

肉包智能采购 验证系统

把“创建任务、拼多多搜索、候选判断、人工确认”
连成一条可控、可审计、可回传证据的采购验证流程

统一后端



管理 Web + Android App + Go-Gin + VLM

当前: T-205 后端领取与租约完成

下一步: T-206 Android 接入

MVP 边界: 不自动下单 · 不支付 · 风控立即停止

从重复人工比对，变成可控的验证闭环

目标不是替人付款，而是减少提词、搜索、比较和记录的重复劳动。

今天的人工流程

- 1

看蝦皮文字和图片

人工理解 SKU、数量和关键外观
- 2

凭经验组合搜索词

不同人使用不同口径
- 3

逐个打开拼多多商品

比较过程耗时且难复盘
- 4

口头或零散记录结果

证据、理由和失败位置分散

系统带来的变化

- 01

把输入变成统一任务

标题、SKU、数量、预算和参考图保留原始事实，模型不能改写硬约束。
- 02

把候选判断变成可解释过程

最多检查 5 个可见候选，记录匹配项、缺失项、拒绝原因和截图证据。
- 03

把最终决定留给采购人员

自动化在确认点硬停止；人员接受、拒绝或转人工后只回传验证结论。

业务结果：同一口径 · 有界执行 · 有据可查 · 可持续优化

肉包智能采购验证系统

从后台任务到人工确认与证据回传；MVP 不提交订单、不支付



安全边界

- 采购人员手动领取
- 最多检查 5 个候选
- 验证码/风控立即停止
- 人工确认后只回传结果

AI 做识别和比较，不获得操作授权

模型输出受 schema 约束；搜索动作、推荐规则和人工结论由确定性代码控制。



确定性约束

- SKU、数量和预算来自原任务，模型不得改写
- 推荐候选由本地规则按 score、confidence 和拒绝项产生
- 模型不能返回点击坐标、页面动作或订单授权

口径提醒

“5 个候选”是特定账号、地区、时间和平台排序下的前 5 个可见结果，不是拼多多全平台最优 Top 5。

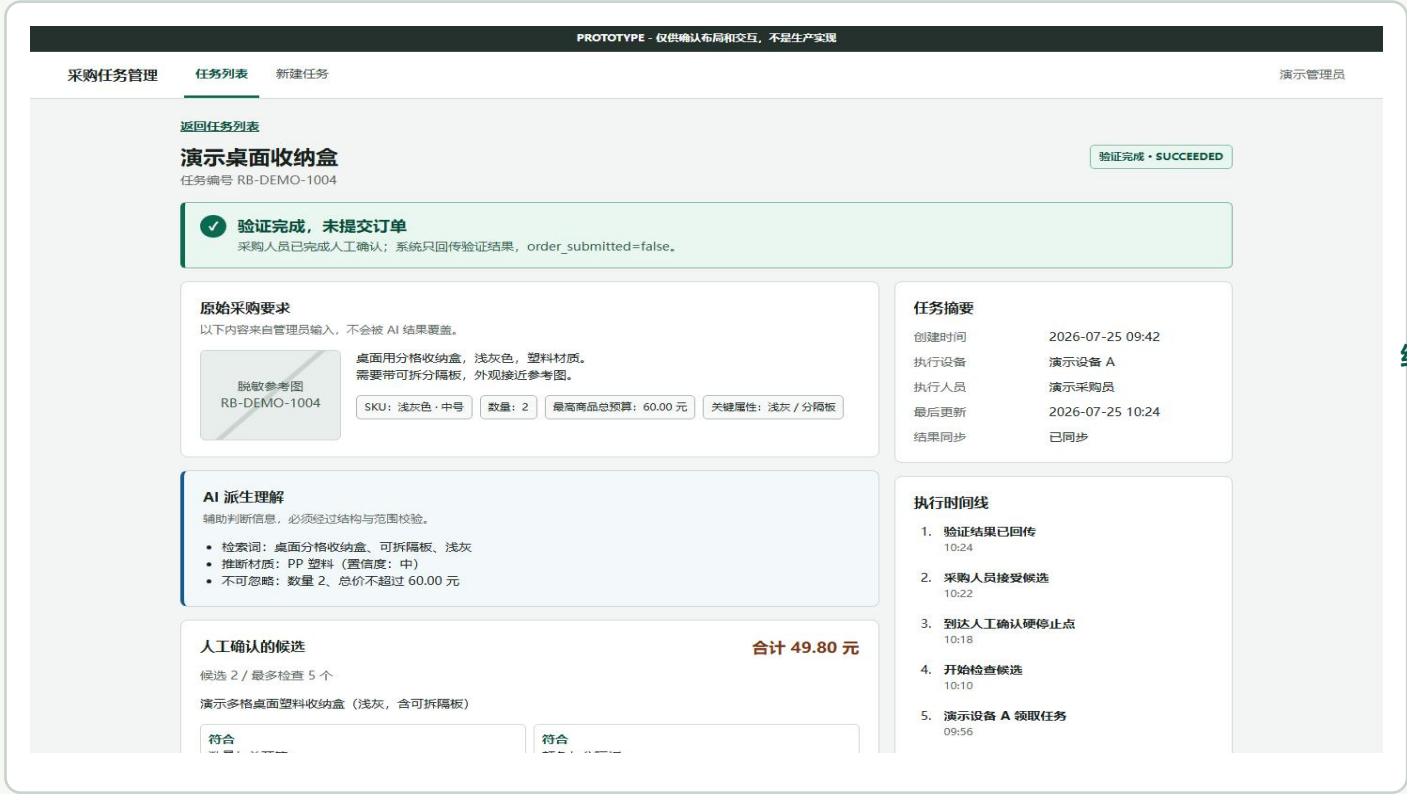
管理端和采购端各做自己擅长的事

两端共享同一个 Go-Gin 后端；管理凭证和采购设备凭证完全隔离。

管理 Web · 任务与证据

Android · 领取与人工确认

已确认低保真原型



统一后端



创建/取消任务 · 查看执行状态 · 查看候选、理由和截图

预检 · 手动领取 · 执行进度 · 安全停止

关键风险已验证，当前缺口是 Android 接入后端

后端 T-205 已完成；新版 APK 尚未安装，真实 VLM 供应商仍待确认。



现在已经具备

- Android 能基于本地任务搜索、采集并评估最多 5 个候选
- 后台能创建任务，BUYER 设备能被授权并原子领取
- 租约、幂等、安全取消和参考图授权已实现

现在还不能宣称

- 后台任务已经自动进入 Android 并跑完整流程
- 真实 LLM 的商品匹配质量已达到业务门槛
- 当前看到的 5 个候选是全平台最优结果

安全不是附加项，是流程能否继续的条件

模型不能扩大动作权限；服务端状态、设备身份和人工确认共同约束自动化。

MVP

不会自动
下单或支付

order_submitted = false

成功只表示验证流程完成并获得人员结论，不代表已购买商品。

01 手动领取

App 点击获取任务，不接受推送后无人确认地自动执行

02 有界浏览

每次最多检查 5 个可见候选，不无限滑动或全站抓取

03 风险即停

验证码、登录失效、风控、未知页和支付页立即停止

04 人工硬停止

候选确认页不会恢复自动点击，人员决定接受或拒绝

05 身份与租约

ADMIN 与 BUYER/设备凭证隔离，错误设备不能继续任务

06 证据受控

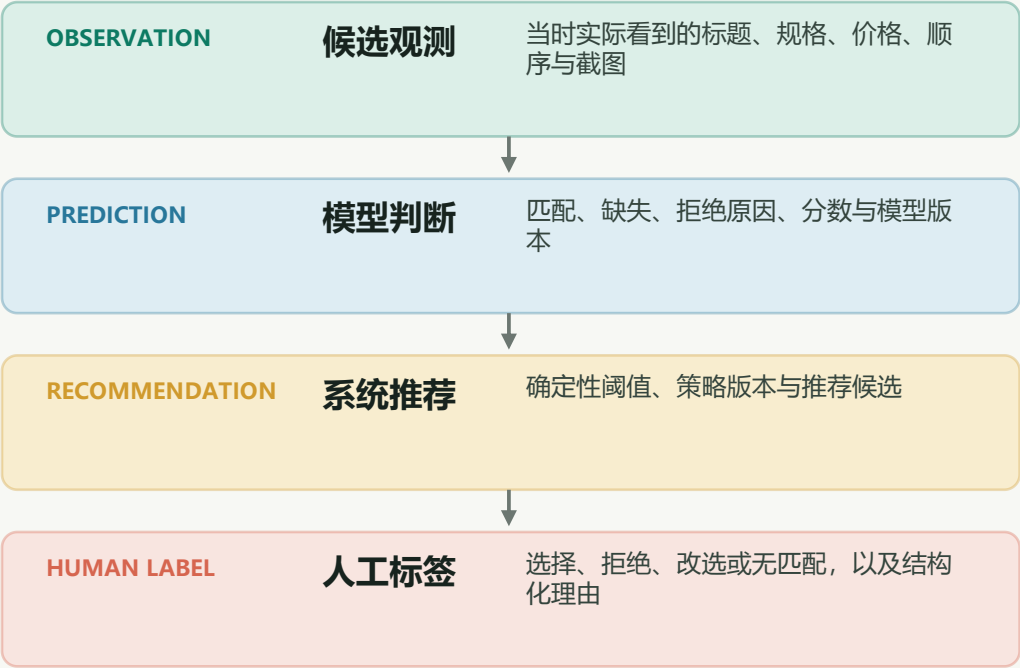
图片经鉴权、哈希和路径校验，不公开本地文件或任意 URL

验证码 / 风控 / 未知页面 / 支付边界 → 立即停止，不绕过、不猜测继续

先跑通第一版，再把每次人工判断变成可信数据

T-208 后置建设数据闭环；20 条真实任务试验只用人工结论评估模型。

后续数据闭环（T-208）



四层分开保存：模型理由不能自动成为人工理由

需要确认的四件事

- 1 真实 VLM 供应商
模型、测试凭证、调用预算和质量门槛
- 2 试验负责人
指定采购人员，并统一“可接受/拒绝”的标注口径
- 3 数据保留规则
截图保留期、隐私脱敏、平台条款和训练用途
- 4 20 条试验样本
覆盖代表性 SKU、图片质量、预算和异常类型

建议批准的推进顺序

T-206 App 接入 → T-207 结果回传 → T-208 数据闭环 → 20 条试验