**移动应用安全服务项目(2023-2024年度)需求**

# 项目名称

移动应用安全服务项目(2023-2024年度)

# 服务内容

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **详细描述** | **服务范围** |
| 1 | 移动应用渗透测试服务 | 1.渗透工程师模拟黑客方式，分别从源码/代码、调试安全、数据安全、加密算法安全、常见安全漏洞、传输协议安全、身份鉴别安全、接口安全等方面进行全量渗透测试，并输出渗透报告；  2.对发现的问题整理修复建议，并针对于报告中的问题提供线上的答疑支持。 | App/公众号/小程序渗透测试，远程及现场服务 |
| 2 | 个人信息安全检测服务 | 对标监管部门相关政策要求，依据《APP违法违规收集使用个人信息自评估指南》为检测内容，检测覆盖范围包括但不限《工信部发布信管函[2019]337号《关于开展APP侵害用户权益专项整治工作的通知》、《App违法违规收集使用个人信息行为认定方法》、《工业和信息化部《关于开展纵深推进 APP 侵害用户权益 专项整治行动的通知（工信部信管函〔2020〕164号》等检测要点，对小程序进行个人信息违法违规检测，并提供相应评估报告及修复意见，包含初测、整改咨询、复测服务。 | App/小程序个人信息安全检测，远程及现场服务 |
| 3 | APP安全加固服务 | **一、Android安全加固：** 1、Android基础加固项：含DEX函数分离+DEX整体加壳、资源防篡改、代码防篡改、防dump、动态调试、防注入、防二次打包； 2、资源文件加密：对应用中assets、res目录下的资源进行加密，防止资源查看以及盗用； 3、SO库加壳：利用自主研发的加密算法对C/C++源码编译出来的so文件进行加壳，使加壳后的so文件无法通过ida反编译工具查看导出符号，并在加壳的过程中对数据段进行加密压缩，从而加壳后的so文件具备无法正确反编译和反汇编并体积会有减小的趋势； 4、签名文件保护：对应用签名信息进行校验，防止APK被其他签名证书签名； 5、本地数据加密：对应用中本地数据读写接口进行自动拦截加密出来，防止应用缓存数据明文落地。 **二、IOS安全加固：** 对C/C++/OC代码进行混淆加固，包括字符串加密、指令多样化、基本块分裂、控制流引入、跳转指令插入、控制流扁平化、控制流间接化等功能。 | App安全加固，服务期内不限制应用加固次数 |
| 4 | APP自动化平台检测服务 | APP加固完成后对APP进行自动化平台检测，针对Android和IOS移动应用通过静态反编译技术对APK文件进行反编译，通过词法分析、语法分析、控制流、数据流分析等技术对移动应用程序代码和配置文件进行扫描，验证移动应用是否满足规范性、安全性、可靠性、可维护性等进行检测，同时通过沙箱模型、云手机等方式对移动应用的安装、运行过程中的行为进行监测分析，验证应用是否存在安全性问题。 | Android、IOS加固完成后，对已加固APP分别进行自动化平台检测，并提供自动化平台检测报告 |
| 5 | 移动应用资产排查及梳理 | 服务期内，定期针对我单位的移动应用资产进行摸排统计（包括APP、公众号、小程序等），形成移动应用资产数据表，并定期对所有移动应用进行安全检查及防护。 | 移动应用资产数据表 |
| 6 | 重大节假日前后扫描支持 | 服务期内，在重大节假日前后针对移动应用开展安全扫描服务。 | App/公众号/小程序安全扫描 |
| 7 | 移动应用安全培训服务 | APP安全检测报告、个人信息安全检测报告解读，标准规范咨询、解读培训等。 | 报告解读及标准规范咨询、解读培训等，现场培训 |

1. **移动应用渗透测试服务**

针对我方的APP/公众号/小程序开展人工渗透测试复测，通过专业的渗透工程师模拟黑客方式对APP/公众号/小程序分别从源码/代码、调试安全、数据安全、加密算法安全、常见安全漏洞、传输协议安全、身份鉴别安全、接口安全等方面进行人工渗透，输出渗透报告，并针对于渗透报告中的问题提供线上的答疑支持。

1. **个人信息安全检测服务**

根据《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《GB/T 35273-2020-信息安全技术 个人信息安全规范》、《APP违法违规收集使用个人信息自评指南》、《APP违法违规收集个人信息行为认定方法》等20条及以上标准依据和范围，涵盖所有用户隐私合规指南，输出评估报告、整改建议及指导完成整改。

**检测内容包括但不限于：**

1. **隐私政策的独立性、易读性：**从APP应用中找到隐私政策，对其包括展现形式、发布形式、访问形式、阅读形式等方面进行识别评估。
2. **清晰说明各项业务功能及所收集个人信息类型：**从软件开发设计方案、APP应用软件业务功能、隐私政策文本等方面进行识别评估。
3. **清晰说明个人信息处理规则及用户权益保障：**从单位基本情况、个人信息的存储位置、存储期限、处理方式、个人信息使用规范、个人信息出境情况、个人信息安全保护情况、对外共享、转让、公开披露个人信息规则、用户权利保障机制、隐私政策时效与更新情况等方面进行识别评估。
4. **不应在隐私政策等文件中设置不合理条款：**从隐私政策条款等方面进行识别评估。
5. **收集个人信息应明示收集目的、方式、范围：**从隐私政策文本、APP应用系统权限、个人信息收集、使用、提示形式等方面进行识别评估。
6. **收集使用个人信息应经用户自主选择同意，不应存在强制捆绑授权行为：**从APP应用软件功能选项、授权请求、用户自主行为、私自收集使用、超频调用、自启动关联启动、截留个人信息等方面进行识别评估。
7. **收集个人信息应满足必要性要求：**从收集个人信息类型范围、业务功能、用户自主选择行为、系统权限等方面进行识别评估。
8. **支持用户注销账号、更正或删除个人信息：**从APP应用软件系统功能、用户申诉处理情况、不合理条件等方面进行识别评估。
9. **及时反馈用户申诉：**从APP反馈用户申述处理情况等方面进行识别评估。

**检测技术要求：**

1. 能够检测APP首次启动后用户未同意隐私政策前收集个人信息行为，包括收集MAC地址、IP地址、IMEI、IMSI、AndroidID、MEID、GET\_TASK检索了应用程序等行为，并能提供问题的详细堆栈信息。
2. 能够检测APP前台打开、静默或处于锁屏状态时，APP收集使用个人信息与权限的频率是否超频，并能提供问题的详细堆栈信息。
3. 能够检测APP是否存在频繁自启动和关联启动；
4. 能够在APP处于后台运行状态时或保活后台时，检测是否存在调用收集用户个人信息，并能提供问题的详细堆栈信息。
5. **APP安全加固服务**

本次APP安全加固服务内容范围包括Android APP加固、IOS APP加固、及APP安全培训服务等。

1. **Android APP加固：**
2. 支持通过多DEX整体加壳、DEX分离加壳、DEX代码VMP保护等方式，实现DEX文件保护。
3. 支持通过SO库文件加壳、SO库高级混淆、SO Linker、SO防调用、SO虚拟化保护等方式，实现SO库文件保护。
4. 支持通过DEX文件防篡改、SO库文件防篡改、H5代码防篡改、DLL文件防篡改等方式，实现代码防篡改。
5. 支持通过assets资源防篡改、res资源防篡改、AndroidManifest配置文件防篡改等方式，实现资源防篡改。
6. 支持通过签名文件保护等方式，实现签名防篡改。
7. 支持通过防动态调试、防进程调试、防内存代码注入、防内存dump、防加速器、防止模拟器运行等方式，实现反调试。
8. 支持通过防内存数据读取、防内存数据修改、防日志泄漏、本地数据加密等方式实现数据防泄漏。
9. 支持通过应用防截屏、应用防劫持等方式，实现页面数据保护。
10. 支持通过加固后APK体积压缩等方式，实现加固后体积压缩等。
11. **IOS APP加固：**

支持通过对C/C++/OC代码进行混淆加固，包括字符串加密、指令多样化、基本块分裂、控制流引入、跳转指令插入、控制流扁平化、控制流间接化等功能，实现iOSapp代码保护。

1. **APP自动化平台检测服务**

APP加固完成后对APP进行自动化平台检测，针对Android和IOS移动应用通过静态反编译技术对APK文件进行反编译，通过词法分析、语法分析、控制流、数据流分析等技术对移动应用程序代码和配置文件进行扫描，验证移动应用是否满足规范性、安全性、可靠性、可维护性等进行检测，同时通过沙箱模型、云手机等方式对移动应用的安装、运行过程中的行为进行监测分析，验证应用是否存在安全性问题。

1. **移动应用资产排查及梳理**

采用大数据监测技术对全国范围类的app应用市场、贴吧、论坛、网盘等进行监测及数据收集，梳理出我单位的移动应用资产，并对梳理出移动应用开展安全检测及防护。

1. **重大节假日前后扫描支持**

服务期内，在重大节假日前后针对移动应用开展安全扫描服务。

1. **移动应用安全培训服务**

针对APP安全检测报告、个人信息安全检测报告解读，标准规范咨询等提供解读培训。

# 服务方式

服务商成立专门的项目组开展工作，指派专人负责，按时完成工作内容。

# 服务时间

合同生效起 24个月内。

# 服务响应要求

1. **服务响应时间**
2. 工作期间（正常工作日8：00-18：00），服务响应时间不超过0.5小时，到达现场时间不超过2小时；
3. 非工作期间，服务响应时间不超过1小时，到达现场时间不超过3小时。
4. 服务商应提出问题解决方案，工作至问题完全修复为止，修复时间不超过2个工作日。
5. **服务商应作出无推诿承诺：**即服务商在收到院方应急通知及要求后，须立即组织人员远程或派技术人员到场，全力协助、使问题尽快恢复正常。
6. **提供详细的服务人员清单**

服务商应有专门的服务部门并指定固定技术力量用于项目服务，并向用户提供详细的服务人员清单及其联系方式。

# 服务验收

1. 验收时间：由服务商向院方申请验收，合同到期后 5 个工作日内院方需启动验收。
2. 验收人员：双方相关人员。
3. 验收标准

1. 服务商提供完整的技术资料，包括但不限于检测报告、整改方案、信息安全政策法规文件。

2. 提供给我方的服务应符合国家、行业相关标准及用户需求。

# 合同款支付方式

(一) 服务期开始后，在收到开具相应金额正式发票后，支付合同总金额的50%。

(二) 服务时间达到50%，服务商提供第一年度服务记录及开具相应金额正式发票后，支付合同总金额的20%。

(三) 合同期满（服务时间达到100%）且通过验收，服务商提供完整服务记录及开具相应金额正式发票后，支付合同总金额的30%。