**附件1**

**等保测评服务技术规格说明书**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | | **指标要求** |
|  | 遵循的法规 | | 等保测评遵循以下法律、法规：   1. 《中华人民共和国网络安全法》； 2. 《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）； 3. 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）； 4. 《关于印发<关于信息安全等级保护工作的实施意见>的通知》（公通字[2004]66号文）； 5. 《关于印发<信息安全等级保护管理办法>的通知》（公通字[2007]43号文）； 6. 《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号文）； 7. 《广东省深化信息安全等级保护工作方案》(粤公通字[2010]45号)； 8. 卫生部关于印发《卫生行业信息安全等级保护工作的指导意见》的通知（卫办发〔2011〕85号）。 |
|  | 遵循的技术标准和规范 | | 等保测评遵循以下技术标准和规范：   1. 《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）； 2. 《信息系统安全等级保护定级指南》（GB T 22240-2008） 3. 《信息安全技术 信息系统安全等级保护测评过程指南》； 4. 《信息安全技术 信息系统安全等级保护实施指南》； 5. 《信息安全技术 信息系统安全等级保护测评要求》； 6. 《信息安全技术 信息系统安全等级保护安全设计技术要求》（信安秘字[2009]059号）； 7. 《信息安全技术 网络基础安全技术要求》（GB/T20270-2006）； 8. 《信息安全技术 操作系统安全技术要求》（GB/T20272-2006）； 9. 《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2006）； 10. 《信息安全技术 服务器技术要求》（GB/T21028-2007）； 11. 《信息安全技术 终端计算机系统安全等级技术要求》（GA/T671-2006）； |
|  | 评估范围 | | 本次测评包括以下信息系统：   1. HIS系统 三级 2. LIS系统 二级 3. PACS系统 二级 4. OA系统 二级 5. 门户网站系统 二级 |
|  | 差距评估要求 | | 以等级保护的法规、技术标准、技术规范为依据，中标人对以上5个信息系统在物理安全、主机安全、应用安全、网络安全、数据安全及备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理方面进行测评，发现安全保护现状，并为确立安全策略、制定安全规划、开展安全建设提供决策建议。 |
|  | 差距评估服务 | | 安全评估服务  根据南方医科大学第五附属医院的信息系统的划分情况、定级情况和承载业务情况，分析明确信息系统安全需求，采用设计合理的、满足等级保护要求的总体安全方案，制定安全实施计划，用以指导信息系统安全建设工程实施。同时，将采取包括现场观察、询问人员、查询资料、检查记录、检查配置、技术测试等有效措施和必要的漏洞扫描和配置审查等工具，对可能存在的信息安全风险进行识别分析，对信息系统的安全保护现状与等级保护要求之间的差距进行评估。 |
|  |
|  | 安全保障体系设计服务  根据等级保护差距评估报告与评估结果，针对存在的安全隐患以及未落实的安全措施制订安全整改方案，明确整改的目标、项目和进度，拟定信息安全保障标准与规范。  （1）提出符合等级保护《基本办法》要求的安全专用产品，完成相应安全域的划分及拓扑设计。  （2）协助落实安全技术措施，提供统一的信息安全规范与标准。 |
|  | 系统渗透测试服务 | | 站在实战角度对系统进行的安全评估，可以让相关人员直观的了解到网络、系统、应用中隐含的漏洞和危害发生时可能导致的损失。检查包括：SQL注入、跨站脚本、WEB目录泄露、机密信息泄露等。 |
|  | 测评工作实施内容完整性要求 | | 测评内容应至少包括：   1. 安全技术测评，主要包括：物理安全技术测评、网络安全技术测评、主机安全技术测评、应用安全技术测评、数据安全与备份恢复技术测评等五个层面上的测评； 2. 安全管理测评，主要包括：安全管理制度测评、安全管理机构测评、人员安全管理测评、系统建设管理测评、系统运维管理测评等五个层面上的测评； 3. 系统整体测评，主要包括：安全控制间安全测评、层面间安全测评、区域间安全测评、系统结构安全测评等四个层面上的测评。 |
|  | 安全评估系统(安全脆弱性扫描)工具指标要求 | 支持的WEB服务器 | 如：IIS、Websphere、Weblogic、Apache等； |
|  | 支持的数据库类型 | 如：Access，Mysql,ORACLE,DB2,PostgreSQL,Sybase,Informix,sqlite  MSSQLSERVER等 |
|  | HTTP参数 | 能够检测GET、POST、User-Agent、Cookie等多种方式提交的HTTP请求参数，并进行相应检测。 |
|  | 支持的第三方组件 | Discuz、大汉CMS、PHPCMS、DEDECMS、ECSHOP、WordPress、eWebEditor、FCKeditor、Struts2等国内外常见第三方组件 |
|  | 网页木马 | 支持对各种挂马方式的网页木马进行全自动、高性能、智能化分析，并对网页木马传播的病毒类型做出准确剖析和网页木马宿主做出精确定位。 |
|  | 脚本木马 | 支持指纹识别和暴力猜解定位出是否存在脚本木马（WebShell） |
|  | 暗链 | 是否支持扫描各种隐藏连接的暗链，并且定位到哪个页面被挂暗链 |
|  | WEB漏洞扫描 | 支持常见的WEB应用弱点检测，支持OWASP TOP 10等主流安全漏洞，如：SQL注入、Cookie注入、Base64注入、XSS跨站脚本、框架注入、链接注入、隐藏字段、CSRF跨站伪造请求、命令注入、命令执行、代码注入、遍历目录、弱口令、表单绕过、文件包含、管理后台、敏感信息泄漏、第三方组件、其他各类CGI漏洞等各种类型。 |
|  | 策略分类 | 是否支持将漏洞以紧急、高危、中危、低危、信息进行危害程度的分类，并且可根据用户需要自定义漏洞等级 |
|  | 策略自定义 | ▲支持根据自行需要以插件形式自定义添加策略提高扫描结果，以满足更高级用户的需求。 |
|  | 扫描功能 | 支持主动扫描、被动扫描两种模式的深度扫描；支持多域名批量扫描；  支持多任务并发扫描：单个程序可执行多个扫描任务同时并发扫描；  支持定制扫描：用户可根据目标扫描网站的特点以及所在网络环境，对扫描过程进行定制，如爬行、检测、过滤、网络环境等；  支持WEB2.0扫描：采用自主研发的网页执行模块，执行网页中的JavaScript脚本获取其中的链接，也可通过正则表达式匹配页面中的链接； |
|  | 渗透测试 | 通过所发现的应用漏洞，模拟黑客使用的漏洞攻击手段，对目标应用进行深入安全分析，利用沙盒技术实施无害攻击，包括后台数据库中的数据提取、执行控制台命令、获取注册表数据、获取目录树、数据库操作、备份数据库、远程文件下载、文件上传等，取得系统安全威胁的直接证据； |
|  | 逻辑漏洞检测 | 提供逻辑漏洞检测，能够对数据包进行拦截、重放，可以对历史数据进行重放测试 |
|  | 漏洞分析 | 提供直观的风险危害等级图表和风险类型统计图表、漏洞的描述、漏洞的风险级别、加固建议 |
|  | 趋势分析 | 可根据对网站的多次扫描提供横纵向的趋势分析报告 |
|  | 输出格式 | PDF、WORD、XLS、XML等 |
|  | 报告导出 | 单任务多网站可批量导出单个网站报告 |
|  | 品牌要求 | 产品应通过国家信息安全测评信息技术产品安全测评证书EAL3+级别 |
|  | 品牌要求 | 产品厂家应为《信息安全技术 Web应用安全扫描产品安全技术要求》标准起草单位之一 |
|  | 品牌要求 | 厂商具备国家级网络安全应急服务支撑单位 |
|  | 项目实施基本要求 | | 测评服务机构必须具备独立完成本项目的能力；  测评服务机构应对了解到的信息保密，并提供保密承诺。  测评服务机构必须为本项目成立等级保护测评小组，安排包括项目经理和核心技术人员。  测评服务机构必须按照等级保护的标准要求展开，并最终达到市公安网监等级保护的相关要求。 |