 发送包含Session ID的Cookie
Cookie: **PHPSESSID=028a8c...**

通过验证Session ID来判定对方是真实用户

什么是会话


用户登录
手机号码
登录
我要注册 | 忘记密码?


一起分享购物车
赢清空购物车大奖
购物车 (11)
降价 常购 清理
袁咏仪靓靓的购物车
明星 袁咏仪
双11 Hermes爱马仕唇妆系列润唇膏
双11 Hermes爱马仕橘绿之泉
双11 【官方正品】Hermes爱马仕口红缎光唇膏
双11 3M口罩
分享我的购物车
打开好逛的淘宝 搜索"袁咏仪"
首页 逛逛 消息 购物车 我的
购物车 (13)
大湾区酷魔的购物车
明星 张智霖
双11 故宫 事事如意 成套茶器 朱漆釉 生日礼物
双11 断舍离 山下英子著
双11 【扶贫助农】陕西宜君红富士苹果9斤脆甜多汁
双11 Hermes/爱马仕丝巾香水50ml+保湿身体乳
打开好逛的淘宝 搜索"张智霖"
头条@观察者网


我的调节
最近浏览偏好
可根据喜好调节内容推荐强度
生活vlog 调节
球类运动 调节
生活分享 调节
民生新闻 调节
高分影视 增加推荐中
动漫 调节
美女 增加推荐中
明星资讯 调节
健身干货 调节
剧情创作 调节
3DMGAME

02

会话的定义

- ✓ 会话的定义
- ✓ 会话的生命周期

什么是会话？

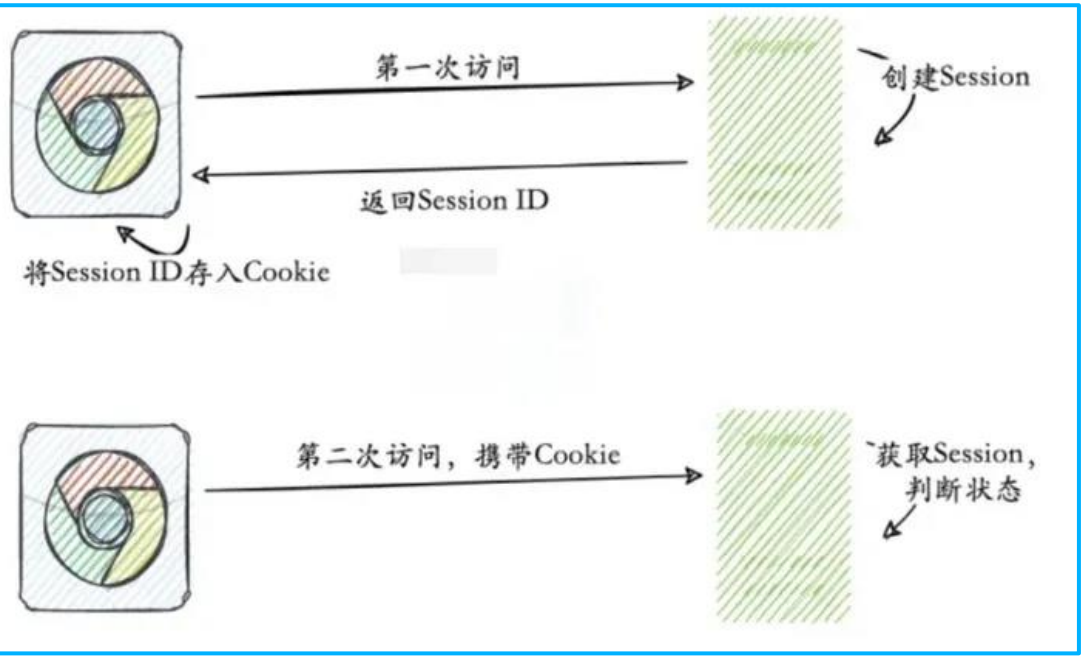
wondershare 万兴科技

会话的定义

会话是指一个客户端与web服务器之间连续发生的一系列请求和响应的过程。就像是从拨通电话到挂断电话之间聊天的过程就是一个会话。

一些概念：

1 SessionID	会话标识是由服务器/应用程序生成的用于唯一标识当前会话的值。
2 Cookie	客户端用户存储信息（如sessionID）的机制，分成会话cookie和持久cookie两种。
3 Token	会话Token是服务器为确认客户端请求的有效性而随机生成一段字符串。



什么是会话？

会话的生命周期

01

对于用户正在访问的页面，服务器将会判断会话是否已认证，并且用户是否有权限访问。

02

用户通过服务器端认证以后，服务器会创建一个随机会话标识来维持当前用户和服务器之间的连接。

03

在会话生成阶段完成后，使用会话标识来维护当前用户与服务器的连接，以及验证会话连接合法性的过程。

04

当客户端与服务器主动断开连接或者客户端长时间没有活动的情况下，服务器端删除会话标识、释放会话信息等过程。

认证前　会话生成　会话维持　会话销毁

03

会话的攻击和防御

- ✓ 会话预测攻击
- ✓ 会话劫持攻击
- ✓ 会话固定攻击

wondershare 万兴科技

会话攻击步骤

1

收集cookie

了解web应用系统如何创建和管理cookie

- ✓ 系统使用了多少cookie?
- ✓ Cookie如何被创建?
- ✓ Cookie什么时候被修改?
- ✓ Cookie被用于什么功能?

2

分析cookie

检查会话是否具备随机性、唯一性、抗统计分析、信息泄露。

- ✓ sessionID是否为随机数，能重现吗?
- ✓ 两次生成的sessionID是否相同?
- ✓ sessionID是否可有抗统计或密码分析?
- ✓ sessionID是否包含时间要素?
- ✓ sessionID是否包含可预测部分?

3

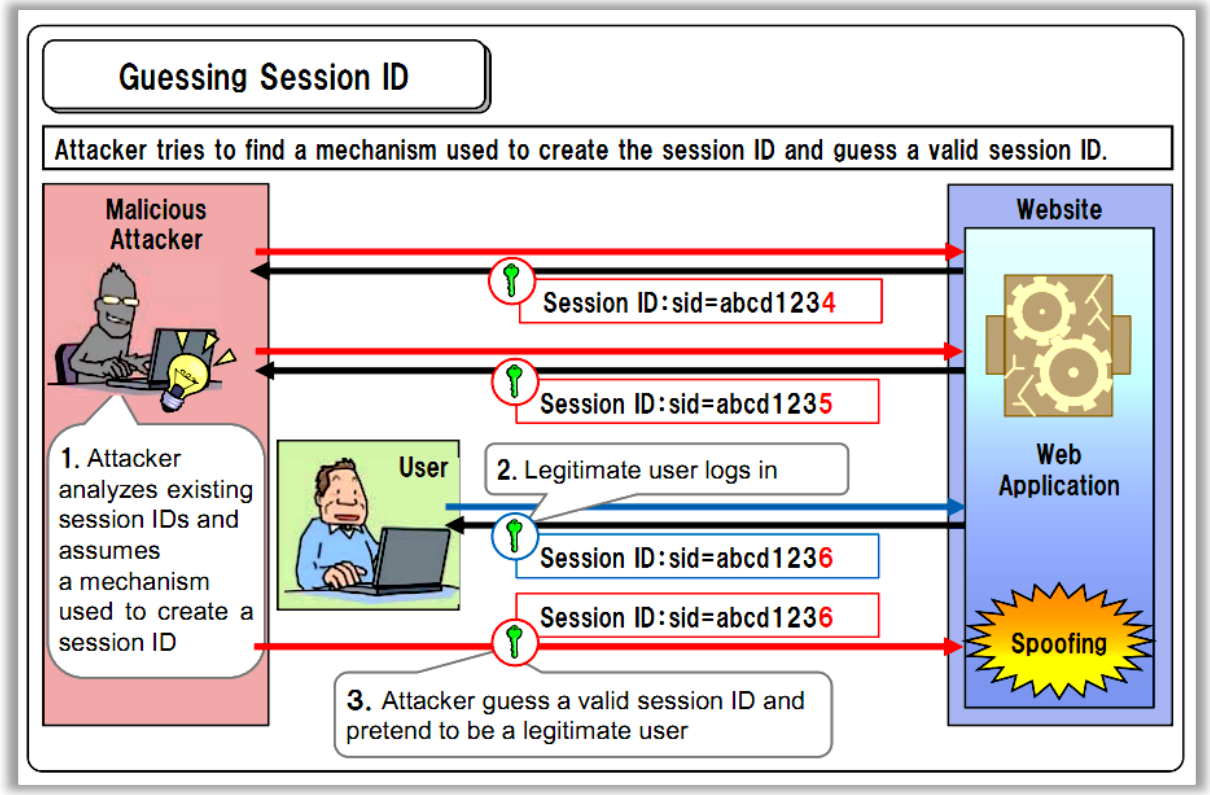
会话攻击

- ✓ 暴力破解攻击
- ✓ 会话猜解攻击
- ✓ 中间人攻击
- ✓ XSS跨站脚本攻击
- ✓ CSRF跨站请求伪造攻击
- ✓ 会话固定攻击

会话的攻击和防御

会话生成—攻击方式

会话预测



暴力破解

会话猜解时间				
会话长度	熵值	猜测速度（次/每秒）	有效会话数	猜测时间
64bit	32bit	1000	10000	4分钟
128bit	64bit	10000	100000	292年
猜解时间（秒）=2^熵值/(2*次/每秒*有效会话总数)				

会话的攻击和防御

wondershare 万兴科技

会话生成—攻击方式

sessionID的名称不应过于具体，以免泄露不必要的信息。

Cookie名字暴露了编程语言和应用服务器

sessionID Name	Example	Product Name	Product Type
JSESSIONID			J2EE Application server
ASP.NET_SessionId	0hqed4qelkxvj j153tplacm0	Microsoft Internet Information Services	Application server
PHPSESSID		PHP	Web server
WebLogicSession		BEA	BEA Weblogic
CFTOKEN	Macromedia	Coldfusion	Application server

服务器“指纹”

会话的攻击和防御

wondershare 万兴科技

会话生成—防御措施

1. **长度**：sessionID值的长度不小于24字节，192bits。
2. **名称**：sessionID名称改成通用名称，如“sessionID、ID”。
3. **随机数**：sessionID的值应该使用安全伪随机数生成；
4. **存储**：session对象应存储在服务器端，客户端只保存标识符，且标识符不包含敏感信息。

会话的攻击和防御

wondershare 万兴科技

会话劫持

实现手段

- 中间人攻击：嗅探传输中的sessionID
- XSS跨站脚本：Javascript脚本读取cookie
- CSRF跨站请求伪造：浏览器自动发送cookie
- 会话固定攻击：提前生成sessionID发送给用户

会话的攻击和防御

中间人攻击

Man-In-the-Middle attack

防御措施

1. TLS（如HTTPS）安全协议可以防止攻击者通过中间人攻击窃取或者篡改session ID；
2. 设置cookie的属性Secure为true，可以保证cookie只能通过加密通道（如HTTPS）传输。

注意：保证传输全链路安全，不仅在用户认证时，从客户端到服务器端整个传输过程采用HTTPS，在HTTP切换到HTTPS时容易发生信息泄露。

会话的攻击和防御

会话管理—攻击方式

服务器和客户端传输sessionID的方式：

- URL参数

https://www.example.com/index.html?sessionID=321

- POST隐藏参数
- Cookie。

Cookie

cookie能够让网站服务器把少量数据储存到客户端的硬盘或内存中，并可以从客户端的硬盘或内存中读取数据的技术。

Cookie由键值对的形式： KEY=VALUE;

例如：sessionid=EA51776A8B5C54349D35E055AD6C7CF7;

临时cookie

把cookie放在浏览器内存里, 浏览器关闭会话cookie就会被删除;

持久cookie

把cookie固化在用户的计算机硬盘上，直到超过过期时间才会被删除。

浏览器安全基础——同源策略

- 协议相同
- 端口相同
- 域名相同

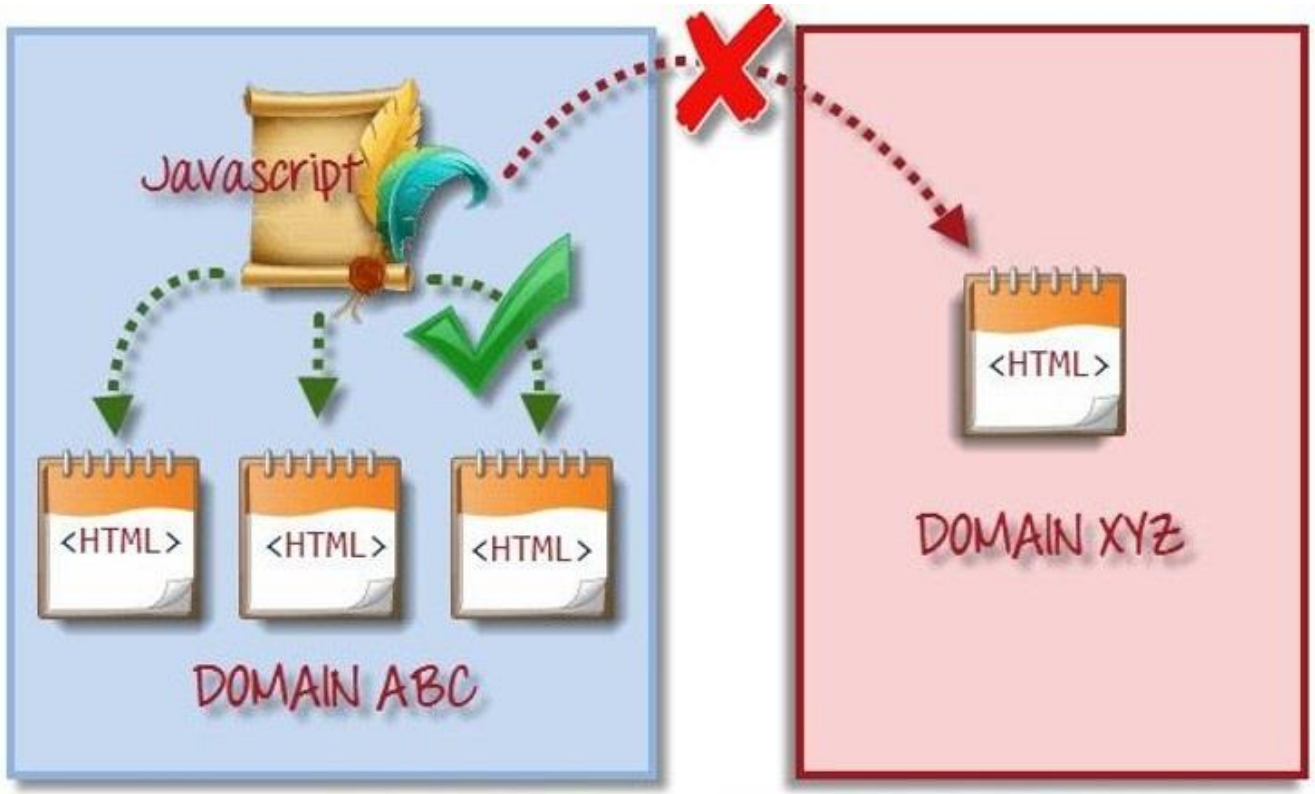
举例：

http://www. wondershare.com/

http://www.wondershare.com/dir/page.html

https://www.wondershare.com/

http://oa.wondershare.com/



under same origin policy, a Javascript program can only access pages on the same domain where it belongs. It cannot access pages from different domains

会话的攻击和防御

Cookie安全属性		
	含义	值
HttpOnly	只允许HTTP读取cookie	True
Secure	只允许安全协议传输，如TLS	True
SameSite	设置浏览器跨站请求携带cookie的等级	Strict|Lax|None
Domain&Path	定义了cookie的使用范围，即cookie能发给哪些URL	域名
Expire	过期时间，如果定义了Expire值，说明是持久性cookie	GMT格式的日期字符串
Max-Age	Cookie的最大生存周期，值为-1代表会话cookie	S

举例

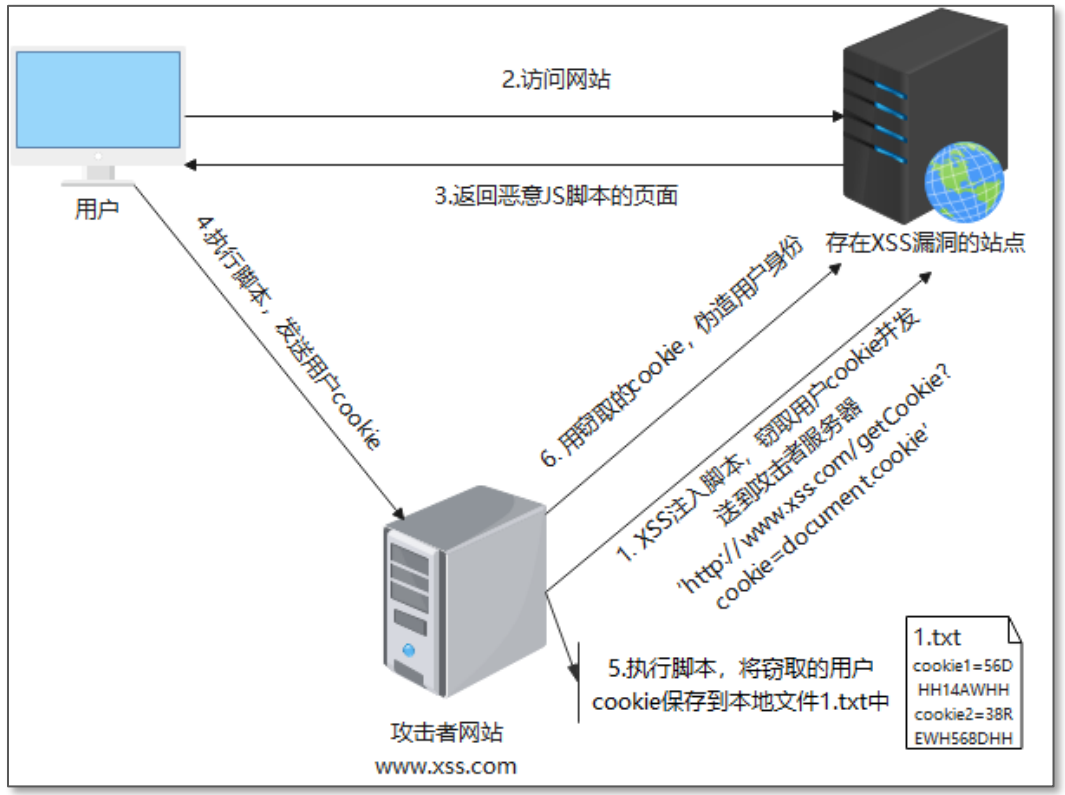
Set-Cookie: id=a3fWa; Expires=Thu, 21 Oct 2023 07:28:00 GMT; Secure; HttpOnly

会话的攻击和防御

会话管理—攻击方式

跨站脚本请求攻击

XSS攻击



HTTPOnly：True

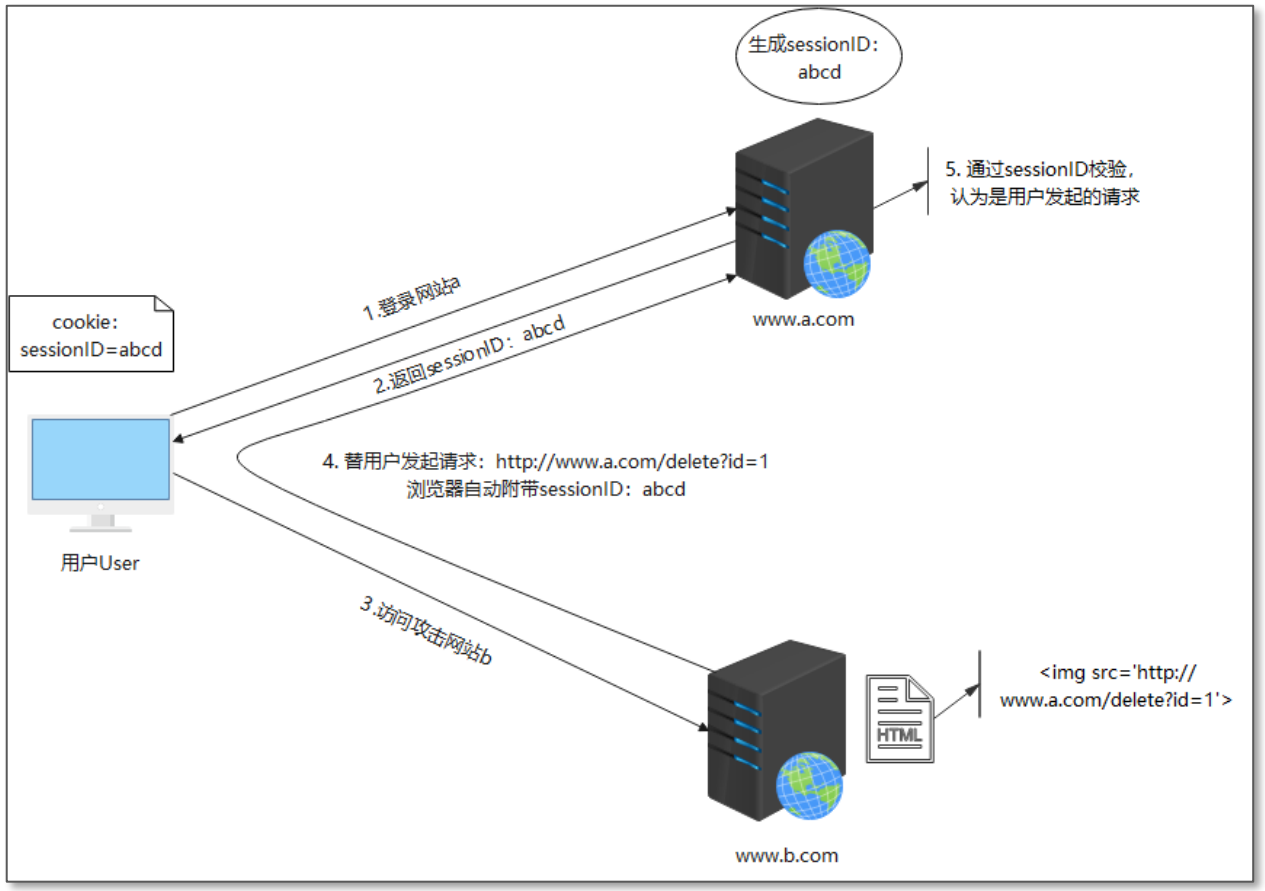
防御措施

会话的攻击和防御

会话管理—攻击方式

跨站请求伪造攻击CSRF

CSRF攻击



防御措施

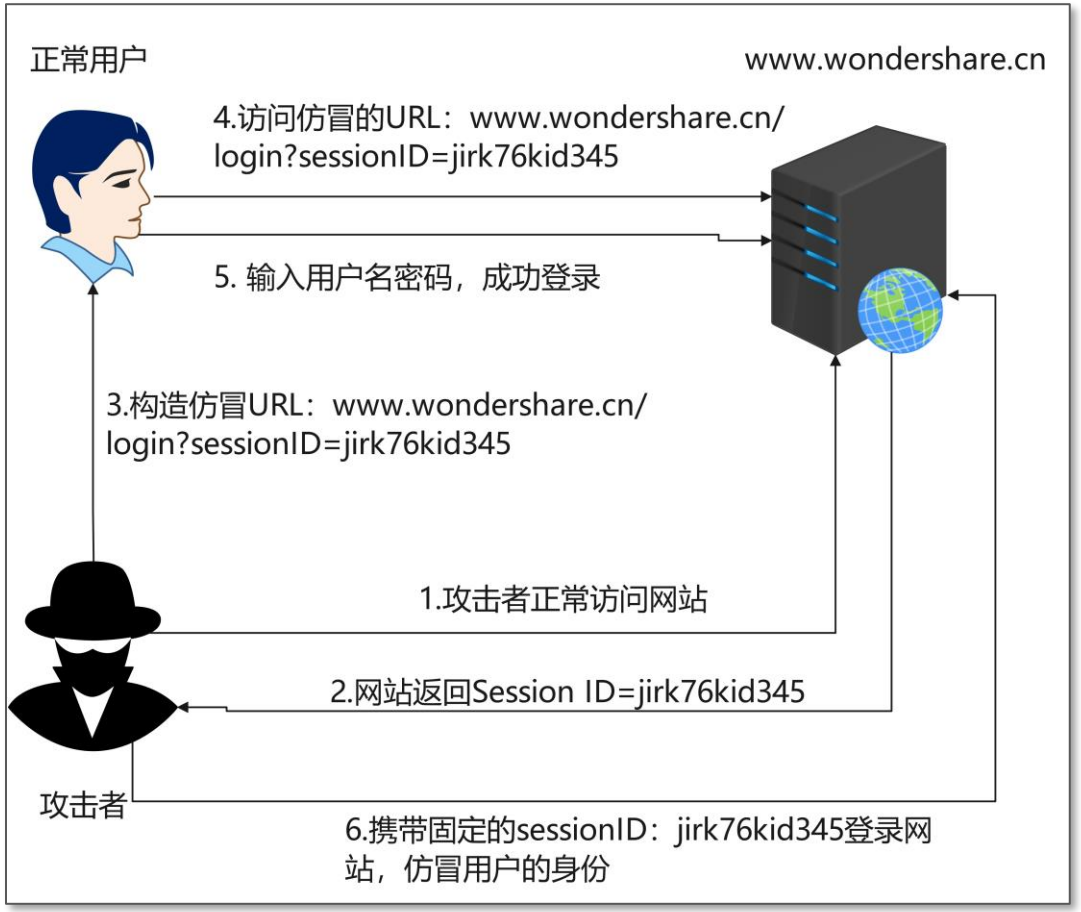
1. 校验客户端IP地址
2. 校验会话token（csrf token）
3. 检查Referer字段

会话的攻击和防御

会话管理—攻击方式

会话固定攻击(Session Fixation)

会话固定攻击



更换sessionID，并使旧的sessionID失效。

示例

更换会话标识Java代码示例：

```
HttpSession session = request.getSession(false);
if(session != null) {
    session.invalidate(); // 失效旧的会话
}
session = request.getSession(true); // 生成新的会话
```

防御措施

会话的攻击和防御

GDPR和CCPA关于cookie的条款

- 在读取cookie之前必须通知用户；
- 用户有权拒绝读取cookie数据；
- 即使用户拒绝读取cookie，也能使用网站的大部分服务。

04

会话安全设计方案

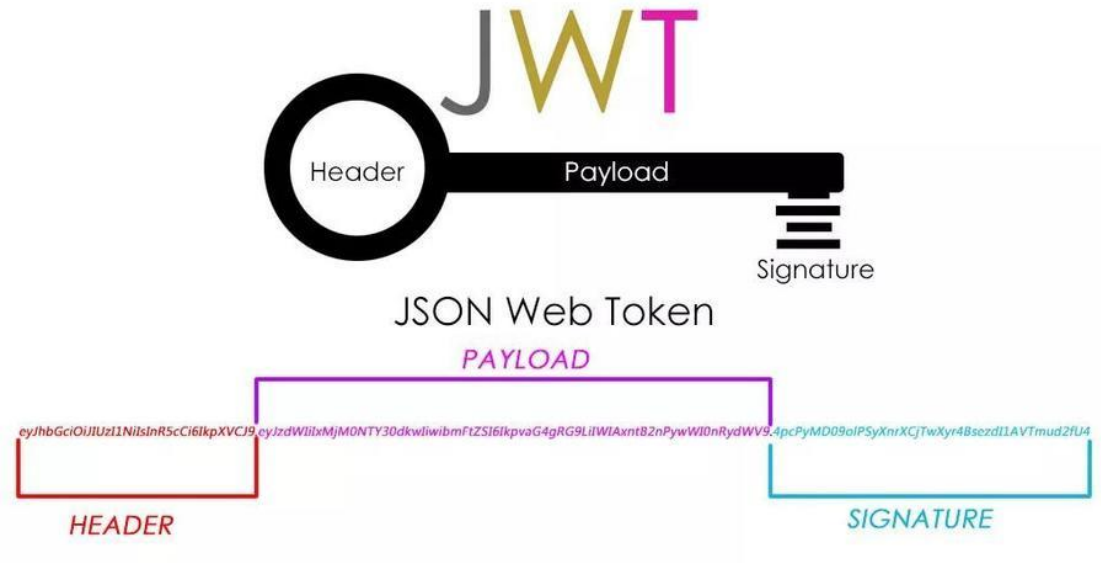
- ✓ 跨域认证解决方案JWT
- ✓ 会话设计方案

基于会话的跨域认证解决方案JWT

“它是一种公开标准（RFC 7519），定义了一种简洁的，自包含的方法用于通信双方之间以Json对象的形式传递会话信息。”

{ JWT }

JSON Web Token



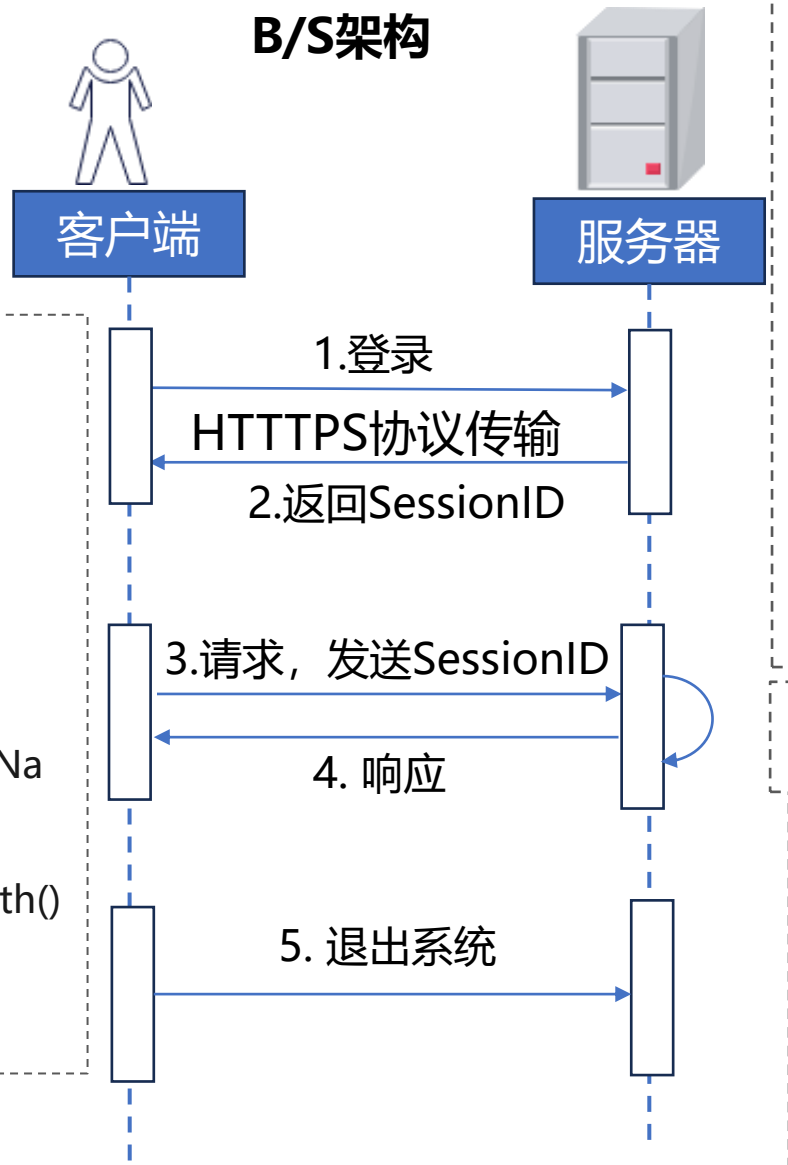
会话安全设计方案

wondershare 万兴科技

会话安全设计要求

1. sessionID值的长度不小于24字节，192bits 。
2. sessionID名称改成通用名称，如“sessionID、ID”。
3. sessionID的值应该使用安全伪随机数生成。
4. session对象应存储在服务器端，客户端只保存sessionID。
5. 使用安全传输协议（如TLS）传输sessionID。
6. 客户端使用cookie传输和保存sessionID。
7. Cookie设置安全属性：HTTPOnly、Secure、SameSite、Domain、Path、Expire、Max-Age
8. 重要操作或金融类交易使用token校验。
9. 认证成功以后立即重置session。
10. 用户退出系统时使会话失效。
11. 禁止在URL或日志中暴露会话标识。

会话安全设计方案



客户端用Cookie保存SessionID

```
Cookie cookie=new
Cookie( ‘sessionID’ ,sessionID);
cookie.setHttpOnly(true);
cookie.setSecure(true);
cookie.setMaxAge(-1);//临时cookie
cookie.setDomain(request.getServerNa
me());
cookie.setPath(request.getContextPath()
);
cookie.setSameSite(Strict);
```

登录成功，生成会话

```
//随机生成SessionID，长度不小于24字节
SecureRandom random = new SecureRandom();
byte[] bytes = new byte[24];
String SessionID=random.nextBytes(bytes);
//生成新会话，并使旧会话失效
HttpSession session = request.getSession(false);
if(session != null) {
session.invalidate(); // 失效旧的会话
}
session = request.getSession(true); // 生成新的会话
session.setId(SessionID);
session.setMaxInactiveInterval(10*60);//设置超时时
间10分钟
```

服务器端校验SessionID
如果是管理类或交易类操作，校验Token值

退出系统，删除会话

```
public void logout() {
// 根据用户请求获取用户对应会话
HttpSession session = request.getSession(false);
// 删除会话信息
if (session != null) {
session.invalidate();
...// 将用户退出操作记录到日志中
}
... // 清理逻辑
```

思考和建议

工作中的3点应用（或行动）建议

1. 参加《手把手带你掌握WS研发安全体系》课程

2. 研发过程中提升安全意识；

3. 遵守《万兴科技研发安全会话规范》；

1个学习方向建议

1. 《白帽子讲Web安全》吴翰清

1. 会话的出现使互联网拥有了“记忆”；
2. 会话的定义和生命周期，如SessionID、cookie、token；
3. 会话的攻击技术和防御措施：中间人攻击、XSS、CSRF、会话固定攻击，防御措施各不相同；
4. 如何设计安全的会话方案。

wondershare 万兴科技

学习心得提交

1、提交路径：

日志——学习心得

2、提交时间：

当天24:00前完成总结提交，按时提交可获得相应的学习积分。


始于实践 终于实践
向内反思 向外求知
2023让我们一起学习成长