csrf需要掌握的

1、cross-site request forgery 跨站请求伪造

2.攻击原理：在B网站引诱用户访问A网站（用户之前登陆过A网站，浏览器cookie缓存了身份验证信息），调用A网站的接口攻击A网站

3.防御措施：

（1）token验证：登陆成功后服务器下发token令牌存到用户本地，再次访问时要主动发送token，浏览器只能主动发cookie，做不到主动发token

（2）referer验证：判断页面来源是否自己站点的页面，不是不执行请求

（3）隐藏令牌： 令牌放在http header头中，而不是链接中

xss

1.cross-site scripting跨域脚本攻击

2.不需要登陆认证，向你的页面通过合法渠道注入脚本

3.防御：令xss无法执行

CSRF与xss的区别：

csrf需要用户登陆，利用网站自己的接口漏洞进行攻击

xss通过注入脚本执行自己的代码