# 安全漏洞扫描系统项目参数

## 一、项目概述

本项目旨在构建符合网络安全规范、具备全面漏洞检测能力的医院安全漏洞扫描系统，通过核心扫描技术实现对医院网络资产、应用程序、代码及口令的全方位风险检测，建立风险告警与闭环处理机制，保障用户网络环境的安全性、稳定性与合规性；同时提供标准化硬件配置与全周期技术服务，确保系统高效部署、稳定运行，并满足医院对漏洞管理、风险管控及安全审计的长期需求，最终实现网络安全风险的可检测、可追溯、可处置。

## 二、技术参数

## （一）漏洞扫描核心功能系统

### ★1.1 漏洞检测能力

1.1.1 支持检测的漏洞数大于 370000 条，兼容 CVE、CNCVE、CNNVD、CNVD 等主流漏洞标准；

1.1.2 需提供 CVE Compatible 证书及证明截图，确保漏洞检测标准的合规性与权威性。

### ★1.2 代码审计扩展模块

1.2.1 支持扩展代码审计功能，可对 C/C++、Python、Java、Php、Go 等主流编程语言进行代码解析；

1.2.2 具备语言词法、语法分析能力，内置标准化缺陷模板与缺陷检测规则；

1.2.3 支持用户自定义缺陷规则，满足个性化代码安全检测需求；

1.2.4 需提供代码审计模块功能截图，证明功能落地性。

### ★1.3 口令猜测扫描模块

1.3.1 具备单独口令猜测扫描任务创建功能，支持多协议口令猜测，涵盖 SMB、RDP、SSH、Telnet、SQL SERVER、MySQL、Oracle、Sybase、DB2、MongoDB、Memcached、Redis、PostgreSQL、HighGo、UXDB、Kingbase、STDB、FTP、SFTP、ActiveMQ、POP3、Tomcat、SMTP、IMAP、Onvif、RTSP、SNMP、SIP、Vmware ESXi、HTTP Digest、Weblogic、Elasticsearch、Websphere 等；

1.3.2 允许外挂用户自定义用户名字典、密码字典及用户名密码组合字典，提升口令猜测灵活性；

1.3.3 需提供口令猜测扫描功能截图，展示协议支持与字典配置界面。

### ★1.4 系统性能参数

1.4.1 支持最大并发主机数≥60 台，确保大规模网络资产同时扫描的效率；

1.4.2 支持最大并发任务数≥10 个，可同时处理多维度漏洞扫描需求。

### ★1.5 软件授权管理

1.5.1 包含 Web 应用扫描模块授权（数量 1 套）：对 Web 应用提供专业漏洞检测、挂马检测与深度分析功能；

1.5.2 包含云大物扫描模块授权（数量 1 套）：对云计算平台、大数据组件、物联网设备提供针对性漏洞检测与分析功能；

1.5.3 包含云平台环境虚拟镜像：默认支持 4 个虚拟 CPU，适配主流虚拟化平台（如 VMware、Hyper-V 等）部署；

1.5.4 包含 IP 点授权（数量 1 套）：授权可扫描的 IP 地址或域名总数量≥1000 个。

### ★1.6 风险告警与闭环管理

1.6.1 支持风险告警配置：可在集中告警平台灵活设置告警内容（如漏洞等级、影响范围）、告警方式（邮件告警、页面弹窗告警）、告警资产范围（指定 IP 段或设备）；

1.6.2 支持风险闭环处理：可单个或批量修改风险状态（如待处理、处理中、已解决、误报），并记录处理日志（处理人、处理时间、处理方案）；

1.6.3 支持风险处理进度跟踪，确保漏洞风险可追溯、可管控。

### 1.7 风险值自定义配置

1.7.1 支持主机风险等级评定标准自定义：用户可根据业务重要性调整主机漏洞的风险权重（如高危漏洞、中危漏洞的分值占比）；

1.7.2 支持网络风险等级评定标准自定义：可基于网络拓扑、业务类型配置网络层面漏洞的风险计算规则，适配不同场景的风险管控需求。

### 1.8 报表自定义功能

1.8.1 支持报表个性化定制：可自定义报表标题、封面 LOGO、页眉（如单位名称、报表类型）、页脚（如生成时间、报表编号）；

1.8.2 支持报表章节内容配置：可选择是否显示漏洞详情、风险统计、处理进度、资产分布等章节，满足不同场景下的报表输出需求（如审计报表、运维报表）。

### 1.9 产品市场成熟度要求

1.9.1 产品需为国内市场广泛应用的成熟产品，近三年在网络安全漏洞扫描领域的市场占有率排名不低于前 3 名；

1.9.2 需提供知名第三方机构（如 IDC）出具的市场占有率排名有效证明材料（复印件加盖供应商公章）。

## （二）硬件配置要求

### 2.1 配套笔记本电脑配置

2.1.1 CPU：≥酷睿 Ultra 5 125H，确保系统运行与漏洞扫描的计算性能；

2.1.2 内存：≥16G，满足大规模漏洞扫描任务的内存需求；

2.1.3 硬盘：≥512G 固态硬盘，保障系统启动、扫描数据存储与读取的效率。

## 三、商务要求

**★(一)软件产品从激活之日起提供前三年服务包（数量 1 套），包含以下服务：**

3.1 产品系统升级授权：免费获取系统功能迭代与版本更新服务；

3.2 远程支持服务：提供 7×24 小时远程技术支持（含漏洞咨询、故障排查）；

3.3 Web 漏洞扫描模块升级授权：提供 2 套 / 年的 Web 漏洞库升级服务，确保 Web 漏洞检测的时效性；

3.4 系统漏洞扫描模块升级授权：提供 2 套 / 年的系统漏洞库升级服务，覆盖最新系统漏洞类型。

**（二）部署与培训：**

供应商需负责产品的全流程部署安装服务（含系统环境配置、授权激活、扫描任务测试）；同时提供免费的产品操作培训服务，确保用户运维人员掌握核心功能（如漏洞扫描、风险处理、报表生成）。

**（三）技术文档交付**

项目验收时，服务商应提交《系统测试计划及测试报告》、《系统部署安装操作说明书》、《用户操作手册》、《功能规格说明书》、《系统设计说明书》、《数据库设计说明》、《用户使用报告》等技术文档材料。

## 项目管理与团队要求

**（一）项目管理方案**

服务商需提供详尽项目管理方案，涵盖实施进度表、项目组织结构、项目质量控制等内容，确保项目按计划有序推进，各环节质量达标，满足医院信息化建设标准。

**（二）项目团队组成**

1. **项目工作组成立**：为了保证本项目成功实施，应成立针对本项目的项目工作组，以配合院方相关部门及人员进行系统的运行维护和平台、业务的应用推广。在项目实施期内，保持项目团队稳定，未经院方同意，项目组人员不得变更。项目实施人员需严格遵守医院的有关管理制度。
2. **成员组成及资质要求**

**实施工程师 ：**至少配备 1 名具备丰富同类项目管理经验的实施工程师，且需获得我院认可，保证项目实施的专业性和针对性。

**项目开发人员 ：**开发团队成员均需具备同类项目实施经验，能熟练运用相关技术解决项目中遇到的问题，保障系统开发质量。

**3.项目交付期**

项目实施工期为90天。服务商应确保签订合同后完成系统部署及多轮测试优化等全部上线前必备工作内容。上线后进入90天系统试运行阶段，服务商需对试运行期间出现的各类功能缺陷、性能瓶颈及用户反馈问题进行实时监测与快速修复。

**（三）项目验收**

**1.验收组织** ：实施完毕后，由我院信息网络中心牵头组织验收工作，全面检查系统功能、性能、文档等是否符合要求。

**2.验收依据** ：采购文件条款、软件使用说明及国家有关的检验标准均为验收的依据。

**3.验收程序** ：验收时服务商必须派代表在场,功能确认无误后，由双方签署验收报告。

## 售后服务要求

**（一）技术服务支持**

1. **服务方式**

提供7×24 小时技术支持（含日常检查、故障恢复、预防性维护、性能优化），相关费用由服务商全额承担，工程师直接与需求方沟通解决问题；

热线无法解决时，及时派工程师现场支持，服务经需求方确认后方可离场，现场故障处理参照紧急故障标准；

需求方遇主机、存储、数据库、中间件相关且难定位的故障，或系统性能影响正常使用时，服务商工程师需按合理安排到场，配合定位故障、优化调整。

**2.质保期**

项目免费质保3年（自验收之日起算），质保期内按用户需求完善软件功能。

**（二）系统维护与升级**

**1. 定期巡检**

保修期内每季度开展 1 次巡检，制定含目标、项目、操作方式的巡检计划，完成后提交巡检报告（含过程记录、分析及预防性建议）。

**2.系统升级**

质保期内免费提供软件升级（含补丁安装、版本升级），需结合原厂商发布情况及需求方系统运行状态提升级建议，负责提供介质与许可证、实施升级、配合测试，并制定升级方案、操作流程及回退方案，保障关键业务不受影响，最终提交升级实施报告与测试报告。

**3.系统调整支持**

需求方进行硬件搬迁、应用升级 / 割接等系统调整时，服务商工程师需按要求准时到场，配合完成系统启停、故障排除，协助需求方及其他厂商分析系统运行情况，保障稳定。

1. 培训要求
2. 服务商需结合所供系统功能及需求方现有管理人员水平，制定详细业务培训方案，确保管理人员能独立管理系统主要功能及开展日常维护。
3. 免费提供原厂正规培训及相关资料，投标书中需明确培训课程、人员数量、培训时间，该指标纳入技术服务评价。
4. 项目实施期间及系统运行后，结合项目与产品情况，不定期与需求方开展技术交流、提供培训。

七、其他要求

**（一）数据安全与保密**

服务商需采取严格的数据安全措施，确保医院数据在传输、存储、使用等环节的安全，防止数据泄露、篡改等安全事件发生。同时，对在项目实施及服务过程中获取的医院敏感信息负有保密义务，未经医院书面同意，不得向任何第三方披露或使用。

**（二）网络安全自查**

服务期内，服务商需积极配合我院定期开展网络安全自查工作，自查内容至少包括系统日常运行情况、系统漏洞等，及时发现并处理安全隐患，保障医院信息系统的安全性。

**（三）安全审计配合**

配合我院定期进行安全审计工作，审计内容至少涵盖系统账号、权限、操作行为和安全技术措施有效性等方面，确保系统运行符合安全规范，及时整改审计发现的问题。

**（四）数据资源共享**

1. 服务商须严格履行数据资源共享义务，积极配合完成与上级主管部门指定系统平台的数据接口对接及系统平台互联互通工作，打破信息孤岛，实现数据共享共用，提升医疗信息化水平。
2. 在技术对接过程中，不得附加任何形式的接口调用费用条款，杜绝因接口对接费用等争议影响跨层级、跨部门政务数据资源共享与业务协同工作，保障数据共享工作的顺利推进。

**（五）知识产权合法**

服务商须确保所提供的系统、软件及技术未侵犯任何第三方知识产权。若所供系统涉及第三方软件使用，服务商应保证该软件为正版且具备合法授权。如因服务商过错致使医院在使用过程中面临第三方知识产权侵权指控，服务商将承担全部法律责任及经济赔偿，并需积极采取措施以消除负面影响，确保医院的正常运营与声誉不受损。

**（六）永久使用权**

医院将拥有该系统的永久使用权，有权自主决定系统的安装、运行、管理及升级等事宜，确保医院能够长期、持续、稳定地使用系统开展业务活动，不受时间限制。

**（七）技术支持和服务**

服务商应提供必要的技术支持和服务，并支持医院对系统进行统一版本的升级与改造及使用科室变更，确保医院能够根据自身发展需求。