Web 漏洞挖掘的奇淫技巧

一、商城网站

1.1 登录

1.2 注册

1.2.1 短信轰炸

1.参数修改短信轰炸
2.cookie 短信轰炸
3.根据业务判断

1.2.2 任意用户注册

1.验证码爆破，burpsuite
2.绕过验证码，修改或者删除参数
3.返回包中包含验证码

1.2.3 绕过验证

1.删除参数
2.修改参数将验证码修改为 0000
3.构造验证码

1.2.4 批量注册

userid 参数

1.2.5 手机号枚举遍历

1. 绕过风控继续遍历
2.简单遍历接口

1.3 找回密码

短信验证码
邮箱验证码
找回链接 url 参数修改、步骤逻辑绕过
修改参数：修改每一个可疑参数
绕过找回密码

1.4 第三方登录

任意用户登录
登录凭证劫持
短信验证码

1.5 业务层逻辑

1.5.1 个人中心

url 中 id 参数越权

1.5.2 购买产品

找到喜欢的商品，添加购车，提交订单，支付订单，基本的流程是这样的，但是在这三个物过程中可能都会存在某个缺陷根据业务的设计来判断，其次可以修改产品的数量，产品的时间，优惠卷，产品的id，sku值，等等

支付漏洞

1.5.3 商城活动

优惠券、积分兑换

1.6 细心+细节

1细心.Post参数 get参数 cookie 参数 js参数
对这些参数都需要细心的测试，重复组合测试
2细节.在测试的过程中对每一个可能存在漏洞的按钮进行测试，重复利用，相同的功能可能一个存在着漏洞一个不存在这都是可能有这些问题。

1.7 漏洞组合拳

self-xss+csrf 组合拳
逻辑漏洞组合拳
设计缺陷组合拳