渗透测试工程师技术实战课

CSRF漏洞

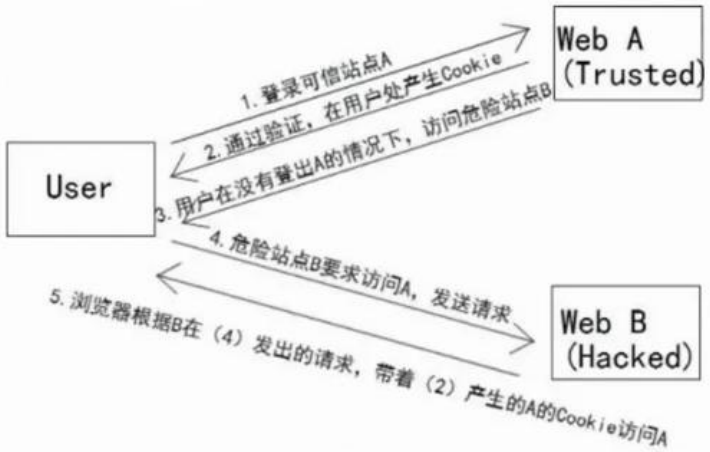
CSRF漏洞基础

- Cross-site request forgery
- 与XSS经常混淆
- 从信任的角度来区分
  - XSS：利用用户对站点的信任
  - CSRF：利用站点对已经身份认证的信任

- 构造代码 → 伪装代码 → 发送给受害者 → 受害者打开 → 攻击者获取受害者的Cookie → 攻击者使用受害者的Cookie去干坏事 → 攻击完成
- 构造代码 → 伪装代码 → 发送给受害者 → 受害者打开 → 受害者执行了恶意代码 → 攻击完成

CSRF漏洞基础

- 结合社工在身份认证会话过程中实现攻击
  - 会员中心、后台管理、用户注册、发布帖子、用户后台、交易管理
  - 修改账号密码、个人信息（email、收货地址）
  - 发生伪造得业务请求（网银、购物、投票）
  - 在用户非自愿，不知情得情况下提交请求



CSRF漏洞测试

- 业务逻辑漏洞
  - 对关键操作缺少确认机制
  - 自动扫描程序无法发现此类漏洞
- 漏洞利用条件
  - 被害用户已经完成身份认证
  - 新请求的提交不需要重新身份认证或确认机制
  - 攻击者必须了解Web APP请求的参数构造
  - 诱使用户触发攻击的指令（社工）
- Burpuste CSRF PoC generator
  - Post/Get方法

CSRF漏洞防御

- 通过CSRF-token或者验证码来检测用户提交
- 验证Referer/Content-Type
- 对于用户修改删除等操作最好都使用POST操作
- 避免全站通用的cookie，严格设置cookie的域

谢谢观赏