**采购需求**

一、测试目标

1.漏洞识别。识别源代码中存在的各类安全漏洞，包括但不限于缓冲区溢出、注入攻击、跨站请求伪造、认证与授权缺陷、敏感信息泄露等。发现可能导致系统被非法访问、数据泄露、服务中断等安全事件的代码缺陷。

2.合规性检查。验证源代码是否符合相关的安全标准和规范。检查代码是否遵循组织内部的安全开发生命周期要求和安全编码标准。

3.代码质量评估。评估代码中与安全相关的质量问题，如错误处理不当、日志记录不完整、异常处理机制不完善等。识别可能影响系统安全性的代码设计缺陷和实现问题。

4.风险评估。对发现的安全问题进行风险等级评估，确定其可能造成的影响范围和严重程度。提供针对性的修复建议和缓解措施，降低安全风险。

二、测试原则

1.全面性原则。审计范围应覆盖软件系统的所有关键模块和核心功能代码。综合采用自动化工具扫描与人工代码审查相结合的方式，确保审计的全面性。

2.客观性原则。基于明确的安全标准和规范进行审计，避免主观臆断。审计结果应可验证，发现的问题应具有明确的证据支持。

3.保密性原则。审计过程中接触到的源代码和相关信息属于敏感信息，应严格遵守保密规定。审计人员需签署保密协议，防止信息泄露。

4.最小影响原则。审计过程应尽量避免对软件系统的正常开发和运行造成影响。如需在测试环境中运行代码，应采取必要的隔离措施。

三、服务要求

1.审计团队要求：审计过程中源代码审计项目组应不少于5人，现场审计人员不得少于2人。供应商应确保人员稳定，如需更换人员，须经采购人同意。

2.审计环境要求：建立独立的审计环境，配置必要的审计工具和测试设备。 审计环境应具备与生产环境相似的配置，以确保审计结果的准确性。采取必要的安全措施保护审计环境，防止审计过程中引入新的安全风险。

3.报告要求：审计完成后应提供详细的审计报告，包括审计范围、方法、发现的问题、风险等级、修复建议等。报告应采用清晰、易懂的语言，避免使用过多的技术术语。对发现的问题进行分类整理，按风险等级排序，便于委托方优先处理高风险问题。

4.保密要求：供应商应签订保密协议，项目组所有人员均应签订保密承诺书，供应商及项目组人员应严格遵守保密要求，不得以任何方式向任何第三方泄漏在本项目中接触到的任何信息，包括但不限于被测单位信息、被测系统信息、系统源代码等。在源代码审计服务合同执行完毕后，供应商应立即将采购人提供的资料、信息、系统源代码等所有内容返还采购人，或按照采购人要求彻底销毁。

四、服务内容

1.身份认证与授权机制审计。检查用户身份认证机制的安全性，包括密码策略、多因素认证、会话管理等。评估授权机制的有效性，验证不同角色的权限分配是否合理，是否存在越权访问的可能。检查是否存在默认账号、弱口令等问题。

2.算法进行保护。评估数据传输过程中的安全性，检查是否使用了安全的传输协议。检查数据备份和恢复机制的安全性，确保备份数据的完整性和保密性。

3.输入验证与输出编码审计。检查对用户输入的验证机制，验证是否能有效防止注入攻击、跨站脚本等漏洞。评估输出数据的编码处理，确保在不同的上下文环境中正确编码。检查文件上传功能的安全性，验证是否对上传文件的类型、大小、内容等进行了有效验证。

4.错误处理与日志审计。检查错误处理机制，评估是否会泄露敏感信息（如堆栈跟踪、数据库路径等）。审计日志记录功能，验证是否记录了关键的安全事件（如登录失败、权限变更等）。检查日志的保护机制，确保日志不被篡改、删除，且只有授权人员可以访问。

5.安全配置审计。检查软件系统的安全配置，验证是否采用了安全的默认配置。评估配置文件的保护机制，确保配置信息（如数据库连接字符串、密钥等）不被未授权访问。检查是否存在不必要的服务、端口、模块等，减少攻击面。

五、交付成果

源代码安全审计报告（包含详细的漏洞描述、风险等级、修复建议等）。

六、本项目需要落实的政府采购政策：

1、中小企业发展政策：《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19号）《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）；《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）；《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）；《陕西省中小企业政府采购信用融资办法》（陕财办采〔2018〕23号）。

2、绿色发展政策：《国务院办公厅关于建立政府强制采购节能产品制度的通知》（国办发〔2007〕51号）；《关于印发环境标志产品政府采购品目清单的通知》（财库〔2019〕18号）《关于印发节能产品政府采购品目清单的通知》（财库〔2019〕19号）；《财政部、国家发展改革委、生态环境部、市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）；《商品包装政府采购需求标准（试行）》和《快递包装政府采购需求标准（试行）》（财办库〔2020〕123号）。

3、支持本国产业政策：《财政部关于印发<进口产品管理办法>的通知》（财库〔2007〕119号）；《财政部办公厅关于政府采购进口产品管理有关问题的通知》（财办库〔2008〕248号）。

4、支持创新等政府采购政策。