fcmit.cc

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)

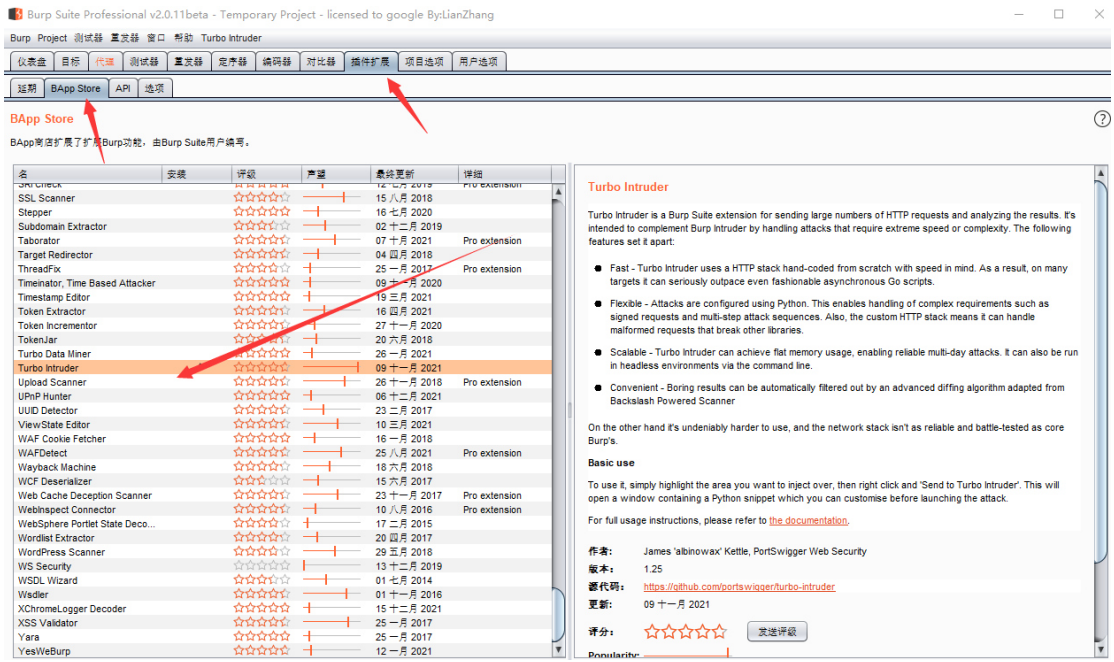
6.用户 2 需要从帐户 A 拿取 10 分(=90 分)，并把它放在帐户 B (=110 分)

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：

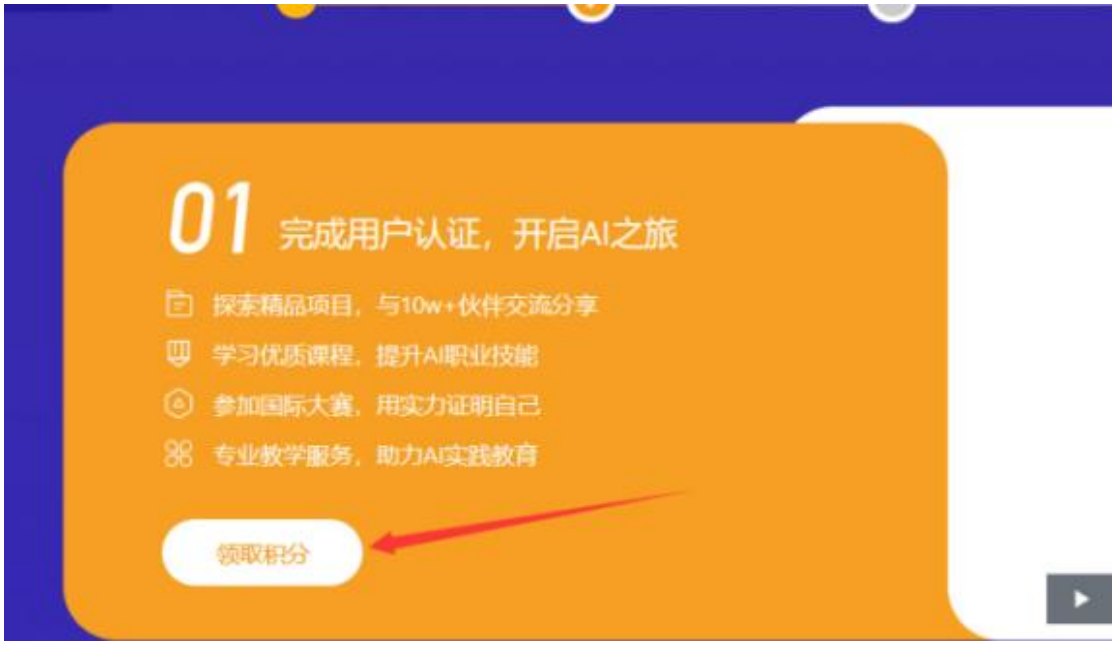
Turbo intruder 工具是 burp 自带的插件，可以用于对密码的爆破，验证码的爆破和并发漏洞测试。



测试方法:使用 Turbo intruder 模块对其抓包进行测试：

3.案例 ：

某某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：

fcmit.cc

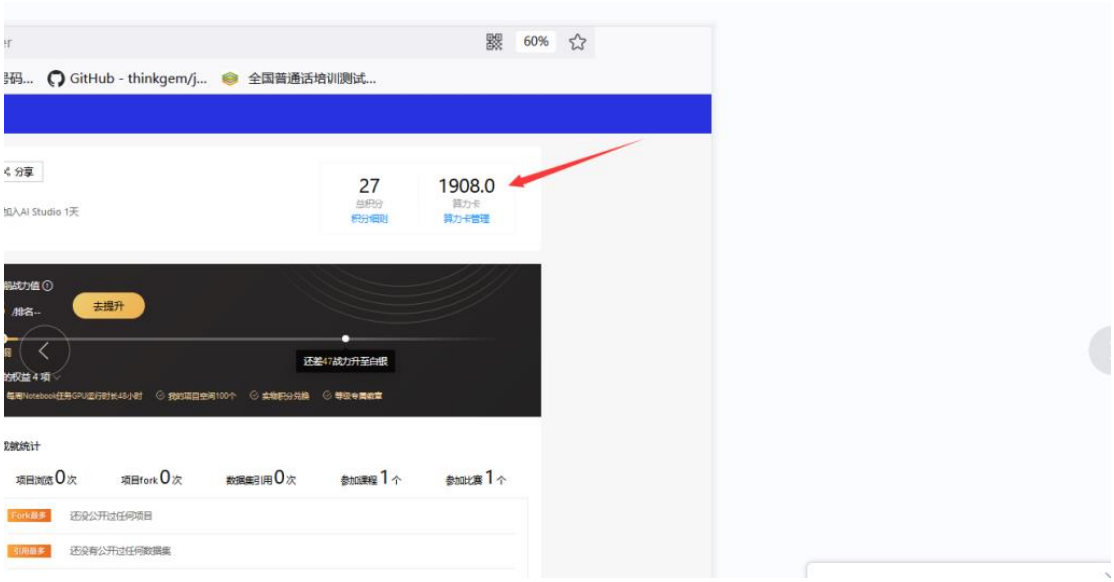
fcmit.cc

```
POST /[redacted] HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4495.0 Safari/537.36
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: https://aistudio.baidu.com/aistudio/newbie
x-requested-with: XMLHttpRequest
x-studio-token:
5918FF0281092E55FED7C3D89ADD6FCDA1AA44BC2CEBB7A1ED1C4DC62DA06B454DA7307327
61844A25E56B7864A7B798
Content-Type: application/x-www-form-urlencoded
Origin: [redacted]
Connection: close
Cookie: __cas__st__533=NLI; __cas__id__533=0; __cas__rn__=0;
Hm_lvt_6b7a9d245c3be48de953790e7b6aea6b=1635861297;
Hm_lpvt_6b7a9d245c3be48de953790e7b6aea6b=1635862821;
Hm_up_6b7a9d245c3be48de953790e7b6aea6b=%7B%22user_reg_date%22%3A%7B%22value%22
%3A%2220211101%22%2C%22scope%22%3A1%7D%2C%22user_course_rt%22%3A%7B%22valu
e%22%3A%22%E9%9D%9E%E8%AF%BE%E7%A8%8B%E7%94%A8%E6%88%B7%22%2C%2
2scope%22%3A1%7D%2C%22user_center_type%22%3A%7B%22value%22%3A%221%22%2C%2
2scope%22%3A1%7D%7D; jsdk-uuid=5ac013f5-b603-4d00-897c-bc6956a8f32d;
jsdk-uuid=5ac013f5-b603-4d00-897c-bc6956a8f32d;
[redacted]=0B0FC6F46AD8DA4463B9E4ED787215FF:FG=1;
[redacted]_BFESS=0B0FC6F46AD8DA4463B9E4ED787215FF:FG=1;
BDUSS=01Qb0p2anowLTJJc2tuenF5NDNnTW9QZ1h4QlU5NUpKQ2Y5UXRvUUU1cFlwS2hoRUFBQU
FBJCQAAAAAAAAAAAEAAAB9wwOUamF5Y2hvaXMxMjMAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAFFDgWFRQ4Fhd;
BDUSS_BFESS[redacted]
RUFBQUFBJCQAAAAAA[redacted]AAAAAA
AAAAAA[redacted]AAAAAAAAAAAAAAAAAAAAAAFFDgWFRQ4Fhd;
ai-studio-ticket=9EF17FB007C548CCB26F03E7D05F9BE287F8541252C04D718B6EE412B389DE0E
; match-invite-ticket=
Content-Length: 0
```

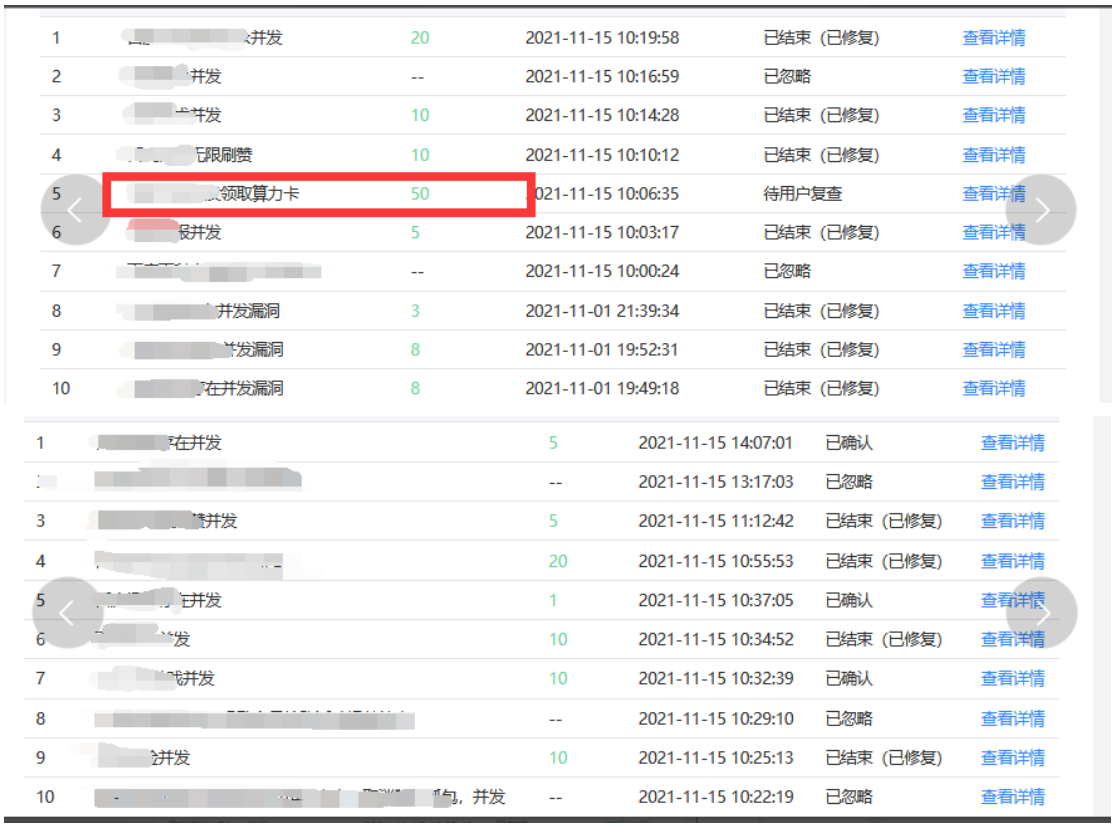
然后攻击刷新页面即可：

fcmit.cc

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：



1	[redacted]并发	20	2021-11-15 10:19:58	已结束（已修复）	查看详情
2	[redacted]并发	--	2021-11-15 10:16:59	已忽略	查看详情
3	[redacted]并发	10	2021-11-15 10:14:28	已结束（已修复）	查看详情
4	[redacted]限刷赞	10	2021-11-15 10:10:12	已结束（已修复）	查看详情
5	[redacted]领取算力卡	50	2021-11-15 10:06:35	待用户复查	查看详情
6	[redacted]并发	5	2021-11-15 10:03:17	已结束（已修复）	查看详情
7	[redacted]	--	2021-11-15 10:00:24	已忽略	查看详情
8	[redacted]并发漏洞	3	2021-11-01 21:39:34	已结束（已修复）	查看详情
9	[redacted]发漏洞	8	2021-11-01 19:52:31	已结束（已修复）	查看详情
10	[redacted]在并发漏洞	8	2021-11-01 19:49:18	已结束（已修复）	查看详情

1	[redacted]在并发	5	2021-11-15 14:07:01	已确认	查看详情
[redacted]	[redacted]	--	2021-11-15 13:17:03	已忽略	查看详情
3	[redacted]并发	5	2021-11-15 11:12:42	已结束（已修复）	查看详情
4	[redacted]	20	2021-11-15 10:55:53	已结束（已修复）	查看详情
5	[redacted]并发	1	2021-11-15 10:37:05	已确认	查看详情
6	[redacted]发	10	2021-11-15 10:34:52	已结束（已修复）	查看详情
7	[redacted]并发	10	2021-11-15 10:32:39	已确认	查看详情
8	[redacted]	--	2021-11-15 10:29:10	已忽略	查看详情
9	[redacted]并发	10	2021-11-15 10:25:13	已结束（已修复）	查看详情
10	[redacted]，并发	--	2021-11-15 10:22:19	已忽略	查看详情

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