CSRF

跨站请求伪造（英语：Cross-site request forgery），通常缩写为CSRF是一种挟制用户在当前已登录的Web应用程序上执行非本意的操作的攻击方法。跟跨网站脚本（XSS）相比，**XSS** 利用的是用户对指定网站的信任，CSRF 利用的是网站对用户网页浏览器的信任。

解决方案：

1）检查Referer字段

2）添加校验token

XSS

跨站脚本（英语：Cross-site scripting，通常简称为：XSS）是一种网站应用程序的安全漏洞攻击，是代码注入的一种。它允许恶意用户将代码注入到网页上，其他用户在观看网页时就会受到影响。这类攻击通常包含了HTML以及用户端脚本语言。

Token

一种验证数据由服务端产生

https://my.oschina.net/jamesfancy/blog/1613994

1. Token 完全由应用管理，所以它可以避开同源策略
2. Token 可以避免 CSRF 攻击
3. Token 可以是无状态的，可以在多个服务间共享

单点登录

单点登录（Single Sign On），简称为 SSO，是比较流行的企业业务整合的解决方案之一。SSO的定义是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统。

实现方式：

1）“共享Cookie”（不安全）

2）使用token标识（整个server群唯一 一个）

JWT

Json web token (JWT), 是为了在网络应用环境间传递声明而执行的一种基于JSON的开放标准（(RFC 7519).该token被设计为紧凑且安全的，特别适用于分布式站点的单点登录（SSO）场景。JWT的声明一般被用来在身份提供者和服务提供者间传递被认证的用户身份信

息，以便于从资源服务器获取资源，也可以增加一些额外的其它业务逻辑所必须的声明信息，该token也可直接被用于认证，也可被加密。