**包11采购需求**

## （一）项目概况

对“海南智慧健康岛建设工程项目”包1至包6的相关软件系统进行网络安全服务，确保信息系统能抵御漏洞和攻击，保障其安全稳定运行。

## **（二）技术商务要求**

根据《关于进一步加强信息安全等级保护工作的通知》（琼等保办〔2013〕2号），本着实际安全保障需要和本项目现有安全防护手段，本项目需根据《海南省政务信息化项目建设管理实施细则（暂行）》要求，开展渗透测试服务和代码审计服务。

### （1）技术要求

##### 1.1服务范围

对海南智慧健康岛建设工程项目开展渗透测试服务和代码审计服务。海南智慧健康岛建设工程项目具体功能清单详见包1至包6采购需求。

##### 1.2服务内容

###### 1.2.1渗透测试

1、渗透测试服务。通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全状况。具体包括对系统的任何弱点、技术缺陷或漏洞的主动分析，从一个攻击者可能存在的位置来进行，从这个位置有条件主动利用安全漏洞，计划为每季度1次。

2、漏洞扫描及管理服务。漏洞扫描及管理服务；对目前现有服务器、信息系统、终端漏洞扫描；对外服务的网站和应用做常规的漏洞扫描；针对业务系统情况从网络层、主机层、应用层三个层面进行安全防护，计划为每季度1次。

3、全服务成果：完成渗透测试工作后，出具《渗透测试报告》，并提出具有针对性的安全加固建议。

###### 1.2.2代码审计服务

**1.2.2.1服务内容**

为降低代码缺陷所带来的安全风险，按照《信息安全技术代码安全审计规范》（GB/T39412—2020），针对本项目涉及的系统源代码进行审计分析，审计开发语言包括但不限于：Java、PHP、Python、C#等，发现源代码层面的安全缺陷，并提供源代码审计报告和改进建议。

代码审计服务的范围为本项目涉及的所有系统源代码，包括使用 ASP、ASP.NET（VB/C#）、JSP（JAVA）、Python、PHP 等主流语言开发的 B/S 应用系统、使用 C++、JAVA、C#、VB 等主流语言开发的 C/S 应用系统，以及使用 XML 语言编写的文件、SQL 语言和数据库存储过程等。

代码审计是由具备丰富编码经验并对安全编码原则及应用安全具有深刻理解的安全服务人员，尤其是具有相关类似软件开发及设计经验的设计开发人员，对系统的源代码和软件架构的安全性、可靠性进行全面的安全检查，同时指导开发人员正确修复程序缺陷。

代码审计服务的目的在于充分挖掘和暴露系统的弱点，从而让管理人员了解其系统所面临的威胁。信息安全问题时刻都有新的变化，新的攻击方法层出不穷，攻击者攻击的方向越来越侧重于利用软件本身的安全漏洞，例如 SQL 注入漏洞、跨站脚本漏洞、CSRF 漏洞等，这些漏洞主要由不良的软件架构和不安全的编码产生。

开展源代码审计能够降低源代码出现的安全漏洞，构建安全的代码，提高源代码的可靠性，提高应用系统自身安全防护能力。源代码安全检测能够帮助开发人员提高源代码的质量，从底层保障应用系统本身的安全，从早期降低应用系统的开发成本。

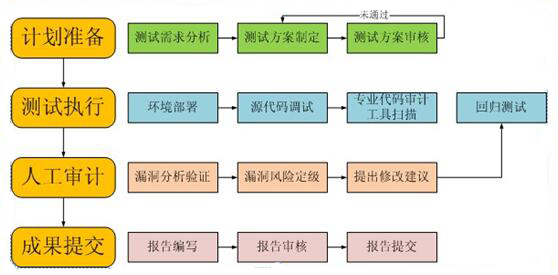
代码审计服务的主要内容包括但不限于：

* OWASP WEB TOP 10漏洞
* Web应用程序的权限架构
* Web应用通信安全
* 数据库的配置规范
* SQL语句的编写规范
* Web应用框架安全性

代码审计参考依据：

* CVE（Common Vulnerabilities & Exposures）公共漏洞字典表
* OWASP OWASP\_Testing\_Guide\_v3
* OWASP OWASP\_Development\_Guide\_2005
* OWASP OWASP\_Top\_10\_2010\_Chinese\_V1.0
* OWASP Mobile Security Project
* 信息安全技术 信息安全风险评估规范（GB/T 20984-2007）
* 信息技术 信息安全管理实用规则（GB/T 19716-2005）（ISO/IEC 17799:2000）
* 信息系统安全风险评估实施指南
* 设备、软件厂商公布的漏洞库

**1.2.2.2服务流程**



代码审计服务主要分为四个阶段，包括测试前期准备阶段、检测阶段实施、复测阶段实施以及成果汇报阶段：

1、前期准备阶段

在实施源代码安全检测工作前，负责项目实施的技术人员会和采购方对源代码安全检测服务相关的技术细节进行详细沟通。由此确认源代码安全检测的方案，方案内容主要包括确认的源代码安全检测范围、最终对象、检测要求的时间等内容，采购方签署源代码安全检测授权书。

在测试实施之前，会做到让采购方对安全测试过程和风险的知晓，使随后的正式测试流程都在采购方的控制下。

2、检测实施阶段

在检测实施过程中，测试人员首先进行环境部署，源代码调试，然后使用专业的代码安全检测工具扫描，完成初步的源代码安全检测测试执行工作。

然后由人工的方式进行确认和分析，对安全扫描的结果进行检测和验证，从而对源代码安全漏洞进行定级，测试人员需整理源代码安全检测服务的输出结果并编制源代码安全检测报告，最终提交采购方和对报告内容进行沟通。

3、复测阶段实施

在经过初次源代码安全检测报告提交和沟通后，等待采购方针对源代码安全检测发现的问题整改或加固。经整改或加固后，测试人员进行回归测试，即二次复测。复测结束后提交给采购方复测报告和对复测结果进行沟通。

4、成果汇报阶段

根据初次源代码安全检测和二次复测结果，整理源代码安全检测服务输出成果，代码审计服务交付物资料包括不限于如下内容：

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **输出时间** |
| 1 | 《代码审计服务方案》 | 启动阶段 |
| 2 | 《源代码缺陷分析报告》 | 执行阶段 |
| 3 | 《源代码缺陷溯源分析报告》 | 执行阶段 |

##### 1.3交付成果

项目交付成果包含但不限于以下内容：

1、海南智慧健康岛建设工程项目《代码审计报告》《代码审计服务方案》《源代码缺陷分析报告》《源代码缺陷溯源分析报告》

2、渗透测试服务成果，包括《渗透测试报告》《漏洞扫描报告》，以及安全加固建议等。

3、服务过程材料，包括但不限于调研表、技术测评记录、会议纪要等。

##### 1.4验收要求

1、服务单位应根据整体工作计划和安排完成安全服务工作，交付代码审计和渗透测试服务成果，海南智慧健康岛建设工程项目通过竣工验收。

2、采购方对代码审计、渗透测试服务材料进行签字确认。

### （2）商务要求

##### 2.1采购标的所属行业

本次采购标的所属行业为软件和信息技术服务业。

##### 2.2服务期限

自合同签订之日起，在采购人下达开工通知书后开始实施，投标人需于60天内完成服务工作并交付安全服务成果。

##### 2.3实施地点

采购人指定地点（海南省内）。

##### 2.4支付方式

1.本合同签订后，采购人待省财政资金下达后，采购人凭测评单位开具的正式有效增值税普通发票在3个工作日内向测评单位支付合同金额的30%预付款。

2.本项目初验合格，且采购人确认测评单位提供的网络安全服务及服务成果符合要求，待省财政资金下达后，采购人在收到测评单位开具的增值税普通发票之日起3个工作日内，向测评单位支付合同总金额的40% 。

3.本项目通过整体竣工验收，且采购人确认测评单位提供的网络安全服务及服务成果符合要求，待省财政资金下达后，采购人在收到测评单位开具的增值税普通发票之日起3个工作日内，向测评单位支付合同总金额的30%。

注：测评单位每次申请付款应提供付款申请书、符合采购人要求的等额发票及采购人报账所必须的相关材料。测评单位申请付款时，如测评单位提供的材料不完整、不真实，采购人有权暂缓付款而不视为违约。

##### 2.5其它相关要求

###### 2.5.1项目组人员要求

1、服务单位须根据项目特点和实际情况，提出项目团队配置方案，包括团队成员、组织架构和分组分工等，满足项目服务实施的需要。

2、项目团队成员应不少于1名项目经理、4名项目团队人员。所有人员必须属于测评单位在册员工**（提供社保缴纳证明为认定依据或出具承诺函）**，并提供相应人员相关简历信息**（包含所学专业、学历等证明材料），相关证明须加盖投标人单位公章**。合同签订后根据采购人实际需要派驻相关资历人员驻场开展服务。

3、合同签订后根据采购人实际需求派驻相关资历人员驻场开展服务直至项目验收，驻场地点由采购人指定。如实际提供的项目团队与投标提供的团队名单材料不符，将视为虚假应标。若采购人认为项目经理或团队成员能力与工作所要求的能力不相称而提出更换时，测评单位必须予以更换，人员更换不得影响测评成果交付时间；测评单位单方面更换项目经理或团队成员必须经采购单位书面同意，否则按违约处理直至合同终止。

4、项目团队实施中提供7×8小时咨询服务。项目验收后提供1年的跟踪咨询服务，自项目验收通过之日起计算。在实施单位提出服务请求时，项目团队应在30分钟内响应，在24个小时内提供解决方案。

###### 2.5.2工作要求

1、提供详细的项目服务实施方案和计划进度说明书。

2、项目实施完成后提供可靠的后期服务工作；

3、严格按照双方确定的计划进度保质保量完成工作；

4、规范项目实施过程中的文档管理；

5、提供必要的增值服务：配合省信息化主管部门开展本项目电子政务工程项目绩效评价考核、跟踪监督及项目档案事后监督等工作。

6、在海南智慧健康岛建设工程项目竣工验收阶段，对信息化主管部门及专家提出的涉及本项目软件系统整改意见的，服务单位应积极配合就整改后的应用系统进行再次代码审计、渗透测试服务，并出具最终报告，确保项目质量。

7、根据《关于进一步加强信息安全等级保护工作的通知》（琼等保办〔2013〕2号），本着实际安全保障需要和本项目现有安全防护手段，本项目需根据《海南省政务信息化项目建设管理实施细则（暂行）》要求，开展代码审计、渗透性测试等网络安全服务。

**2.5.2安全保密要求**

要求服务单位制定服务安全保密制度，确定项目保密责任人，同时要求服务单位：

1、按照国家和海南省有关保密规定，与采购单位签订保密协议，参与服务的工作人员签订保密承诺函；

2、严格履行保密职责，按照保密规定开展工作。

###### 2.5.3售后服务要求

服务单位需根据代码审计和渗透测试结果，应针对性的提出整改建议方案，根据提出的整改建议方案指导采购单位针对存在的问题进行整改，整改完成后提供全面问题复查，提供整改复核服务。

在整改实施过程中，服务单位应全力支持，负责技术把关、整改验收以及其他咨询工作。售后服务期限截至服务成果符合相关要求。如采购单位或主管部门对相关成果提出质疑，服务单位应根据采购单位要求提供无条件的到场服务直至相关成果满足相关要求。