

安全评估

rustSearch 平台的整体安全姿态文档。本文分五部分：[代码规模与组件清单](#) → [攻击面与信任边界](#) → [已实施的安全机制清单](#) → [已知风险与待办](#) → [白盒渗透测试](#)（已完成首轮授权测试，结果见 §五）。

文档用途 本页是[自检](#) + [首轮白盒渗透测试](#)的合并盘点。§五收录了 2026-09-25 完成的授权渗透测试结果（已全程脱敏，不披露任何域名、IP 与内部地址）；修复进展将持续更新。

PDF 版本 [下载《rustSearch 安全评估报告》PDF](#)（与本页内容一致，适合离线阅读与对外提供）

一、代码规模与组件清单

安全评估的前提是知道自己有多少代码、多少组件、多大暴露面。rustSearch 当前仓库（排除 `node_modules` / `target` / `dist` / `.output` / `.nuxt` / `vendor` / `__pycache__` 等产物与第三方依赖目录）的源码规模如下：

1.1 按语言统计

语言	文件数	行数	主要用途
Rust	565	166,727	13 个常驻微服务 + 运维 CLI (crates/ workspace, 34 个成员 crate)
JavaScript / TypeScript / Vue	422	162,824	前端 SPA、Mini App、Cloudflare Worker、文档工程
Go	218	46,749	app-store 商户商店微服务 + 少量 SDK
SQL	314	18,751	PostgreSQL 迁移脚本 (migrations/)
Dart (Flutter)	51	10,399	Android APP
Python	19	5,399	tg-client MTPROTO 客户端 + migration-tools 迁移工具 + 少量 SDK 示例
合计	1,589	410,849	—

仓库另含 [shopForPhp](#) (PHP 蓝本项目, 367 文件 / 27,173 行)，属于参考实现遗留物，**不计入 rustSearch 运行代码面**，不在本评估的攻击面内。

1.2 前端代码分布 (JS/TS/Vue 162,824 行)

目录	文件数	行数	说明
web/	225	100,671	主前台 / 后台管理 SPA

目录	文件数	行数	说明
workers/	69	27,758	Cloudflare Worker (Mini App 后端、文件中转、SSE 透传等)
vuepress/	98	28,361	本文档工程
notebook/	24	3,602	内部脚本/试验
clients/	2	1,436	客户端辅助脚本
prototype/	1	770	原型
gemeni/	1	25	试验
sdk/	2	201	SDK 示例

1.3 Python 代码分布 (5,399 行)

目录	文件数	行数	说明
clients/tg-client/	3	2,209	生产路径: Telethon MTProto 客户端, 关键词监听引擎
migration-tools/	11	2,165	数据迁移工具 (PG / Manticore / ES)
TrxEnergy/	2	756	TRON 能量相关脚本
sdk/supply-api/python/	2	217	SDK 示例
scripts/	1	52	运维辅助

1.4 服务组件清单 (暴露面盘点)

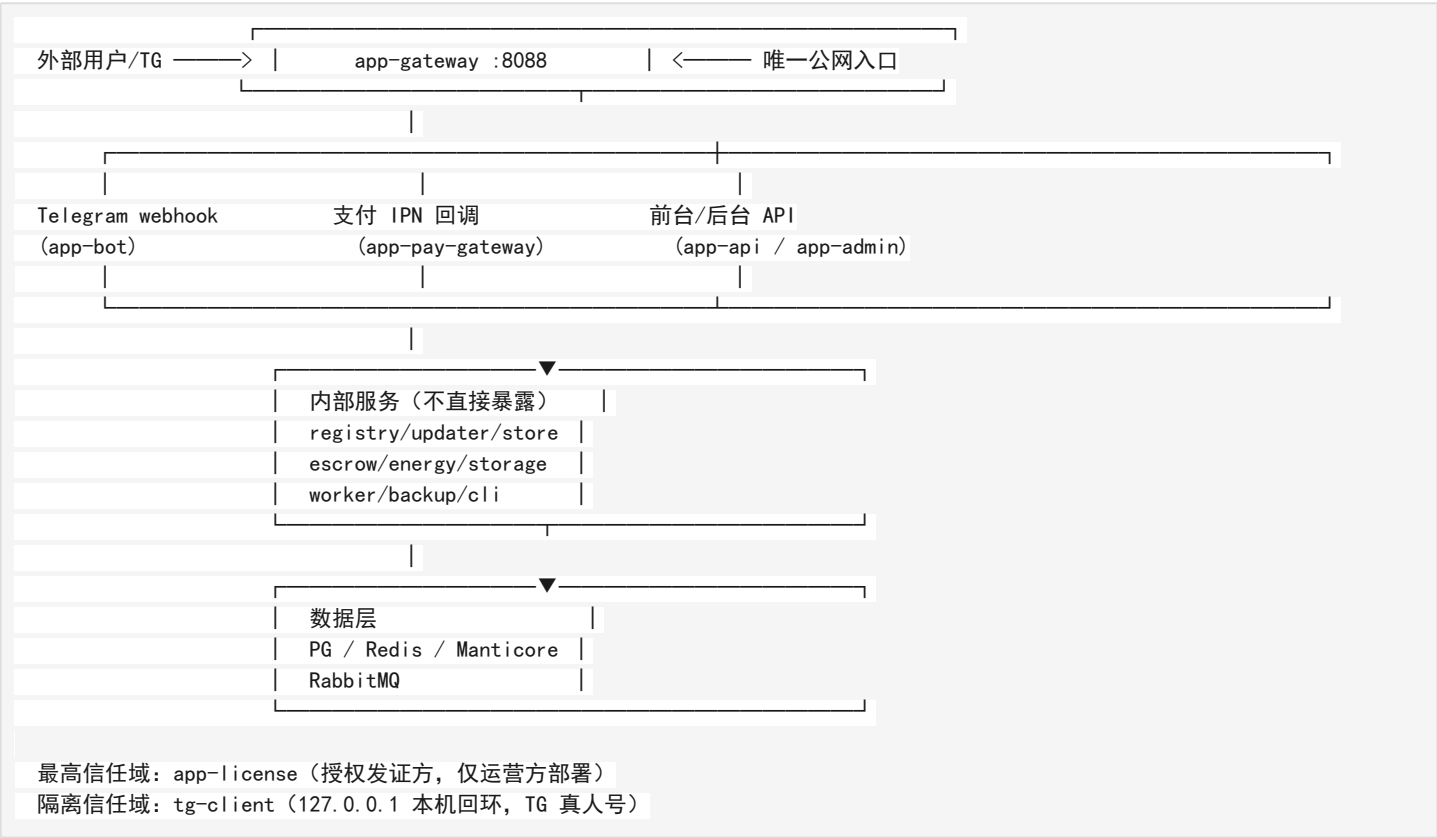
rustSearch 由 15 个常驻微服务 + 1 个运维 CLI 组成:

服务	默认端口	暴露面	信任边界
app-gateway	8088	公网入口 (唯一对外)	外部 → 内部
app-api	8081	仅经 gateway	内部
app-web	8082	仅经 gateway	内部
app-admin	8083	仅经 gateway (管理员鉴权)	内部, 敏感
app-bot	8443 / 8444	Telegram webhook (公网)	外部
app-pay-gateway	8448	支付渠道 IPN 回调 (公网)	外部, 资金敏感
app-ai-gateway	8447	仅经 gateway	内部, 调外部 OpenAI
app-escrow	8450	仅经 gateway	内部, 资金敏感
app-energy	8460	仅经 gateway + TRON 链上监听	内部, 资金敏感
app-storage	8462	仅经 gateway	内部
app-registry	8099	内网	内部, 集群信任根

服务	默认端口	暴露面	信任边界
app-updater	8090	内网	内部，授权大脑
app-license	8096	内网（仅运营方部署）	最高信任
app-backup	8095	内网	内部
app-worker	—	无监听端口	内部
app-store (Go)	8449	仅经 gateway	内部，资金敏感
tg-client (Python)	127.0.0.1:8188	仅本机回环	内部，TG 真人号
app-cli	—	运维工具	内部，高权限

基础设施：PostgreSQL 16、Redis 7（含 Sentinel）、Manticore 6.2、RabbitMQ。

二、攻击面与信任边界



关键边界：

边界	风险等级	主要威胁
公网 → app-gateway	高	DDoS、注入、扫描、凭据爆破
Telegram → app-bot	中	webhook 伪造、消息注入、Bot token 泄露
支付渠道 → app-pay-gateway	极高	IPN 伪造、重放、金额篡改
内部服务间	中	横向移动、共享密钥泄露
应用 → 数据层	高	SQL 注入、越权读写、数据泄露

边界	风险等级	主要威胁
tg-client → Telegram	中	真人号被风控、Session 泄露

三、已实施的安全机制

按域分类列出当前已落地的安全控制。每条都是代码或配置层面的客观事实，可由仓库佐证。

3.1 认证与会话

控制	实现位置	说明
密码散列	全栈	Argon2id (安全散列标准, 抗 GPU 破解)
后台会话	app-admin	JWT (HS256, 密钥由环境变量注入, 不硬编码)
Mini App 认证	app-bot / app-api	Telegram initData 验签 (HMAC-SHA256, 与 Bot token 派生密钥比对)
扫码登录	app-admin	Ticket 取出即焚 (一次性消费, 防重放)
服务间握手	app-registry	HMAC-SHA256 共享密钥 + 时间戳防重放
授权根信任	app-license → app-updater	RSA 签发授权码, 私钥仅运营方持有

3.2 注入与输入净化

控制	实现位置	说明
SQL 注入	全栈 Rust	sqlx 编译期校验的参数化查询, 无字符串拼接 SQL
ORM 层	Go app-store	GORM 参数绑定
HTML/XSS	前端 + Bot	富文本白名单净化 (服务端二次净化, 禁止裸渲染)
商户输入	app-store / app-admin	关键字段 (名称、描述、链接) 服务端净化
模板注入	app-bot	消息模板渲染走白名单变量, 不解析任意表达式

3.3 资金与支付

控制	实现位置	说明
金额约束	PostgreSQL	CHECK 约束 (金额非负、上限校验), 数据库层兜底
金额单位	全栈	微单位整数 (1 USDT = 1,000,000), 无浮点误差
IPN 验签	app-pay-gateway	各支付渠道独立验签 (支付宝 RSA / USDT HMAC 等)
IPN 幂等	app-pay-gateway	订单号 + 流水号唯一约束, 重复回调自动去重
余额事务	wallet 域	扣款/退款走 PG 事务, 失败回滚

控制	实现位置	说明
商户审批	app-escrow	审批与资金解耦（先审批，后资金动作，故障可回滚）
能量租用	app-energy	链上到账监听 + 金额完全匹配才履约，多转/少转不命中

3.4 数据与隐私

控制	实现位置	说明
群消息采集	app-bot	群主显式开启才进入采集（隐私优先，默认关闭）
Bot 撤管理员	app-bot	自动关闭采集与监听，数据流即时切断
敏感字段	全栈	TG token、支付密钥、JWT secret 全部走环境变量，禁止入库、禁入仓
日志脱敏	tracing	默认 INFO 级，敏感字段（手机号、token、密钥）不落日志
备份加密	app-backup	PG / Manticore 备份落盘，路径权限受控

3.5 传输与网络安全

控制	实现位置	说明
公网 TLS	部署层	Nginx / Cloudflare 终止 TLS，强制 HTTPS
WebSocket	app-gateway	WSS 强制，禁 ws://
内部通信	服务间	内网回环 / 私网 IP，不暴露公网
tg-client	tg-client	仅监听 127.0.0.1:8188，外部一律经 app-admin 代理（管理员鉴权）
CORS	app-gateway	白名单域名，禁通配符 *

3.6 限流与防滥用

控制	实现位置	说明
登录限流	app-admin	失败次数 + IP 维度限流
搜索限流	app-api	用户 / IP 双维度
Bot 消息	app-bot	用户级速率限制，防刷
TG 风控	tg-client	进群 30-90 秒随机间隔 + 每日 50 上限 + 失败 24h 冷却
支付回调	app-pay-gateway	单 IP 频率限制

3.7 审计与可观测

控制	实现位置	说明
操作审计	app-admin	关键操作落审计表（管理员、商户审批、资金动作）

控制	实现位置	说明
日志规范	全栈	tracing 结构化日志，统一级别，关键链路限频
链路追踪	tracing	请求 ID 贯穿 gateway → 服务 → 数据层
异常告警	app-bot	关键失败（支付、授权、采集）触发告警通知

3.8 供应链与依赖

控制	实现位置	说明
Rust 依赖	Cargo.lock	锁定版本，构建可复现
构建环境	WSL / CI	统一构建机， SHA256 校验产物
支付插件	app-pay-gateway	.so 动态库按后台配置加载，来源受控
前端依赖	package-lock.json	锁定版本

3.9 运维与部署

控制	实现位置	说明
配置外置	全栈	.env 不入仓，启动时集中校验
服务隔离	部署层	微服务独立进程，单点崩溃不扩散
授权容灾	app-updater	宽限模式 ：授权服务抖动期间业务不中断，但拒绝新激活
启动自检	各服务	启动时校验必需环境变量，缺失即退出

四、已知风险与待办

本节为**当前自检**发现的风险面，按优先级排序。外部渗透测试报告到位后会补充 / 修正。

#	风险	影响面	当前缓解	待办
1	IPN 回调链路 对金额伪造极度敏感	资金	验签 + 幂等 + 金额匹配	外部专项测试
2	app-license 私钥 泄露会导致授权体系崩塌	授权	仅运营方部署、内网隔离	私钥硬件化 (HSM/KMS)
3	tg-client Session 文件被盗 → 真人号被劫持	TG 监听	仅本机回环 + 文件权限	定期轮换 + 异地备份加密
4	PostgreSQL 直连暴露 (运维期)	数据	内网 + 强口令	网络层 ACL 收紧
5	共享密钥 (registry HMAC) 泄露 → 服务伪造	内部	环境变量注入	引入 mTLS / 短期证书

#	风险	影响面	当前缓解	待办
6	Mini App initData 验签失败兜底逻辑	Mini App	强制 HTTPS + 数据库校验	移除环境变量兜底
7	备份文件未加密落盘	数据	路径权限	加密备份 + 异地存储
8	日志可能残留敏感字段	数据	脱敏规范	全量审计 + 自动扫描

五、白盒渗透测试

首轮授权渗透测试已于 2026-09-25 完成。本节合并《安全检测报告》与《安全问题报告》两份产物，**全程脱敏**：不披露任何域名、子域、IP 地址与授权服务器地址，资产一律以角色称呼。

5.1 测试概述

项目	内容
测试日期	2026-09-25
测试性质	已获目标方授权的白盒渗透测试（授权信息由授权服务器确认）
测试方式	被动信息收集（DNS 枚举、证书透明日志分析、HTTP 指纹识别、前端 JS 静态分析） + 主动验证（人工构造请求逐项验证，未使用商业化自动扫描器）
操作边界	全程只读探测与有限次登录尝试；未对生产数据做增删改、未进行拒绝服务类测试
测试工具	自研 Python 请求脚本、视觉模型 OCR（验证码识别验证）、DNS 查询工具、证书透明日志查询、浏览器开发工具

5.2 模拟攻击覆盖面（致谢）

感谢测试方在授权范围内对以下攻击面进行了系统的模拟攻击验证：

攻击面	模拟攻击手段
资产与暴露面	DNS 子域枚举、证书透明日志交叉验证、HTTP 技术栈指纹识别、前端 bundle 反解 API 路径
未授权访问	对候选内部接口（授权状态、健康检查、代理入口等）做未认证直连验证
SQL 注入	搜索接口多参数注入：单引号、布尔条件、UNION 注入、SLEEP 时间盲注
XSS	搜索结果输出点提交 script / img / svg 等 payload 验证输出编码
CSRF	登录表单 CSRF Token 与 Referer/Origin 同源校验检查
弱口令爆破	管理后台有限次弱口令尝试 + 验证码 OCR 自动化识别
SSRF	代理入口路径直连探测
注册流程	邮箱验证码绕过验证
配置基线	安全响应头、robots.txt 残留、验证码机制、API 响应结构

5.3 漏洞清单（是否存在 / 是否被攻破）

测试覆盖三类资产角色：**业务前台**（搜索门户）、**管理后台**（Admin）、**支付后台**（第三方 EPUSDT 支付管理端）。共确认 **9** 项安全问题：高危 1、中危 4、低危 4。

编号	漏洞名称	等级	位置（角色）	是否存在该问题	是否被攻破	是否成功获取权限
VUL-01	未授权访问泄露内部服务架构	低危	管理后台 授权状态接口	是	是——未认证即可获得 13+ 内部微服务清单、进程信息、授权白名单与授权服	否
VUL-02	健康检查接口泄露服务名称	低危	管理后台 healthz	是	是——未认证返回服务名与运行环境	否
VUL-03	全站安全响应头缺失 中危	中危	三站（前台/后台/支付）	是	是——CSP / X-Content-Type-Options / X-Frame-Options / HSTS / Referrer-Policy / Permissions-Policy 六项全缺失，后台无 CSP 兜底	否
VUL-04	登录表单无 CSRF 防护	中危	业务前台 登录页	是	是——表单无 CSRF Token、无同源校验（防护缺失）	否
VUL-05	搜索参数反射型 XSS 特征	中危	业务前台 搜索	是（特征存在）	否——payload 被 HTML 实体转义，未突破；但无 CSP 兜底，输出点变化即可可能升级	否
VUL-06	robots.txt 模板残留	低危	业务前台	是	是——残留模板占位 Sitemap 地址（信息泄露类，无利用概念）	否
VUL-07	验证码机制可自动化破解	低危	管理后台 登录验证码	是	是——4 位字母数字经图片增强 + OCR 多次识别成功，且无失败锁定与频率限制	否
VUL-08	搜索 API 泄露数据库字段结构	低危	业务前台 搜索接口	是	是——空参数即返回 12 条数据，字段命名暴露表结构设计	否
VUL-09	支付管理后台公网暴露	低危	支付后台	是	否——登录入口公网可达，但弱口令测试全部失败	否

5.4 已测试但未攻破的项（防线有效）

以下攻击面经主动验证**未发现可被利用的问题**，说明核心链路防线当前有效：

检测项	测试方法	是否存在该问题	是否被攻破
SQL 注入	搜索接口多参数：单引号 / 布尔 / UNION / SLEEP 时间盲注	否	否——无异常响应、无延迟，判定为参数化 SQL (\$3.2 sqlx 编译期校验一致)
XSS 输出编码	script / img / svg 等 payload	否（当前输出点）	否——全部被 HTML 实体转义

检测项	测试方法	是否存在该问题	是否被攻破
弱口令	多组常见弱口令 + 验证码 OCR 识别后提交	否	否——全部返回 invalid credentials
SSRF	代理入口直接路径访问	否	否——404，无可利用入口
注册绕过	邮箱验证码校验	否	否——email_code 无法绕过

5.5 处置优先级与修复追踪

优先级	编号	修复要点	状态
立即修复	VUL-01	授权状态接口强制 JWT + 角色鉴权；服务清单、PID、心跳、白名单等字段对外脱敏；授权服务器地址改服务	待修复
高优先级	VUL-03	网关层统一注入六项安全响应头；管理后台使用严格 CSP 作为 XSS 第二道防线	待修复
高优先级	VUL-07	提升验证码复杂度（干扰线/行为验证）+ 账号维度失败限制与递增延时；连续失败锁定告警；支付后台接入多因素认证	待修复
高优先级	VUL-09	支付后台限制运维来源 IP 或迁入内网/VPN，按需开放	待修复
常规	VUL-02	healthz 限内网/监控系统访问，响应移除 service / environment 字段	待修复
常规	VUL-04	登录及状态变更请求增加 CSRF Token；Cookie SameSite=Lax/Strict；服务端校验 Referer/Origin	待修复
常规	VUL-05	持续审计输出点上下文编码；XSS 用例纳入自动化回归	待修复
常规	VUL-06	清理 robots.txt 模板残留，排查同类配置残留	待修复
常规	VUL-08	搜索 API 响应字段最小化；空参数/异常参数限流与审计	待修复

管理侧建议（测试方附带）：建立资产台账与子域管理规范（避免泛解析掩盖真实资产）；内部接口与配置统一纳入访问控制与审计日志
2 周内安排复测。

复测计划 上述 9 项修复完成后将安排回归复测，复测结论与本表状态同步更新。

六、合规与法律

- 法律声明：见 法律声明，平台定位为搜索引擎与信息中介，用户生成内容（UGC）由用户负责。
- 数据保留：群消息采集遵循「群主显式开启」原则，撤管理员即停止；用户数据（钱包、订单）按业务需要保留，未设自动过期。
- 跨境：支付涉及多币种（含 USDT），运营方需自行评估当地合规要求。

评估口径：\$一 ~ \$四基于源码静态盘点，\$五为 2026-09-25 完成的首轮授权白盒渗透测试合并结果（已脱敏）；代码统计口径为 wc -l 物理行，含空行与注释，未剔除生成代码（若有）。本页作为安全总览持续更新，修复进展与复测结论将同步刷新 \$5.5。