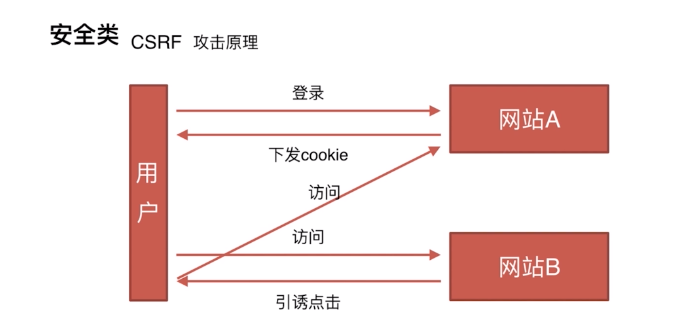
CSRF和XSS

## 基本概念和缩写

CSRF：跨站请求伪造 Cross-site request forgery



能实现CSRF的两个条件：

1. 网站中某个接口存在这种漏洞
2. 用户在这个网站登陆过

## CSRF防御措施

1. Token验证：本地存在一个token 如果点击了引诱链接，这个链接只会携带cookie而不会携带token 所以能防止。
2. Referer验证：页面来源 如果服务器判断我这个页面是不是我的站点下面的页面，如果是 就允许
3. 隐藏令牌：和tonken相似，比如说隐藏在http head头中，不会放在链接上

## XSS

基本概念和缩写：

XSS（cross-site scripting） 跨域脚本攻击

它的攻击原理：是向页面注入脚本（JS）

防御措施：核心的宗旨就是让你插入的JS不可执行。

XSS是向你页面注入JS运行，JS函数体里去加入它向让你做的事情。

CSRF是利用你本身的漏洞，去帮你自动执行那些接口，而且CSRF依赖你用户登录过网站。