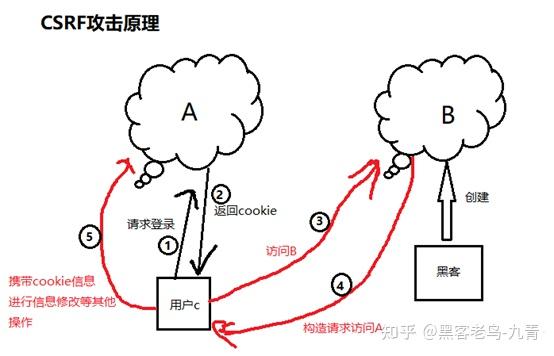
CSRF(跨站请求伪造漏洞)

攻击者盗用你的身份，以你的名义发送恶意请求，但是对服务器来说，这个请求是完全合法的，但是却完成了攻击者所期望的操作，比如发送邮件，信息，甚至是购买东西



关键就是在用户不知情的情况下携带cookie信息进行信息修改等操作

在用户未退出网站A的情况下，在同一浏览器中请求了黑客构造的恶意网站B

B网站收到用户请求后返回攻击性代码，构造访问A网站的语句

CSRF攻击的防御

1. 验证HTTP Referer

HTTP中有一个referer的字段，它几率该HTTP请求的访问来源地址。通常情况下访问一个安全受限页面的请求来自同一个网站。所以要防御CSRF，可以通过验证其referer是否合法

2 在请求地址中添加token并验证

CSRF 攻击之所以能够成功，是因为黑客可以完全伪造用户的请求，要抵御CSRF 关键在于在请求中放入黑客不能伪造的信息，且该信息不存在与cookie之中。 可以在HTTP请求中以参数的形式加入一个随机产生的token，并在服务器端建立一个拦截器来验证这个token