##  业务逻辑漏洞

 ——————并发
1.漏洞描述：
 竞争/并发漏洞，常属于逻辑业务中的漏洞类型，例如攻击者通过并发http/tcp请求而达到多次获奖、多次收获、多次获赠等非正常逻辑所能触发的效果。

下面以简化的例子说明在交易的Web应用程序中潜在的并行问题：

1.帐户A有100存款，帐户B有100存款。用户1和用户2都希望从帐户A转10分到帐户B.

2.如果是正确的交易的结果应该是：帐户A 80分，帐户B 120分。

3.然而由于并发性的问题，可以得到下面的结果：

4.用户1检查帐户A ( = 100 分)

5.用户2检查帐户A ( = 100 分)

6.用户2需要从帐户A拿取10分(=90分)，并把它放在帐户B (=110分)

7.用户1需要从帐户A拿取10分(仍然认为含有100个分)(=90分)，并把它放到B(=120分)

8.结果：帐户A 90 分，帐户B 120 分。

#### 2.漏洞测试工具：

Turbo intruder 工具是burp自带的插件，可以用于对密码的爆破，验证码的爆破和并发漏洞测试。



测试方法:使用Turbo intruder模块对其抓包进行测试：

#### 3.案例 ：

百度并发领取智能算力：





然后进入领取奖励的时候点击抓包发送到turb0模块：



然后攻击刷新页面即可：



刷新一下:

 

这个漏洞大概给了50积分 也就是250元 ，当然并发漏洞在我们测试是非常多的下面看看这些审核通过的：



![GI{}~Q3B]Q1I5S)@2%O5PO5]()

挖这些漏洞只需要努力和坚持就行，对于学生来说一个月挖几百块的零花钱完全不是问题，下面是我对并发测试场景的总结

**并发测试主要测试场景：签到、每天领积分，点赞，评论点赞处等**，测试是否并发发送请求服务器可多次响应

1. 提升危害
思考：如何提升并发漏洞的危害呢？
 如果要提升并发漏洞的危害，那我们必须和金钱的地方挂钩或者要让厂商感觉可以利用这一点来到达辱羊毛的效果，此时我们的并发漏洞也可以获取的高额赏金：
![BN{]BHZ)Y8BP3)VPO9SU71S]()
该漏洞获取了150积分，在比赛期间是4倍就是600分也就是3000rmb,可以说此漏洞毫无技术可言，只需要自己善于发现即可
而且这样的漏洞点还很多：
 