渗透测试工程师技术实战课

业务逻辑漏洞的原理以及分析

业务逻辑漏洞基础

- 之所以称为业务逻辑漏洞，是由于代码逻辑是通过人的逻辑去判断，在我们所测试过的平台中基本都有发现，包括任意查询用户信息、任意删除等行为；最严重的漏洞出现在账号安全，包括验证码暴力破解、任意用户密码重置、交易支付、越权访问等等

业务逻辑漏洞分析

- 业务
- 注册
  - 任意用户注册
  - 短信轰炸/验证码安全问题/密码爆破
  - 批量注册用户
  - 枚举用户名/进行爆破
  - SQL注入/存储型XSS
- 登录
  - 短信轰炸/验证码安全问题/密码爆破
  - SQL注入
  - 可被撞库
  - 空密码绕过/抓包把password字段修改成空值发送
  - 权限绕过/Cookie仿冒

业务逻辑漏洞分析

- 密码找回
  - 短信邮箱轰炸/短信邮箱劫持
  - 重置任意用户密码
  - 新密码劫持/直接跳过验证步骤
  - 本地验证，修改返回值
- 购买支付/充值
  - 交易金额/数量修改
  - 如果返回当参数中有一些奇怪的参数，可以把这个而参数添加到请求包中然后重发
  - 修改充值账户可控参数
- 优惠券/代金券
  - 刷优惠券/代金券
  - 修改优惠券金额/数量

业务逻辑漏洞分析

- 传输过程
  - 明文传输账号密码
  - 修改信息处无session/token导致csrf
  - POST/COOKIE注入
- 评论
  - POST注入/存储XSS
  - 无session/token导致CSRF

业务逻辑漏洞分析

- 漏洞处
- 验证码问题
  - 万能验证码0000，8888，1234
  - 返回包中存在验证码
  - 删除验证码或者cookie中的值可以爆破账号密码
- 短信轰炸
  - 重放数据包
  - 删除修改cookie
  - 手机号前面加 +86或者空格
  - 请求参数修改大小写，或者添加请求参数比如&id=1
- 水平越权
  - 主要登陆后还是修改参数，主要找到多个接口不断测试
  - 多个账号
- 数据泄露
- 任意用户密码重置

●业务逻辑漏洞分析

●确定业务流程--->寻找流程中可以被操控的环节-->分析可被操控环节中可能产生的逻辑问题--->尝试修改参数触发逻辑问题

●案例

谢谢观赏