背景技术

软件系统的开发总伴随这漏洞隐患。有别于常见漏洞，逻辑漏洞是系统设计逻辑不严谨导致的漏洞类型，具有较大的危险性和检测难度。支付逻辑漏洞是逻辑漏洞中一种攻击成本低，但危害大的类型。由于它会直接涉及财产交易，且存在于民众日常使用的在线支付系统中，因此经常受到攻击者的关注。

目前为止没有一套稳定而有效的针对支付逻辑漏洞的自动化检测手段，因此在生产环境中，针对其检测仍主要采用人工挖掘的方式。人工逻辑漏洞挖掘不仅效率低下、假阴性概率高，并且还受限于检测人员的专业水平，难以大规模、成体系地进行检测。如果能够开发一种自动化检测或辅助检测系统，就能够极大缓解这一系列问题。

目前自动化的逻辑漏洞检测技术主要包括以下几类：

基于白盒测试技术的检测技术：在拥有软件系统源码或二进制文件的前提下，可以基于符号执行框架和污点分析，来达到源码语义树抽象，以及进一步进行逻辑漏洞挖掘的目的。

基于行为分析的黑盒测试技术：通过对用户行为流量的截取，进而提取其行为模式并分析软件系统业务流，以此为依据进行测试序列的生成和执行。此类技术还会应用有限状态机等模型，以便更好更全面地描述软件系统、为测试用例生成提供更多信息。

用户行为驱动的测试技术：此类技术抛弃原有的用户流量检测的手段，通过对用户行为的直接记录与重放，基于专家预设规则，实现实时的测试用例执行，进一步提高黑盒测试的时效性。

本发明主要基于用户行为驱动以及用户行为模式分析技术。与现有黑盒测试技术相比，本发明有以下两个优点：首先，该发明尽可能地剔除了用户需要的额外操作以及专业知识，仅基于用户操作，实现了一套测试用例生成、执行、反馈全过程全自动的支付逻辑漏洞检测系统，极大提高了其在生产环境下的易普及性和可用性。其次，该发明由用户行为驱动，同时通过信息采集与测试操作分离，统筹分析用户行为及软件系统实现更为系统且时效性更高的逻辑漏洞检测。

发明内容

本发明针对现有技术上的不足和缺陷，提出一种基于用户操作收集和有限状态机的自动化支付漏洞检测技术。行为控制模块对用户在待测平台购买一件商品的操作进行记录，获取用户的操作信息。执行模块重放该操作的同时，系统解析模块监听器用户操作流量，生成对应的用户行为有限状态机，格式化后放入数据库备用。针对该状态机进行统筹分析，并根据专家攻击知识库变异生成漏洞测试用例。执行模块根重放用户行为的同时，据测试用例对流量进行拦截、篡改、释放，并由攻击结果分析模块获取、分析反馈信息判断漏洞是否被触发。最后系统将统计检测结果，生成完整的检测报告。

本发明的主要技术方案如下：

用户行为控制模块与执行模块主要基于开源自动化测试工具PlayWright。PlayWright的用户行为记录和重放接口实现了检测系统的执行与记录功能，配合本系统中的分析模块，实现了用户行为和访问流量的匹配，以及测试用例的执行功能。

用户行为会被描述为一个五元有限状态机，包含了标记主键、URL、用户行为描述、请求报文各项信息以及正常响应。针对该用户行为业务流有限状态机，系统检测主要基于敏感参数检测和基于有限状态机的参数传播链生成两类，其中参数传播链生成是测试用例的基础。

专家攻击知识库是基于常见的支付逻辑漏洞的调研结果，得到支付系统的各类敏感信息总结，以及针对这些系统薄弱点的常见攻击行为。本发明基于该库实现系统薄弱点的发现以及流量变异来产生测试用例，执行器会以此为依据进行流量的拦截与篡改。

攻击反馈模块（TODO）

具体实施方式