



服务采购合同

项目名称：紫金山实验室 AI 赋能自动化渗透测试系统开发服务

甲方：紫金山实验室（采购人）

乙 方：南京联成科技发展股份有限公司（供应商）



根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律法规的规定，甲乙双方按照紫金山实验室的招标结果签订本合同。

第一条 合同标的

乙方根据甲方需求提供AI赋能自动化渗透测试系统开发服务：

1. 技术指标

1.1 系统总体要求

序号	功能指标	功能、性能、配置要求不低于以下要求
1	单机便携部署	系统须支持在虚拟机上完成全部安装、配置与运行，无需额外集群或云端依赖。操作系统支持 kali 系统，提供一键式安装脚本或向导。
2	核心任务类型	必须支持Web渗透与主机渗透两类核心任务，后续可通过模块化扩展其他类型。每种任务具备独立的配置界面和执行引擎。
3	总体态势展示	提供可视化仪表盘，集中汇聚展示：漏洞总数、高危漏洞数量、中危漏洞数量、正在进行任务数、已完成任务数、近 24 小时漏洞趋势曲线。支持按时间范围筛选。
4	活动概览呈现	首页显著位置展示近一周活动记录（时间、任务名称、状态）及最近任务列表（至少显示 4 条），点击可跳转至任务详情。卡片或时间轴样式呈现。

1.2 AI 渗透业务流程要求

序号	功能指标	功能、性能、配置要求不低于以下要求
1	任务生命周期管理	支持创建渗透任务（填写目标、类型、参数），删除任务（需二次确认），查看任务列表及详情。任务状态包括：等待中、执行中、已完成、失败。
2	多层次任务树生成	根据任务目标，利用大模型自动生成多层次的攻击任务树（任务→子任务→具体操作步骤），树状结构清晰展示父子依赖关系，每个节点包含描述、状态。
3	任务树动态更新	渗透执行过程中，系统根据实时结果（如端口开放情况、漏洞存在与否）自动裁剪、扩展或修改任务树节点。在对话中显示变更原因。前端需实时刷新显示树结构变化。
4	人工干预与附件上传	支持管理员在任务执行时终止任务，后续通过对话继续执行，或对某个子任务进行“跳过/强制重新执行”。允许上传任务附件（如自定义字典、特定漏洞利用脚本）作为任务输入。



5	漏洞验证与导出	当漏洞验证成功后，前端自动推送通知，展示漏洞详情（名称、CVE 编号、风险等级、漏洞描述、漏洞证明信息）。支持导出为 PDF 格式漏洞文件，包含完整复现步骤。
6	渗透报告生成与导出	任务结束后，自动生成结构化渗透报告，涵盖：概览、漏洞列表、攻击流程图、影响评估、修复建议。支持导出为 PDF 格式。
7	任务卡片化展示	任务列表以卡片形式展示，每张卡片直观显示：任务名称、目标、漏洞发现数量（高危/中危/低危）、运行进度百分比、运行状态（进度条），点击卡片进入详情。
8	执行过程实时推送	基于 WebSocket 或 Server-Sent Events 技术，将渗透执行过程日志、当前攻击步骤、漏洞产出信息实时推送到前端页面。

1.3 Web 渗透能力要求

序号	功能指标	功能、性能、配置要求不低于以下要求
1	基于 URL 创建任务	支持输入完整目标 URL（如 https://example.com）创建 Web 渗透任务，系统自动解析协议、域名、端口及路径。
2	渗透深度	提供配置选项： 测试深度：轻量扫描（仅基础指纹与常见漏洞）、标准扫描（含目录遍历、注入检测）、深度扫描（含复杂逻辑漏洞、认证绕过尝试）。

1.4 主机渗透能力要求

序号	功能指标	功能、性能、配置要求不低于以下要求
1	基于 IP 创建任务	支持输入目标 IP 地址创建主机渗透任务。系统自动进行主机存活探测和端口扫描。
2	操作系统	可手动指定目标操作系统类型（Windows/Linux）以提高效率； 测试深度：基础信息收集、漏洞扫描、弱口令爆破、本地提权模拟等递进层次。

1.5 模型管理要求

序号	功能指标	功能、性能、配置要求不低于以下要求
1	模型接入管理	支持对接多种大语言模型（添加的模型要兼容 Anthropic 接口）。提供界面进行模型的新增（配置 API 地址、密钥、模型名称）、删除、修改、查看。支持配置模型参数如温度、最大 Token 数。
2	默认模型切换	系统允许将任意已接入且测试通过的模型设为“默认模型”，后续创建任务默认使用该模型。



3	连通性测试	对于已配置的模型，提供“测试连接”按钮，系统发送测试请求，确保模型可用。测试失败须明确提示错误原因（如网络不可达、认证失败）。
---	-------	---

1.6 系统管理要求

序号	功能指标	功能、性能、配置要求不低于以下要求
1	系统基本设置	支持自定义系统名称（显示在标题栏）、上传系统 Logo（支持 png/jpg）。
2	用户认证与安全	内置用户管理：支持用户登录/登出，采用 JWT 或 Session 认证；用户可修改自己的登录密码（需验证旧密码）。
3	多语言界面	系统前端界面须支持中文、英文两种语言，提供切换按钮，语言包需完整覆盖所有菜单、提示、报告模板。默认语言可配置。
4	系统版本升级	支持离线升级方式。管理员可通过后台上传升级包，系统自动校验完整性、备份当前版本，然后执行升级。升级过程中应有进度提示，失败后支持回滚。

2. 其他技术要求

（1）性能要求：常规页面加载及交互响应时间不超过 2 秒；渗透任务执行过程中，系统内存占用稳定，不导致宿主机卡死。

（2）安全性：系统自身不得包含任何后门、恶意代码；通讯采用 TLS 加密；系统须能防御常见 Web 攻击（XSS、CSRF 等）。

（3）可靠性：系统应具备异常捕获与自动恢复能力，任务意外中断后支持断点续作。

（4）可扩展性：系统架构应支持后续扩展更多渗透类型（如移动应用、云环境）和 AI 模型。

乙方应按照投标文件中的承诺安排专人提供本合同项下的服务，未经委托人允许不得随意更换。

第二条 合同总价款



本合同项下服务总价款为人民币 捌万壹仟 元 (大写)(¥81000元), 除此之外, 甲方不再向乙方支付任何其他费用。

本合同总价款包含乙方提供服务发生的所有含税费用以及投标人认为需要的其他费用等。

本合同总价款还包含乙方应当提供的伴随服务/售后服务费用。

本合同执行期间合同总价款不变。

第三条 组成本合同的有关文件

下列关于紫金山实验室 JSZC-320100-JZCG-T2026-0180 号标的采购文件及有关附件是本合同不可分割的组成部分, 与本合同具有同等法律效力, 这些文件包括但不限于:

- (1) 乙方提供的响应文件和报价表 ;
- (2) 函件 ;
- (3) 分项报价表 ;
- (4) 项目实施方案与服务说明 ;
- (5) 偏离表及说明 ;
- (6) 服务承诺 ;
- (7) 中标通知书 ;
- (8) 甲乙双方商定的其他文件等。

第四条 保密及知识产权

1、双方均应该保护对方的知识产权, 未经对方同意, 任何一方均不得对对方的资料及文件擅自修改、复制或向第三方人转让或用于本合同以外的项目。如发生以上情况, 泄密方需向披露方承担一切由此引起的后果及赔偿责任。

2、如果乙方向甲方提供的服务或交付的工作成果涉及第三人知识产权等引发争议或诉讼, 由乙方承担一切法律责任、费用和后果。若甲方因此而遭致诉讼和损失, 则乙方还应赔偿甲方因此支出的律师费、鉴定费、交通费、诉讼费等一切合理开支和全部损失。

3、本项目开发产生的全部源代码、文档及技术成果, 其知识产权归采购人所有。供应商须保证代码无第三方知识产权风险。



4、源代码与知识产权：交付完整、无加密的源代码，代码规范清晰。供应商须协助采购人完成代码编译与独立部署验证，确保无隐藏依赖。

5、保密义务：供应商及项目参与人员须签署保密协议，对项目实施中获取的任何网络结构、系统信息、漏洞数据永久保密，不得留存或另作他用。

第五条 禁止贿赂条款

甲乙双方保证不向另一方及与本合作有关的任何第三方的工作人员直接或间接给予或收受任何可能影响公正执行公务的礼品、礼金、有价证券等财物，或接受、提供可能影响公正执行公务的宴请、旅游、健身、娱乐等活动安排。

如有一方违反本条规定，经核查清楚，守约方有权以书面形式通知违约方终止本合同，同时保留依法采取进一步法律措施的权利，违约方应承担由此造成的一切损失。

第六条 服务保障

1、乙方所提供的服务应与采购文件规定的要求及所附的偏离表相一致；若无特殊说明，按国家有关部门颁布的标准及规范为准。

2、乙方应保证服务完全符合合同规定的要求。

3、质保期：自最终验收合格之日起，提供不少于 1 年的免费软件质保与技术支持服务。质保期内任何软件缺陷、安全漏洞，乙方须在 48 小时内响应，5 个工作日内修复。

4、培训服务：提供至少 2 次现场或远程培训（管理员操作培训、使用人员培训），每次不少于 2 小时，并交付培训视频及教材。

第七条 交付和验收

1、乙方应当在合同签订后 60 天内交付软件开发服务。



2、采购内容与交付物清单

①AI赋能自动化渗透测试系统软件（完整安装包，支持单机便携部署）壹套。

②《软件使用说明书》（中文版，包含功能操作、配置说明、常见故障排除）纸质版2份及电子版。

③《系统部署与运维手册》（包含环境依赖、安装步骤、参数调优指南）电子版。

④《系统接口文档》（如涉及与其他系统对接，需提供详细API说明）。

⑤全部软件源代码（无加密、无混淆，含完整注释，可直接编译部署）。

⑥测试报告与验收材料（包括功能测试、性能测试记录）。

3、验收要求

在采购人指定环境中部署调试完毕，验收依据“技术需求”逐条功能测试，所有指标均满足后方可签署验收报告。

4、验收标准：

①文档齐全性验收：检查软件、源代码、使用说明书、部署手册、接口文档等交付物是否完整、版本一致。

②功能符合性验收：在采购人提供的测试环境中，依据技术要求逐条验证，所有功能须实现且无严重Bug。

③安全性审查：采购人有权委托第三方进行代码安全审计和渗透测试，若发现系统存在高危漏洞、后门或恶意代码，视为一票否决，供应商须承担相应责任。

④性能验收：在模拟负载下，验证响应时间、并发等非功能性指标满足要求。

⑤最终验收：全部验收通过后，双方签署《项目验收报告》。

第八条 合同款支付



1、本合同项下所有款项均以人民币支付。

2、付款方式：

合同签订后，甲方支付合同总价款的 30%作为预付款。

验收合格后，甲方支付合同总价款的 70%。

甲方开票信息：

单位名称：紫金山实验室

纳税人识别号：12320100MB19771475

开户银行：中国建设银行股份有限公司南京九龙湖支行

银行账号：32050159604400000585

联行号：105301001090

单位地址：南京市江宁区秣周东路 9 号

单位电话：025-52091570

乙方账户信息：

开户名：南京联成科技发展股份有限公司

开户行：中国银行南京南钢支行

账 号：475471175914

第九条 违约责任

1、甲方无正当理由拒收服务、拒付款的，甲方向乙方偿付合同总价的 5%违约金。

2、甲方未按合同规定的期限向乙方支付款项的，每逾期 1 天甲方向乙方偿付欠款总额的 5‰滞纳金，但累计滞纳金总额不超过欠款总额的 5%。

3、如乙方不能按合同约定提供服务、交付服务成果的，甲方有权要求乙方支付合同总价 5%的违约金。

4、乙方逾期提供服务、交付服务成果的，每逾期 1 天，乙方向甲方偿付合同总额的 5‰的滞纳金。如乙方逾期达 10 天，甲方有权解除合同，解



除合同的通知自到达乙方时生效，乙方应向甲方另行支付合同总价款 25% 违约金并赔偿给甲方造成全部损失。

5、乙方所提供的服务或交付的服务成果不符合合同规定的，甲方有权拒收。甲方拒收的，乙方应向甲方支付价款总额 5% 的违约金。甲方未拒收的，采购中心发现后将向有关部门反映，并责成乙方按照采购结果提供服务，同时视情况给予暂停一至三年参加南京市政府采购中心组织的政府采购活动的处理。

6、乙方在承担上述 4-5 款一项或多项违约责任后，仍应继续履行合同规定的义务（甲方解除合同的除外）。甲方未能及时追究乙方的任何一项违约责任并不表明甲方放弃追究乙方该项或其他违约责任。

7、乙方投标属虚假承诺，或经权威部门监测提供的服务不能满足采购文件要求，或是由于乙方的过错造成合同无法继续履行的，乙方应向甲方支付不少于合同总价 30% 赔偿金。

8、违约方须承担守约方因追索权利产生的一切费用（包括诉讼费、保全费、保全担保保险费、律师费、差旅费、公证费、鉴定费等）。

第十条 合同的变更和终止

1、除《政府采购法》第 49 条以及第 50 条第二款规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或终止合同。

2、除发生法律规定的不能预见、不能避免并不能克服的客观情况外，甲乙双方不得放弃或拒绝履行合同。乙方放弃或拒绝履行合同，在三年内不得参加南京市政府采购中心组织的政府采购活动。

第十一条 合同的转让

乙方不得部分或全部转让其应履行的合同义务或其享有的合同权利。

第十二条 争议的解决



1、因服务的质量问题发生争议的，一方可邀请国家认可的检测鉴定机构对服务质量进行鉴定。服务符合标准的，鉴定费由甲方承担；服务不符合标准的，鉴定费由乙方承担。

2、因履行本合同引起的或与本合同有关的争议，甲、乙双方应首先通过友好协商解决，如果协商不能解决争议，则向甲方所在地有管辖权的人民法院提起诉讼解决争议。

3、在诉讼期间，本合同应继续履行。

4、双方确认本合同载明的地址可作为合同履行过程中相关文书、法院送达诉讼文书的地址，因载明的地址有误或未及时告知变更后的地址，导致相关文书及诉讼文书没能实际被接收的、邮寄送达的，相关文书及诉讼文书退回之日即视为送达之日；因一方拒收的，相关文书及诉讼文书退回之日即视为送达之日。

第十三条 诚实信用

乙方应诚实信用，严格按照采购文件要求和投标承诺履行合同，不向甲方进行商业贿赂或者提供不正当利益。

第十四条 合同生效及其他

1、本合同自双方盖章之日起生效。

2、本合同一式伍份，甲方执肆份，乙方执壹份，招标公司执壹份，具有同等法律效力。

3、本合同应按照中华人民共和国大陆地区现行有效的法律进行解释。

(以下无正文)



(本页系编号

《服务采购合同》签署页，无正文)

甲 方：紫金山实验室 (盖章) 法人代表：尤肖虎 地 址：南京市江宁区秣周东路 9 号 邮 编： 电 话： 授权代表 (签字)  签订日期：2020 年 07 月 16 日	乙 方：南京联成科技发展股 份有限公司 (盖章) 法人代表：凌飞 地 址：南京市江北新区南京软 件园团结路 99 号孵鹰大厦 A 座 14F 邮 编：211899 电 话：15365130347 授权代表 (签字)： 签订日期：2020 年 7 月 20 日
--	--



