

权利要求书

1. 一种小程序的安全扫描方法，所述方法包括：
获取待发布的目标小程序；
调用安全扫描策略组合对所述目标小程序进行多维度的安全扫描；
5 当所述目标小程序通过所述多维度的安全扫描时，将所述目标小程序发布至与搭载所述目标小程序的目标 APP 对应的服务端。
2. 根据权利要求 1 所述的方法，所述安全扫描策略组合包括以下安全扫描策略中多个的组合：
对所述目标小程序进行恶意代码扫描；
10 对所述目标小程序进行安全漏洞扫描；
对与所述目标小程序对应的服务端接口进行安全漏洞扫描。
3. 根据权利要求 2 述的方法，所述对所述目标小程序进行恶意代码扫描，包括以下示出的扫描方式中的一个或者多个的组合：
检测所述目标小程序是否携带攻击载荷；
15 检测所述目标小程序调用的所有函数是否存在为所述目标小程序定义的合法调用函数以外的恶意调用函数；
检测所述目标小程序调用的媒体以及文本内容是否存在违规内容。
4. 根据权利要求 2 述的方法，所述对所述目标小程序进行安全漏洞扫描，包括以下示出的扫描方式中的一个或者多个的组合：
20 检测所述目标小程序是否存在敏感信息泄露漏洞；
检测所述目标小程序是否存在 HTML 代码漏洞；
检测所述目标小程序是否存在 JS 代码漏洞；
检测所述目标小程序是否存在非法外部资源引用漏洞。
5. 根据权利要求 2 述的方法，所述对所述目标小程序的服务端接口进行安全漏洞
25 扫描，包括：
解析所述目标小程序的服务端接口；
对解析出的所述服务端接口进行接口漏洞扫描。
6. 一种小程序的安全扫描装置，所述装置包括：
获取模块，获取待发布的目标小程序；
30 扫描模块，调用安全扫描策略组合对所述目标小程序进行多维度的安全扫描；
发布模块，当所述目标小程序通过所述多维度的安全扫描时，将所述目标小程序发

布至与搭载所述目标小程序的目标 APP 对应的服务端。

7. 根据权利要求 6 所述的装置, 所述扫描模块进一步执行以下扫描策略中的多个的组合:

对所述目标小程序进行恶意代码扫描;

5 对所述目标小程序进行安全漏洞扫描;

对与所述目标小程序对应的服务端接口进行安全漏洞扫描。

8. 根据权利要求 7 述的装置, 所述扫描模块进一步执行以下恶意代码扫描方式中的一个或者多个的组合:

检测所述目标小程序是否携带攻击载荷;

10 检测所述目标小程序调用的所有函数是否存在为所述目标小程序定义的合法调用函数以外的恶意调用函数;

检测所述目标小程序调用的媒体以及文本内容是否存在违规内容。

9. 根据权利要求 7 述的装置, 所述扫描模块进一步执行以下安全漏洞扫描方式中的一个或者多个的组合:

15 检测所述目标小程序是否存在敏感信息泄露漏洞;

检测所述目标小程序是否存在 HTML 代码漏洞;

检测所述目标小程序是否存在 JS 代码漏洞;

检测所述目标小程序是否存在非法外部资源引用漏洞。

10. 根据权利要求 7 述的装置, 所述扫描模块进一步:

20 解析所述目标小程序的服务端接口;

对解析出的所述服务端接口进行接口漏洞扫描。

11. 一种电子设备, 包括:

处理器;

用于存储机器可执行指令的存储器;

25 其中, 通过读取并执行所述存储器存储的与机器学习模型的训练的控制逻辑对应的机器可执行指令, 所述处理器被促使:

获取待发布的目标小程序;

调用安全扫描策略组合对所述目标小程序进行多维度的安全扫描;

当所述目标小程序通过所述多维度的安全扫描时, 将所述目标小程序发布至与搭载

30 所述目标小程序的目标 APP 对应的服务端。