**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. 是否有隐私政策
2. 是否有未成人个人信息保护规则
3. 是否制定专门的未成年人个人信息处理规则
4. 隐私政策是否单独成文
5. 隐私政策是否易于访问
6. 隐私政策是否易于阅读
7. 是否明示收集个人信息的业务功能
8. 业务功能与所收集的个人信息类型是否一一对应
9. 是否明示各项业 务功能所收集的个人信息类型
10. 是否以改善功能、优化体验等为由收集个人信息
11. 是否显著标识个人敏感信息类型
12. 是否明示APP功能划分
13. 必要个人信息是否满足告知同意通用要求
14. App运营者的基本情况
15. 个人信息存储和超期处理方式
16. 强制定向推送信息
17. 显著区分定向推送服务
18. 是否收集唯一设备识别码用于定向推送/用户画像场景
19. 是否存在大数据杀熟的情形
20. 个人信息出境情況
21. 个人信息安全保护措施和能力
22. 对外共享、转让、公开披露个人信息规则
23. 用户权利保障机制
24. 征得授权同意的例外
25. 个人信息的展示限制
26. 用户申诉渠道和反馈机制
27. 隐私政策时效
28. 隐私政策更新
29. 隐私政策等文件是否存在免责等不合理条款
30. 是否同步告知申请打开个人信息权限目的
31. 是否同步告知申请提供个人敏感信息的目的
32. 若使用Cookie及其同类技术收集个人信息，是否向用户明示
33. 若存在嵌入第三方代码插件收集个人信息的功能，是否向用户明示
34. 是否为用户提供第三方应用授权管理功能或渠道
35. 是否向用户明示建立个人信息保护“双清单”制度
36. 是否优化隐私政策和权限调用展示方式
37. 是否欺骗误导用户下载APP
38. 是否规范APP推荐下载行为，改善网页浏览服务体验
39. 应用分发平台上的APP信息是否明示不到位
40. 应用分发平台管理责任落实不到位
41. 以默认选择同意隐私政策等非明示方式征求用户同意
42. 征得用户同意前就开始收集个人信息或打开可收集个人信息的权限
43. 是否存在将多项业务功能和权限打包，要求用户一揽子接受的情况
44. 是否存在过度声明权限的情形
45. 前台收集个人信息的频度等超出业务功能实际需要
46. 后台收集个人信息的频度等超出业务功能实际需要
47. 收集个人信息的频度是否与业务场景对应
48. 是否未征得用户同意读取剪切板/公共存储区
49. 是否存在不给权限不让用
50. APP频繁自启动和关联启动
51. 私自截留第三方应用收集的个人信息
52. 是否以不正当方式误导用户同意收集个人信息
53. 广告关闭选项找不到、关不掉
54. 实际收集的个人信息类型是否超出隐私政策所述范围
55. 收集与业务功能有关的非必要信息，是否经用户自主选择同意
56. 是否在用户明确对于用户明确拒绝后继续索要权限、打扰用户
57. 是否拒绝提供非服务所必需的个人信息时，影响用户使用
58. 是否收集与业务功能无关的个人信息
59. App更新是否更改系统权限设置
60. 是否支持用户注销账号
61. 是否支持用户查询、更正或删除个人信息
62. 是否及时反馈用户申诉

**检测技术要求：**

1. 能够检测APP未经授权同意，私自获取使用个人信息行为，监控行为包含不可变设备识别符（IMEI、MEID、SIM卡序列号、设备硬件序列号、BSSID(WIFI的AMC地址)）/可变设备标识符（Android ID、IP 、GAID、OAID 、IDFA、IDFV）。
2. 能够检测APP在前台及锁屏状态下收集使用个人信息与权限的行为以及频率，支持App在前台状态时收集个人信息行为和个人信息权限的频率检测、支持App在锁屏静默状态时收集个人信息行为和个人信息权限的频率检测。
3. 能够检测APP在后台及保活状态下收集使用个人信息与权限的行为以及频率，支持App在可见后台状态时收集个人信息行为和个人信息权限的频率检测，支持App在保活后台状态时收集个人信息行为和个人信息权限的频率检测。
4. 能够检测App存在频繁自启动，APP结束进程后可通过广播监听自启动。

**测试要求：**

**院方有权要求对供应商进行个人信息安全检测技术验证，验证包括本项要求的全部内容及技术要求，供应商需对Android和IOS、小程序进行全量个人信息安全检测，5个工作日内完成检测并出具检测报告。测试不能满足本项目的基本技术要求时，则视为该不满足参数要求。**

1. **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：**

1、DEX 代码加固技术：

* 多DEX文件加密：对APK中所有DEX文件执行加固，并确保APP兼容性和性能不收影响。
* DEX整体加壳：对DEX源码进行整体加密和隐藏，保留壳代码，防止黑客发现源码。
* DEX分离加壳：对DEX文件中的代码进行函数抽离保护，程序运行时将代码分段动态回填，保证内存中不存在连续、完整的代码。
* DEX代码VMP保护：对DEX中的java代码进行抽离与转换（java代码的native化），根据自定义的虚机指令集去调用C层转换的代码。
* Java2CPP：将DEX文件中的Java代码转换成C++代码，将C++代码编译成动态库。

2、SO代码加固技术：

* SO库文件加壳：对自主研发的SO文件进行加壳处理，隐藏外部函数，自定义elf结构防止SO文件被黑客逆向。
* SO库高级混淆：提供LLVM级别的加密编译器，可将自主研发的SO文件在编译时对代码进行高强度的混淆保护。
* SO Linker：对整个so文件进行加密压缩，包括代码段、符号表和字符串等，运行时再解密解压缩到内存，从而有效的防止so数据的泄露。
* SO防调用：对so文件进行授权绑定，防止so文件被非授权应用调用运行。
* SO虚拟化保护：采用ELF VMP技术，so文件的源码进行虚拟化保护，实现数据隐藏、防篡改、防Dump，增加逆向分析的难度。

3、应用防篡改技术：

（1）代码防篡改：

* 支持对DEX文件防篡改。
* 支持SO库文件防篡改。
* 支持H5代码防篡改。
* 支持DLL文件防篡改。

（2）资源文件防篡改：

* 支持 assets 资源文件防篡改。
* 支持 res 资源文件防篡改。
* 支持AndroidManifest.xml 防篡改。

（3）签名文件保护

* 支持签名防篡改。

4、防调试保护技术

* 防动态调试：防止对App进行进程调试，如GDB动态调试。
* 防进程调试：防止第三方工具对程序进程进行进程附着等调试。
* 防内存代码注入：防止黑客在进程附着后的内存代码注入。
* 防内存dump：防止黑客通过内存dump的方式窃取内存数据。
* 防加速器：通过对加速器整体分析，进行针对性的防护措施。
* 防止模拟器运行：检测App运行环境，禁止在模拟器中运行。

5、数据防泄漏技术

* 内存数据保护：防止内存数据读取工具窃取App内存数据，防止第三方工具对内存数据修改。
* 防日志泄露：防止黑客通过日志调试的方式分析客户端代码。
* 本地数据保护：支持本地sharepreference数据加密、SQLite数据加密。

6、页面数据保护

* 应用防截屏：防止黑客通过对重要页面截屏的方式窃取敏感数据，采用纯净加密方式，无需集成SDK即可实现。
* 应用防劫持：防止黑客通过钓鱼页面攻击的方式，采用纯净加密方式，无需集成SDK即可实现。

1. **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。

# 资质要求

供应商应该同时具有：

1. 中国网络安全审查技术与认证中心颁发的信息安全应急处理服务(二级)及以上资质。（提交加盖公章资质证明文件）
2. 中国网络安全审查技术与认证中心颁发的信息安全风险评估服务(二级)及以上资质。（提交加盖公章资质证明文件）
3. 中国信息安全测评中心颁发的信息安全服务资质证书（安全工程类一级）及以上资质。（提交加盖公章资质证明文件）
4. 近3年（已合同签订日期为准）实施过安全服务类项目案例≥3个。（提供加盖公章的有效合同复印件）

注：未提交证明材料、不符合资质及技术要求的供应商报价视为无效，弄虚作假一经查实则将供应商列入采购人黑名单。