**采购内容**

**1、代码审计服务**

供应商应根据《OWASP安全编码规范快速参考指南》、《OWASP Code Review Guide》、《WEB应用安全编码规范》、《OWASP测试指南》、《医疗卫生健康行业规范》等标准规范，对我单位指定的1个应用系统进行代码审计，完成源代码安全审计工作后，供应商需在规定时间内提交《源代码安全审计报告》，报告应包括风险等级、漏洞文件、漏洞描述、代码片段、修复建议等维度内容。供应商应协助我单位进行漏洞修复，并再次进行系统复测，提交《源代码安全审计复测报告》。审计内容包括但不限于如下：

|  |  |  |
| --- | --- | --- |
| **分类** | **测试项目** | **项目说明** |
| **输入验证** | 用户数据验证 | 检查用户提交给应用程序的数据是否经过了校验，校验规则是否完善，对非法字符是否进行了阻断，检查是否存在注入、跨站等漏洞 |
| 接口数据验证 | 检查外部接口传输给应用程序的数据是否经过了校验，校验规则是否完善，对非法字符是否进行了阻断 |
| 数据库访问安全 | 检查进入数据库语句的变量是否经过了合法性验证，是否使用了安全的数据库访问方法，是否可能导致SQL注入等漏洞 |
| 文件操作安全 | 检查应用程序调用系统文件的过程是否安全，文件名、文件路径等变量是否经过了合法性校验，是否可能导致文件上传等漏洞 |
| 命令操作安全 | 检查应用程序调用系统命令的过程是否安全，进入命令的参数的变量是否经过了合法性校验，是否可能导致命令执行等漏洞 |
| **身份认证** | 用户登录逻辑 | 检查应用程序中用户登录的逻辑是否合理，用户能否通过特定的方法绕过身份认证 |
| 用户枚举 | 检查登录时是否可以枚举系统中存在的账号 |
| 暴力破解 | 检查是否可以暴力破解系统中的账号 |
| 用户密码策略 | 检查应用程序中用户注册、密码修改等页面中，是否包含密码复杂度检查模块，对用户要设置的密码进行了复杂度验证（密码中至少包含数字、字母和特殊字符，密码长度不小于6位字符），如果不符合密码复杂度要求，禁止提交 |
| 图形验证码 | 检查应用程序中用户注册、用户登录等页面中，是否存在图形验证码，图形验证码处理机制是否合理 |
| 注销测试 | 检查注销后，session是否销毁 |
| **授权测试** | 越权访问 | 检查是否存在水平越权和垂直越权 |
| 路径遍历 | 检查是否存在路径遍历漏洞 |
| 业务逻辑 | 检查业务逻辑是否存在漏洞 |
| **错误处理** | 敏感信息泄漏 | 检查应用程序和用户交互过程中，返回的提示中是否会泄漏敏感信息 |
| 应用异常处理 | 检查应用程序是否自定义错误信息，在应用服务异常导致错误发生时，是否能够跳转到错误信息页面，防止错误信息中包含服务器版本信息、应用程序路径等敏感信息 |
| **会话测试** | 会话泄露 | 检查是否存在会话泄露漏洞 |
| **加密测试** | 敏感信息加密存储 | 检查应用程序中的敏感信息，例如：用户密码，是否以明文方式存放在数据库或者文件系统中 |
| 加密算法 | 检查加密算法是否存缺陷，是否可逆等 |
| **日志记录** | 关键操作日志 | 检查应用程序是否对用户操作进行日志记录，至少应包含：记录时间、模块信息、操作信息、操作结果 |
| **其他** | 其他 | 检查是否存在框架等其他漏洞 |

**2、渗透测试服务**

供应商应通过模拟黑客攻击的方式，对我单位指定的1个业务系统进行一次渗透测试，针对渗透测试中发现的问题形成《系统渗透测试报告》。对渗透测试结果提出修复意见，协助我单位和系统开发单位进行整改，在实施完针对性的优化加固服务之后，还需要再验证业务系统加固和优化服务后的有效性，并提供《系统渗透测试复测报告》。渗透测试包含但不限于如下：

|  |  |  |
| --- | --- | --- |
| 分类 | 测试项目 | 项目说明 |
| 配置管理 | 应用管理界面 | 检查是否对外开放了应用管理界面 |
| HTTP方法 | 检查是否开放了不安全的HTTP方法 |
| 测试、备份文件 | 检查是否存在测试、备份文件 |
| 认证测试 | 认证绕过 | 检查是否可以绕过认证模式 |
| 用户枚举 | 检查登录时是否可以枚举系统中存在的账号 |
| 暴力破解 | 检查是否可以暴力破解系统中的账号 |
| 竞争条件 | 检查是否存在多线程竞争条件漏洞 |
| 图形验证码 | 检查图形验证码是否可以绕过 |
| 密码管理 | 检查密码相关点是否存在漏洞 |
| 注销测试 | 检查注销后，session是否销毁 |
| 授权测试 | 越权访问 | 检查是否存在水平越权和垂直越权 |
| 路径遍历 | 检查是否存在路径遍历漏洞 |
| 业务逻辑 | 检查业务逻辑是否存在漏洞 |
| 数据验证 | SQL注入 | 检查是否存在SQL注入漏洞 |
| 跨站脚本 | 检查是否存在XSS漏洞 |
| 命令执行 | 检查是否存在命令执行漏洞 |
| 代码注入 | 检查是否存在代码注入漏洞 |
| 文件上传 | 检查是否存在文件上传漏洞 |
| URL跳转 | 检查是否存在URL跳转漏洞 |
| 其他注入 | 检查是否存在XPATH注入、XML注入等漏洞 |
| 会话测试 | Cookie安全 | 检查cookie的属性 |
| 会话泄露 | 检查是否存在会话泄露漏洞 |
| 其他 | 其他 | 检查是否存在框架等其他漏洞 |

评分内容

|  |  |  |
| --- | --- | --- |
| **条款号** | **评审因素** | **评审标准** |
| （90分） | 供应商资质（16分） | 1.具有质量管理体系、环境管理体系、职业健康安全管理体系认证证书，得2分。2.具有信息安全管理体系认证证书，得2分。3.具有信息技术服务管理体系认证证书，得2分。4.具有信息安全服务资质认证证书-信息安全风险评估三级及以上资质，得2分。5.具有信息安全服务资质认证证书-信息系统安全运维三级及以上资质，得2分。6.具有信息安全服务资质认证证书-软件安全开发三级及以上资质，得2分。7.具有信息安全服务资质认证证书-信息系统灾难备份与恢复服务三级及以上资质，得2分。8.具有商品售后服务评价体系认证证书，得2分。**注：响应文件中提供上述证书扫描件及全国认证认可信息公共服务平台网站有效期内信息查询截图并加盖供应商公章，未提供的不得分。** |
| 服务方案（10分） | 根据响应文件中提供的服务方案是否具有合理性、服务流程是否清晰可执行、服务措施是否具体、应急方案是否可操作等由评委进行综合评审：1、服务方案合理完全满足项目要求，服务流程清晰、服务措施具体、应急方案具有可操作性的得10分；2、服务方案合理完全满足项目要求，服务流程较清晰、服务措施具体、应急方案可操作性较强的得8分；3、服务方案较合理并满足项目要求、服务流程较清晰、服务措施具体、应急方案基本可操作的得6分；4、服务方案基本合理并满足项目要求、服务流程基本清晰、有服务措施、有应急方案基本可操作的得4分；5、服务方案较差或未提供不得分。 |
| 人员实力（24分） | 1、供应商拟为本项目配备的项目负责人（1人）：（1）具有信息系统项目管理师认证证书；（2）具有系统规划与管理师认证证书；（3）具有中国网络安全审查技术与认证中心颁发的CISAW证书风险管理专业级认证证书；注：提供不全或未提供不得分，全部提供得12分。2、供应商拟为本项目配备的技术负责人（1人）：（1）具有信息系统项目管理师认证证书；（2）具有网络规划设计师认证证书；（3）具有CISP注册信息安全专业人员认证证书；注：提供不全或未提供不得分，全部提供得12分。**注：人员不得兼任；响应文件中同时提供以下证明材料：****（1）人员名单（格式自拟）；****（2）上述人员有效期内证书扫描件；****（3）供应商为上述人员缴纳的近3个月内（任意一个月）社保证明材料扫描件。** |
| 服务团队资质（26分） | 供应商拟为本项目配备的安全服务团队人员（除项目负责人和技术负责人外）：（1）团队人员具有中国网络安全审查技术与认证中心颁发的CISAW证书（安全集成、安全运维、应急服务、安全软件方向专业级及以上）每个得2分，最多得8分；（2）团队人员具有信息系统项目管理师、信息安全工程师、系统架构设计师、数据库系统工程师认证证书，每个得2分，最多得8分；（3）团队人员具有注册渗透测试工程师（CISP-PTE）、注册数据安全治理专业人员（CISP-DSG）、注册应急响应专家（CISP-IRS）认证证书，每个得2分，最多得6分；（4）团队人员具有CCSC网络安全能力认证数据安全方向、网络安全技术方向认证证书，每个得2分，最多得4分。**注：证书重复按单个得分计算，人员不得兼任；同一人员具有多个证书不累计计分，投标文件中同时提供以下证明材料：****（1）人员名单（格式自拟）；****（2）上述人员有效期内证书扫描件；****（3）供应商为上述人员缴纳的近3个月内（任意一个月）社保证明材料扫描件。** |
| 业绩案例（14分） | 1、供应商具有医疗卫生行业网络安全运维或服务业绩，每具有一个业绩得3分，最多得6分；不提供的不得分。2、供应商具有省委网信办、省通管局主管部门安全服务合同案例的;每提供一个，得4分；未提供，不得分；最多得8分。**注：1、以合同签订时间为准；****2、上述要求业绩可为已完成或正在履约项目业绩；****3、投标文件中须提供业绩合同扫描件或影印件，如合同中无法体现签订时间、金额、服务内容等主要评审因素的不得分。** |
| 投标报价得分计算 | 投标报价得分（10分） | 满足招标文件要求且投标报价在有效范围内所有有效供应商的投标报价为有效报价，评分基准价取所有有效报价的算术平均值，满分10分。 |
| 偏差率=（供应商评审价格−评审基准价）/评审基准价×100%所有有效报价与评分基准价作比较，与评分基准价一致不扣分，每高于评分基准价1%的扣0.3分，每低于评分基准价1%扣0.25分；（不足1%采用插入法计；保留小数点后两位，第三位小数四舍五入）。 |