BETA SPRINT · DAY 5 · 测试岗交付

不鸽工程队

Beta 冲刺 Day5 测试报告

高并发混合场景与安全加固专项

测试岗　王嘉萍

报告日期　2026 年 11 月 17 日

团队名称　不鸽工程队

目 录

摘要 1
一、环境与基线 1
二、M1 混合并发（BUG-6） 2
三、M2 幂等验证 3
四、M3 信用流水（BUG-7） 3
五、安全用例（BUG-8） 4
六、BUG-4 / BUG-5 结案 4
七、新契约变化 4
八、明日安排 5

摘要

> Day5 三项任务全部完成并推送。混合并发压测（M1）与多人并发评价（M3）各发现一个 P1 级并发缺陷：**BUG-6 取消活动在混合并发下死锁回滚返回 5000**；**BUG-7 并发评价信用分丢失更新，+30 分只到账 +4**。幂等验证（M2）通过：同一用户 20 连点恰好 1 成功 + 19 次拦截。安全用例 10 条落地，发现配置面缺陷 BUG-8（默认 JWT 密钥可离线伪造任意用户 token）。全量回归 77 条：73 通过、0 失败、1 skip、2 xfail、1 xpass，执行 24.5 秒。Day4 挂账的 BUG-4、BUG-5 验证结案。

被测版本为 master 4e48df4（含实名三档与 AES 加密改造）。当日两条 P1 并发缺陷均已写成守门用例挂账，配合 BUG-8 一并排入 Day6 修复计划。

一、环境与基线

- master 更新：李佳实名三档校验（4018/4019）+ AES 加密改造（6c53936）+ 互评资格校验（e09ce85，修复 BUG-4）合入；本人 Day4 两条提交已随 48be8cc 进 master。
- 本地库补跑三个迁移脚本（幂等）：day5_real_name_roster、day5_verify_status_migrate、day6_sensitive_hash；2024 级软工真实名册 216 人已导入 real_name_roster（数据文件在 sql/local/，gitignore 保护，不入库不外传）。
- 本地 application.yml 补 sensitive.crypto 密钥段（32 字节 Base64 AES-256 密钥 + pepper），否则新版后端无法启动。
- 测试框架适配实名校验：学号改 9 位纯数字；新注册默认「待核验」不能发起活动（4019），测试发起人账号做库侧核验造数（flows.verify_user，与 set_credit 同性质）。

二、M1 混合并发：报名 + 退出 + 取消（BUG-6，P1）

场景：活动 20 人上限（发起人占 1，可报名 19 坑），预热 9 人占坑；同一 Barrier 同刻释放 16 线程——10 人报名（恰好填满余坑）、5 人退出、发起人取消活动。

指标	实测
返回码	报名 10 条全 0；退出 5 条全 0；取消 1 条 5000
本轮死锁（日志增量）	5 条，DeadlockLoserDataAccessException
死锁位置	ActivityServiceImpl.cancelActivity 第 383 行批量退名额 UPDATE
名额账本	current_people=15 = 14 条有效报名 + 发起人，无超卖、无重复行
延迟	avg 46~63ms，p95 69~77ms

复跑 4 次的形态：死锁受害者轮换——第一轮取消失败、另一轮 2 条退出失败、第三轮取消又失败。锁序冲突随机打在一个事务上，MySQL 挑一个回滚，表象不稳定但死锁 4/4 全复现。

根因：signup 事务「插 registration + UPDATE activity.current_people」，cancel 事务「UPDATE activity 之后批量 UPDATE registration」，两个事务以相反顺序获取 activity 与 registration 行锁，形成环形等待。

BUG-6（P1）：混合并发下取消活动死锁回滚，接口返回 5000（应为 0）。修复建议：统一加锁顺序（先锁 activity 再动 registration）或缩小取消事务。守门用例 test_08_concurrency.py::test_cc01（xfail 挂账，复现概率约 2/3，判定以 M1 压测为准）。

三、M2 同一用户并发重复报名（幂等验证，通过）

指标	实测
20 连点返回	1 条 code=0 + 19 条 4011，0 条其它
库侧	有效报名恰 1 行，current_people=2
结论	通过：应用层防重快查 + 唯一索引兜底可靠

前端连点、消息重发这类场景可以放心。

四、M3 多人并发评价同一活动（BUG-7，P1）

场景：被评人起始 50 分，15 名参与者并发各评一次（每评 +2，不触发 100 封顶）。期望 15 条流水、score_after 逐笔 +2 递增（52 到 80）、终值 80。

核对项	期望	实测
评价成功 / 库中评价行 / 流水行	15 / 15 / 15	15 / 15 / 15
score_after 序列	52,54,…,80 严格递增	52×10，54×5
终值	80	54

BUG-7（P1）：并发评价信用分丢失更新。加分实现是「读分数、内存算新值、整值写回」，并发事务读到同一旧值后互相覆盖；流水每笔都记了账，档案却对不上——15 人评价 30 分的信用增量蒸发 26 分。修复建议：改原子自增 UPDATE（SET credit_score = credit_score + 2，封顶用 LEAST），或 SELECT 之后 FOR UPDATE 加行锁。守门用例 test_cc02（xfail 挂账，5 人并发 +10 必须精确到 60）。

五、安全用例（10 条，发现 BUG-8）

组	用例	结果
认证	无 token、垃圾 token、改 payload 不改签名	全 401，通过
越权	水平越权退他人报名（4040，本人可退）	通过
越权	待核验发起活动 4019，报名不受限	通过
实名	名册命中免造数直发活动；冒用学号 4018 且文案不泄露归属	通过
注入	登录 SQL 注入 4 组 payload；存储型注入原样入库、表完好	通过
密钥	仓库默认 dev secret 离线伪造 userId=1 合法 token	伪造被接受，挂账

BUG-8（P2，配置面）：bugedu.jwt.secret 默认值随仓库可见，未设 JWT_SECRET 环境变量时，拿到仓库的人可离线签发任意 userId 的合法 token。修复建议：部署侧强制注入随机密钥并废弃默认值。守门用例 test_sec_d03（xfail 挂账）。

六、BUG-4 / BUG-5 结案确认

李佳 e09ce85 合入后，Day4 两条挂账按预期转正：越权评价 4016、未结束评价 4017，xfail 转硬断言；被评价人不存在由资格层在 insert 前拦截（4016），5000 路径消除，按新契约断言结案。

七、新契约变化与用例修正

- 消息分页 size/page 越界从「静默收敛」改为显式 4001（林严泽 ddb9b20），BD-M01/M02 按新契约改写。
- 非发起人看报名名单从 4040 改为 4030，BD-P04 同步更新。

- 评价负向三态：4015 重复 / 4016 非参与者 / 4017 未结束，endpoints.Err 已补全。

八、明日安排（Day6）

1. BUG-6 / BUG-7 排给李佳，都是事务内改动，Day6 上云前修完风险最低。
2. BUG-8 在云端部署时一并处理（部署本来就要注入 JWT_SECRET）。
3. 修完跑 perf/mixed_load.py --scene ALL + test_08_concurrency.py 验收，去掉两条 xfail 标记转正式回归。
4. Day6 计划：1000 请求混合压测出 QPS/RT 图表，问卷数据整理。