(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112860552 B
(45)授权公告日 2023.12.15

(21)申请号 202110145266.5
(22)申请日 2021.02.02
(65)同一申请的已公布的文献号
申请公布号 CN 112860552 A
(43)申请公布日 2021.05.28
(73)专利权人 贝壳找房(北京)科技有限公司
地址 100000 北京市海淀区创业路2号1幢1层102室
(72)发明人 李成龙 肖德超
(74)专利代理机构 北京润平知识产权代理有限公司 11283
专利代理师 肖冰滨 王晓晓
(51)Int.Cl.
G06F 11/36(2006.01)
G06F 16/903(2019.01)
(56)对比文件
CN 104834588 A,2015.08.12
CN 106354624 A,2017.01.25
CN 107103243 A,2017.08.29
CN 109491900 A,2019.03.19
US 2018089066 A1,2018.03.29
CN 110210212 A,2019.09.06
CN 104503900 A,2015.04.08
CN 106155891 A,2016.11.23
CN 109542780 A,2019.03.29
CN 110399306 A,2019.11.01
CN 111078863 A,2020.04.28
US 2013104106 A1,2013.04.25
梁俊.基于Selenium和TestNG的自动化测试框架的设计与实现.《中国优秀硕士学位论文全文数据库 信息科技辑》.2020,(第03期),I138-370.
truelovezte.开源项目 sosotest 自动化测试平台.《https://blog.csdn.net/truelovezte/article/details/103030571》.2019,1-4.
(续)
审查员 严丽

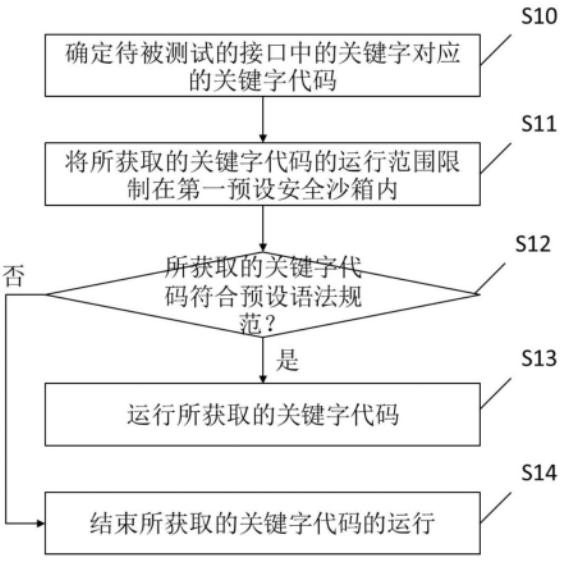
权利要求书2页 说明书10页 附图4页

(54)发明名称

关键字机制运行方法和装置

(57)摘要

本发明实施例提供一种关键字机制运行方法和装置,属于接口测试领域。该关键字机制运行方法包括:确定待被测试的接口中的关键字对应的关键字代码;将所获取的关键字代码的运行范围限制在第一预设安全沙箱内;在所述第一预设安全沙箱内运行所获取的关键字代码时,验证所获取的关键字代码是否符合预设语法规范;以及在所获取的关键字代码不符合预设语法规范的情况下,结束所获取的关键字代码的运行。藉此,实现了对关键字代码的运行进行隔离,对关键字代码的运行范围进行限制,隔离关键字的运行环境;在关键字代码运行异常时可以正确捕获到运行异常,及时发现关键字代码中的异常情况。



CN 112860552 B

[转续页]

[接上页]

(56)对比文件

董韫超.搜索引擎测试系统的设计与实现.《中国优秀硕士学位论文全文数据库 信息科技辑》.2015,(第06期),I138-192.

1.一种关键字机制运行方法,其特征在于,该关键字机制运行方法包括:

确定待被测试的接口中的关键字对应的关键字代码;

将所获取的关键字代码的运行范围限制在第一预设安全沙箱内;

在所述第一预设安全沙箱内运行所获取的关键字代码时,验证所获取的关键字代码是否符合预设语法规范;以及

在所获取的关键字代码不符合预设语法规范的情况下,结束所获取的关键字代码的运行;

所述确定待被测试的接口中的关键字对应的关键字代码包括:

从预设关键字数据库中获取所述关键字对应的关键字字符串;以及

执行所述关键字字符串,将所述关键字字符串转换成所述关键字代码,以确定待被测试的接口中的关键字对应的关键字代码;

在执行所述关键字字符串将所述关键字字符串转换成所述关键字代码之前,该关键字机制运行方法还包括:

判断所获取的关键字字符串是否是恶意代码字符串,其中,所述执行所述关键字字符串将所述关键字字符串转换成所述关键字代码的条件为所获取的关键字符串不是恶意代码字符串。

2.根据权利要求1所述的关键字机制运行方法,其特征在于,所述预设关键字数据库基于以下内容被创建:

接收被编写的编写关键字代码转换的编写关键字字符串;

判断所述编写关键字字符串是否是所述恶意代码字符串;

在所述编写关键字字符串不是所述恶意代码字符串的情况下,执行所述编写关键字字符串,以将所述编写关键字字符串转换成对应的编写关键字代码;

将所述编写关键字代码的运行范围限制在第二预设安全沙箱内;

在所述第二预设安全沙箱内运行所述编写关键字代码时,验证所述编写关键字代码是否符合所述预设语法规范;以及

在所述编写关键字代码符合所述预设语法规范的情况下,将所述编写关键字字符串存储在数据库中,以构建所述预设关键字数据库。

3.一种关键字机制运行装置,其特征在于,该关键字机制运行装置包括:

关键字代码确定模块,用于确定待被测试的接口中的关键字对应的关键字代码;

安全沙箱创建模块,用于将所获取的关键字代码的运行范围限制在第一预设安全沙箱内;

验证模块,用于在所述第一预设安全沙箱内运行所获取的关键字代码时,验证所获取的关键字代码是否符合预设语法规范;以及

处理模块,用于在所获取的关键字代码不符合预设语法规范的情况下,结束所获取的关键字代码的运行;

所述关键字代码确定模块确定待被测试的接口中的关键字对应的关键字代码包括:

从预设关键字数据库中获取所述关键字对应的关键字字符串;以及

执行所述关键字字符串,将所述关键字字符串转换成所述关键字代码,以确定待被测试的接口中的关键字对应的关键字代码;

该关键字机制运行装置还包括：

判断模块，用于在执行所述关键字字符串将所述关键字字符串转换成所述关键字代码之前，判断所获取的关键字字符串是否是恶意代码字符串，其中，所述执行所述关键字字符串将所述关键字字符串转换成所述关键字代码的条件为所获取的关键字符串不是恶意代码字符串。

4.根据权利要求3所述的关键字机制运行装置，其特征在于，所述预设关键字数据库基于以下内容被创建：

接收被编写的编写关键字代码转换的编写关键字字符串；

判断所述编写关键字字符串是否是所述恶意代码字符串；

在所述编写关键字字符串不是所述恶意代码字符串的情况下，执行所述编写关键字字符串，以将所述编写关键字字符串转换成对应的编写关键字代码；

将所述编写关键字代码的运行范围限制在第二预设安全沙箱内；

在所述第二预设安全沙箱内运行所述编写关键字代码时，验证所述编写关键字代码是否符合所述预设语法规范；以及

在所述编写关键字代码符合所述预设语法规范的情况下，将所述编写关键字字符串存储在数据库中，以构建所述预设关键字数据库。

5.一种机器可读存储介质，其特征在于，该机器可读存储介质上存储有指令，该指令用于使得机器执行权利要求1-2中任一项所述的关键字机制运行方法。

6.一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现权利要求1-2中任一项所述的关键字机制运行方法。

关键字机制运行方法和装置

技术领域

[0001] 本发明涉及接口测试领域,具体地涉及一种关键字机制运行方法和装置。

背景技术

[0002] 接口测试有投入少收益高的特点,因此接口测试技术在测试领域中被广泛采用。虽然接口测试技术经历了长久的发展,但目前的接口测试平台(或框架)在使用上仍有较大限制,通常使用者仅能依赖平台(或框架)提供的有限能力来执行测试任务,很难满足接口测试的通用需求,因此基于关键字技术实现的接口测试装置应运而生。当前,接口测试平台(或框架)实现关键字技术有2个不同方案。方案一:以httprunner为主的接口测试框架直接使用关键字代码脚本,利用程序设计语言的反射特性对关键字代码脚本进行加载,并在需要执行关键字的时刻执行关键字代码。方案二:以sosotest为代表的接口测试平台采用程序设计语言的eval或exec等机制实现代码字符串到可执行代码加载的过程,然后使用程序设计语言的反射机制获取关键字执行代码,并在需要执行关键字的时刻执行关键字代码。方案一与方案二的主要区别在于关键字存储的载体,基于代码框架的方案采用代码文件直接加载关键字,而基于测试平台的方案不能直接使用代码文件,需要将代码存入到数据库之中,通过eval或exec将数据库中的关键字文本转化为关键字代码。

[0003] 虽然采用以上两种方案均可以实现关键字装置,但两种方式均有明显不足。两种关键字机制都没有对代码安全性进行检查,使用者可以传入任何恶意代码。两种关键字机制都没有对代码进行运行时隔离,代码可以和系统功能混淆。

发明内容

[0004] 本发明实施例的目的是提供一种关键字机制运行方法和装置,其可解决或至少部分解决上述问题。

[0005] 为了实现上述目的,本发明实施例的一个方面提供一种关键字机制运行方法,该关键字机制运行方法包括:确定待被测试的接口中的关键字对应的关键字代码;将所获取的关键字代码的运行范围限制在第一预设安全沙箱内;在所述第一预设安全沙箱内运行所获取的关键字代码时,验证所获取的关键字代码是否符合预设语法规范;以及在所获取的关键字代码不符合预设语法规范的情况下,结束所获取的关键字代码的运行。

[0006] 可选地,所述确定待被测试的接口中的关键字对应的关键字代码包括:从预设关键字数据库中获取所述关键字对应的关键字字符串;以及执行所述关键字字符串,将所述关键字字符串转换成所述关键字代码,以确定待被测试的接口中的关键字对应的关键字代码。

[0007] 可选地,在执行所述关键字字符串将所述关键字字符串转换成所述关键字代码之前,该关键字机制运行方法还包括:判断所获取的关键字字符串是否是恶意代码字符串,其中,所述执行所述关键字字符串将所述关键字字符串转换成所述关键字代码的条件为所获取的关键字符串不是恶意代码字符串。

[0008] 可选地,所述预设关键字数据库基于以下内容被创建:接收被编写的编写关键字代码转换的编写关键字字符串;判断所述编写关键字字符串是否是所述恶意代码字符串;在所述编写关键字字符串不是所述恶意代码字符串的情况下,执行所述编写关键字字符串,以将所述编写关键字字符串转换成对应的编写关键字代码;将所述编写关键字代码的运行范围限制在第二预设安全沙箱内;在所述第二预设安全沙箱内运行所述编写关键字代码时,验证所述编写关键字代码是否符合所述预设语法规范;以及在所述编写关键字代码符合所述预设语法规范的情况下,将所述编写关键字字符串存储在数据库中,以构建所述预设关键字数据库。

[0009] 相应地,本发明实施例的另一方面提供一种关键字机制运行装置,该关键字机制运行装置包括:关键字代码确定模块,用于确定待被测试的接口中的关键字对应的关键字代码;安全沙箱创建模块,用于将所获取的关键字代码的运行范围限制在第一预设安全沙箱内;验证模块,用于在所述第一预设安全沙箱内运行所获取的关键字代码时,验证所获取的关键字代码是否符合预设语法规范;以及处理模块,用于在所获取的关键字代码不符合预设语法规范的情况下,结束所获取的关键字代码的运行。

[0010] 可选地,所述关键字代码确定模块确定待被测试的接口中的关键字对应的关键字代码包括:从预设关键字数据库中获取所述关键字对应的关键字字符串;以及执行所述关键字字符串,将所述关键字字符串转换成所述关键字代码,以确定待被测试的接口中的关键字对应的关键字代码。

[0011] 可选地,该关键字机制运行装置还包括:判断模块,用于在执行所述关键字字符串将所述关键字字符串转换成所述关键字代码之前,判断所获取的关键字字符串是否是恶意代码字符串,其中,所述执行所述关键字字符串将所述关键字字符串转换成所述关键字代码的条件为所获取的关键字符串不是恶意代码字符串。

[0012] 可选地,所述预设关键字数据库基于以下内容被创建:接收被编写的编写关键字代码转换的编写关键字字符串;判断所述编写关键字字符串是否是所述恶意代码字符串;在所述编写关键字字符串不是所述恶意代码字符串的情况下,执行所述编写关键字字符串,以将所述编写关键字字符串转换成对应的编写关键字代码;将所述编写关键字代码的运行范围限制在第二预设安全沙箱内;在所述第二预设安全沙箱内运行所述编写关键字代码时,验证所述编写关键字代码是否符合所述预设语法规范;以及在所述编写关键字代码符合所述预设语法规范的情况下,将所述编写关键字字符串存储在数据库中,以构建所述预设关键字数据库。

[0013] 此外,本发明实施例的另一方面还提供一种机器可读存储介质,该机器可读存储介质上存储有指令,该指令用于使得机器执行上述的关键字机制运行方法。

[0014] 另外,本发明实施例的另一方面还提供一种电子设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述程序时实现上述的关键字机制运行方法。

[0015] 通过上述技术方案,将关键字代码的运行范围限制在安全沙箱内,如此,对关键字代码的运行进行隔离,对关键字代码的运行范围进行限制,隔离关键字的运行环境;在关键字代码不符合预设语法规范的情况下结束关键字代码的运行,如此,在关键字代码运行异常时可以正确捕获到运行异常,及时发现关键字代码中的异常情况。

[0016] 本发明实施例的其它特征和优点将在随后的具体实施方式部分予以详细说明。

附图说明

[0017] 附图是用来提供对本发明实施例的进一步理解,并且构成说明书的一部分,与下面的具体实施方式一起用于解释本发明实施例,但并不构成对本发明实施例的限制。在附图中:

[0018] 图1是本发明一实施例提供的关键字机制运行方法的流程图;

[0019] 图2是本发明另一实施例提供的关键字机制运行方法的流程图;

[0020] 图3是本发明另一实施例提供的关键字机制运行方法的逻辑示意图;以及

[0021] 图4是本发明另一实施例提供的关键字机制运行装置的结构框图。

[0022] 附图标记说明

[0023] 1 关键字代码确定模块 2 安全沙箱创建模块

[0024] 3 验证模块 4 处理模块

具体实施方式

[0025] 以下结合附图对本发明实施例的具体实施方式进行详细说明。应当理解的是,此处所描述的具体实施方式仅用于说明和解释本发明实施例,并不用于限制本发明实施例。

[0026] 本发明实施例的一个方面提供一种关键字机制运行方法。

[0027] 图1是本发明一实施例提供的关键字机制运行方法的流程图。如图1所示,该关键字机制运行方法包括以下内容。

[0028] 在步骤S10中,确定待被测试的接口中的关键字对应的关键字代码。用户在接口测试平台创建接口,需要使用关键字的地方设置了关键字,在该步骤中确定出设置的关键字对应的关键字代码。

[0029] 在步骤S11中,将所获取的关键字代码的运行范围限制在第一预设安全沙箱内。例如,创建第一预设安全沙箱,将所获取的关键字代码与第一预设安全沙箱关联,例如,使用反射技术实现关联,以实现将所获取的关键字代码的运行范围限制在第一预设安全沙箱内。可选地,第一预设安全沙箱可以是作用域或类。

[0030] 在步骤S12中,在第一预设安全沙箱内运行所获取的关键字代码时,验证所获取的关键字代码是否符合预设语法规范,若是,则执行步骤S13;若否,则执行步骤S14。其中,预设语法规范对关键字代码做限制,例如,对关键字代码包含的内容和/或者形式做限制,说明哪些内容和/或形式是可以的,哪些内容和/或形式是不可以的,预设语法规范可以根据具体情况进行设置。若关键字代码符合预设语法规范,则可以运行关键字代码;若关键字代码不符合预设语法规范,则结束关键字代码的运行,如此,可以在关键字代码中包含异常内容时,及时发现,及时处理。例如,关键字代码中包括1/0,预设语法规范中说明1/0是不可以的,则1/0不符合预设语法规范,则结束关键字代码的运行,及时发现关键字代码中的异常情况。

[0031] 在步骤S13中,继续运行所获取的关键字代码。

[0032] 在步骤S14中,结束所获取的关键字代码的运行。

[0033] 通过上述技术方案,将关键字代码的运行范围限制在安全沙箱内,如此,对关键字

代码的运行进行隔离,对关键字代码的运行范围进行限制,隔离关键字的运行环境;在关键字代码不符合预设语法规范的情况下结束关键字代码的运行,如此,在关键字代码运行异常时可以正确捕获到运行异常,及时发现关键字代码中的异常情况。

[0034] 可选地,在本发明实施例中,可以根据以下内容确定待被测试的接口的关键字对应的关键字代码。从预设关键字数据库中获取关键字对应的关键字字符串;以及执行关键字字符串,将关键字字符串转换成关键字代码,以确定待被测试的接口中的关键字对应的关键字代码。例如,使用eval或exec执行关键字字符串,以将关键字字符串转换成关键字代码。其中,在本发明实施例中,可以通过以下内容从预设关键字数据库中获取关键字对应的关键字字符串。用户在接口测试平台创建接口,在需要使用关键字的地方设置关键字,例如,可以通过使用某种形式来表示此处是关键字,例如,采用${}包含关键字名称与参数来表示关键字,例如,${sign(request,secret)},为一关键字。用户在接口测试平台触发接口运行,接口被调用。获取接口的接口数据。扫描接口数据,若接口数据中某处是表示关键字形式的数据,则认为可以是关键字。例如,采用${}包含关键字名称与参数来表示关键字,例如,${sign(request,secret)},sign为关键字名称,request和secret为参数。若接口数据中的某处是${sign(request,secret)}类型的数据,则认为此处是关键字。需要说明的是${sign(request,secret)}仅仅是为了说明关键字的形式而列举的示例。具体地,在扫描接口数据时,基于正则匹配规则扫描接口数据,以确定接口中的关键字。例如,若关键字采用${sign(request,secret)}形式来表示,匹配表达式可以是r'\$\{def\s+(.+?)\(\([\w+?|,]\)\)\},匹配出${sign(request,secret)}这种形式的地方认为是关键字。其中,在扫描时,第一个扫描结果为关键字名“sign”,第二个扫描结果为关键字参数“request,secret”。若扫描到类似于${sign(request,secret)}形式的数据,则扫描成功,匹配到关键字,返回关键字名称和参数;若没有扫描到类似于${sign(request,secret)}形式的数据,则接口数据中没有关键字,直接执行接口数据,结束流程。在从接口数据中扫描到关键字的情况下,获取到关键字名称和参数,判断关键字名称是否存在在预设关键字数据库中,例如,通过查询关键字数据库,来确定获取到的关键字名称是否存在在数据库中。若获取到的关键字名称存在在预设关键字数据库中,则在预设关键字数据库中查询到关键字名称对应的关键字字符串,以获取到接口数据中的关键字对应的关键字字符串。此外,除了可以获取到关键字字符串以外,还可以获取到运行阶段状态参数,运行阶段状态参数表明了其对应的关键字字符串是否可以启用。

[0035] 可选地,在本发明实施例中,在执行关键字字符串将关键字字符串转换成关键字代码之前,还可以先判断所获取的关键字字符串是否是恶意代码字符串,其中,执行关键字字符串将关键字字符串转换成关键字代码的条件为所获取的关键字符串不是恶意代码字符串。例如,可以采用黑名单机制判断是否是恶意代码字符串。具体地,将恶意代码字符串存储在黑名单中,例如,一个恶意代码字符串写一行。加载黑名单,将黑名单中的数据项逐项与获取到的关键字字符串进行比对,若黑名单中的某一项数据项或者某几项数据项存在在获取到的关键字字符串中,则认为获取到的关键字字符串是恶意代码字符串,不能执行将关键字字符串转换成关键字代码的操作;若黑名单中的数据项均不在获取到的关键字字符串中,则认为获取到的关键字字符串不是恶意代码字符串,可以执行将关键字字符串转换成关键字代码的操作。

[0036] 图2是本发明另一实施例提供的关键字机制运行方法的流程图。其中,步骤S23-S26与图1的步骤S11-S14是相同的,与图1所示方法的不同之处在于,图2所示的方法还包括以下内容。

[0037] 在步骤S20中,从预设关键字数据库中获取关键字对应的关键字字符串,例如,可以参照上述实施例中所述的方法获取关键字字符串。

[0038] 在步骤S21中,判断所获取的关键字字符串是否是恶意代码字符串,若是,则舍弃掉获取的关键字字符串,继续步骤S20;若不是,则执行步骤S22。

[0039] 在步骤S22中,执行关键字字符串,将关键字字符串转换成所述关键字代码,以确定待被测试的接口中的关键字对应的关键字代码。

[0040] 可选地,在本发明实施例中,可以基于以下内容创建预设关键字数据库。具体地,用户编写关键字代码,基于用户编写的关键字代码创建预设关键字数据库。例如,用户在某页面编写关键字代码,编写完成后提交,则可以接收到用户编写的编写关键字代码,随后将编写关键字代码转换成字符串,编写关键字字符串,从而可以接收到被编写的编写关键字代码转换的编写关键字字符串。然后,进行安全判定,也就是判断编写关键字字符串是否是恶意代码字符串,例如,参照上述实施例中所述的方法来进行判断。在编写关键字字符串是恶意代码字符串的情况下,通知用户,以使得用户修改其编写的关键字代码,例如,可以通过在页面显示的方式来通知用户。在编写关键字字符串不是恶意代码字符串的情况下,执行编写关键字字符串,以将编写关键字字符串转换成对应的编写关键字代码,例如,使用eval或exec执行编写关键字字符串来实现。将编写关键字代码的运行范围限制在第二预设安全沙箱内,具体地,可以参照上述实施例中所述的方式。可选地,第二预设安全沙箱可以是作用域或类。在第二预设安全沙箱内运行编写关键字代码时,验证编写关键字代码是否符合预设语法规范。在编写关键字代码符合预设语法规范的情况下,在第二预设安全沙箱内继续运行编写关键字代码,最终编写关键字代码运行成功,将编写关键字字符串存储在数据库中,以构建预设关键字数据库。若编写关键字代码不符合预设语法规范,则编写关键字代码运行失败,通知用户修改其编写的关键字代码。在将编写关键字字符串存储在数据库中后,也可以通知用户,也就是,在用户编写的代码通过安全判定与运行时检查(是否符合预设语法规范)时,将关键字字符串存储到数据库,并通知用户。

[0041] 图3是本发明另一实施例提供的关键字机制运行方法的逻辑示意图。下面结合图3对本发明实施例提供的关键字机制运行方法进行示例性介绍。其中,在该实施例中,方法包括两个方面,关键字创建和关键字运行。

[0042] 首先是关键字创建,也就是构建预设关键字数据库。用户编写关键字代码,基于用户编写的关键字代码创建预设关键字数据库。例如,用户在某页面编写关键字代码,编写完成后提交,则可以接收到用户编写的编写关键字代码,随后将编写关键字代码转换成字符串,编写关键字字符串,从而可以接收到被编写的编写关键字代码转换的编写关键字字符串。然后,进行安全判定,也就是判断编写关键字字符串是否是恶意代码字符串,例如,参照上述实施例中所述的方法来进行判断。在编写关键字字符串是恶意代码字符串的情况下,通知用户,以使得用户修改其编写的关键字代码,例如,可以通过在页面显示的方式来通知用户。在编写关键字字符串不是恶意代码字符串的情况下,执行编写关键字字符串,以将编写关键字字符串转换成对应的编写关键字代码,例如,使用eval或exec执行编写关键字字

符串来实现。将编写关键字代码的运行范围限制在第二预设安全沙箱内,具体地,可以参照上述实施例中所述的方式。在第二预设安全沙箱内运行编写关键字代码时,验证编写关键字代码是否符合预设语法规范。在编写关键字代码符合预设语法规范的情况下,在第二预设安全沙箱内继续运行编写关键字代码,最终编写关键字代码运行成功,将编写关键字字符串存储在数据库中,以构建预设关键字数据库。若编写关键字代码不符合预设语法规范,则编写关键字代码运行失败,通知用户修改其编写的关键字代码。在将编写关键字字符串存储在数据库中后,也可以通知用户,也就是,在用户编写的代码通过安全判定与运行时检查(是否符合预设语法规范)时,将关键字字符串存储到数据库,并通知用户。

[0043] 其次是关键字运行。用户在接口测试平台创建接口,在需要使用关键字的地方设置关键字,例如,可以通过使用某种形式来表示此处是关键字,例如,采用${}包含关键字名称与参数来表示关键字,例如,${sign(request,secret)},为一关键字。用户在接口测试平台触发接口运行,接口被调用。获取接口的接口数据。扫描接口数据,若接口数据中某处是表示关键字形式的数据,则认为可以是关键字。例如,采用${}包含关键字名称与参数来表示关键字,例如,${sign(request,secret)},sign为关键字名称,request和secret为参数。若接口数据中的某处是${sign(request,secret)}类型的数据,则认为此处是关键字。需要说明的是${sign(request,secret)}仅仅是为了说明关键字的形式而列举的示例。具体地,在扫描接口数据时,基于正则匹配规则扫描接口数据,以确定接口中的关键字。例如,若关键字采用${sign(request,secret)}形式来表示,匹配表达式可以是r'\$\{def\s+(.+?)\(\([\w+?|,]\)\)\},匹配出${sign(request,secret)}这种形式的地方认为是关键字。其中,在扫描时,第一个扫描结果为关键字名“sign”,第二个扫描结果为关键字参数“request,secret”。若扫描到类似于${sign(request,secret)}形式的数据,则扫描成功,匹配到关键字,返回关键字名称和参数;若没有扫描到类似于${sign(request,secret)}形式的数据,则接口数据中没有关键字,直接执行接口数据,结束流程。在从接口数据中扫描到关键字的情况下,获取到关键字名称和参数,也就是确定到接口中的关键字的名称。判断关键字的名称是否存在在预设关键字数据库中,例如,通过查询关键字数据库,来确定获取到的关键字名称是否存在在数据库中。若获取到的关键字名称存在在预设关键字数据库中,则在预设关键字数据库中查询到关键字名称对应的关键字字符串,以获取到接口数据中的关键字对应的关键字字符串。此外,除了可以获取到关键字字符串以外,还可以获取到运行阶段状态参数,运行阶段状态参数表明了其对应的关键字字符串是否可以启用。若获取到的关键字的名称不在预设关键字数据库中,则执行出错,结束流程。判断获取到的关键字字符串是否是恶意代码字符串,例如,可以参照上述实施例中所述的方法进行判断。若是恶意代码字符串则流程结束,若不是恶意代码字符串则判断获取到的运行阶段状态参数是否是启用。在获取到的运行阶段状态参数不是启用的情况下,流程结束;在获取到的运行阶段状态参数是启用的情况下,执行获取到的关键字字符串,将关键字字符串转换成关键字代码,例如,使用eval或exec执行关键字字符串。可选地,在本发明实施例中,可以先判断是否是恶意代码字符串,再判断运行阶段状态参数是否是启用;也可以先判断运行阶段状态参数是否是启用,再判断是否是恶意代码字符串,对此,不用于限制本发明。创建第一预设安全沙箱,将关键字代码与第一预设安全沙箱关联,例如,使用反射技术实现关联,以实现将关键字代码的运行范围限制在第一预设安全沙箱内。可选地,第一预设安全沙箱可以是

作用域或类。运行关键字代码前将关键字代码封装到作用域或类对象中,限制关键字代码运行作用域或类对象为子类型,将关键字代码的运行限制到局部,避免关键字代码污染全局命名空间或平台命名空间。在第一预设安全沙内运行关键字代码时,验证关键字代码是否符合预设语法规范,若是,则继续运行关键字代码;若否,则结束流程。执行完关键字代码,返回执行结果,替换原有关键字声明。

[0044] 本发明实施例中的技术方案主要包括两点内容。一个是关键字字符串安全审查,判断关键字字符串是否是恶意代码字符串,匹配关键字字符串中潜在的安全问题并进行拦截,例如执行系统调用指令“rm-rf/”。另一个是隔离关键字代码运行环境,建立安全沙箱,通过使用作用域或类对关键字代码的运行进行包装,使关键字代码的运行限制到局部,并通过异常处理机制捕获关键字代码触发的异常,其中,异常处理机制为判断是否符合预设语法规范。本发明实施例中的技术方案可以有效解决关键字机制带来的安全问题,对关键字运行的范围进行限制,同时隔离关键字运行环境。

[0045] 相应地,本发明实施例的另一方面提供一种关键字机制运行装置。

[0046] 图4是本发明另一实施例提供的一种关键字机制运行装置。如图4所示该装置包括关键字代码确定模块1、安全沙箱创建模块2、验证模块3和处理模块4。其中,关键字代码确定模块1用于确定待被测试的接口中的关键字对应的关键字代码;安全沙箱创建模块2用于将所获取的关键字代码的运行范围限制在第一预设安全沙箱内;验证模块3用于在第一预设安全沙箱内运行所获取的关键字代码时,验证所获取的关键字代码是否符合预设语法规范;处理模块4用于在所获取的关键字代码不符合预设语法规范的情况下,结束所获取的关键字代码的运行。

[0047] 可选地,在本发明实施例中,关键字代码确定模块确定待被测试的接口中的关键字对应的关键字代码包括:从预设关键字数据库中获取关键字对应的关键字字符串;以及执行关键字字符串,将关键字字符串转换成关键字代码,以确定待被测试的接口中的关键字对应的关键字代码。

[0048] 可选地,在本发明实施例中,该装置还包括:判断模块,用于在执行关键字字符串将关键字字符串转换成关键字代码之前,判断所获取的关键字字符串是否是恶意代码字符串,其中,执行所述关键字字符串将关键字字符串转换成关键字代码的条件为所获取的关键字符串不是恶意代码字符串。

[0049] 可选地,在本发明实施例中,预设关键字数据库基于以下内容被创建:接收被编写的编写关键字代码转换的编写关键字字符串;判断编写关键字字符串是否是恶意代码字符串;在编写关键字字符串不是恶意代码字符串的情况下,执行编写关键字字符串,以将编写关键字字符串转换成对应的编写关键字代码;将编写关键字代码的运行范围限制在第二预设安全沙箱内;在第二预设安全沙箱内运行编写关键字代码时,验证编写关键字代码是否符合预设语法规范;以及在编写关键字代码符合预设语法规范的情况下,将编写关键字字符串存储在数据库中,以构建预设关键字数据库。

[0050] 本发明实施例提供的关键字机制运行装置的具体工作原理及益处与本发明实施例提供的关键字机制运行方法的具体工作原理及益处相似,这里将不再赘述。

[0051] 所述关键字机制运行装置包括处理器和存储器,上述关键字代码确定模块、安全沙箱创建模块、验证模块和处理模块等均作为程序单元存储在存储器中,由处理器执行存

储在存储器中的上述程序单元来实现相应的功能。

[0052] 处理器中包含内核,由内核去存储器中调取相应的程序单元。内核可以设置一个或以上,通过调整内核参数来对关键字代码的运行进行隔离,对关键字代码的运行范围进行限制,隔离关键字的运行环境;在关键字代码运行异常时可以正确捕获到运行异常,及时发现关键字代码中的异常情况。

[0053] 存储器可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM),存储器包括至少一个存储芯片。

[0054] 本发明实施例提供了一种机器可读存储介质,其上存储有程序,该程序被处理器执行时实现上述实施例中所述的关键字机制运行方法。

[0055] 本发明实施例提供了一种处理器,所述处理器用于运行程序,其中,所述程序运行时执行上述实施例中所述的关键字机制运行方法。

[0056] 本发明实施例提供了一种电子设备,电子设备包括处理器、存储器及存储在存储器上并可在处理器上运行的程序,处理器执行程序时实现以下步骤:确定待被测试的接口中的关键字对应的关键字代码;将所获取的关键字代码的运行范围限制在第一预设安全沙箱内;在所述第一预设安全沙箱内运行所获取的关键字代码时,验证所获取的关键字代码是否符合预设语法规范;以及在所获取的关键字代码不符合预设语法规范的情况下,结束所获取的关键字代码的运行;所述确定待被测试的接口中的关键字对应的关键字代码包括:从预设关键字数据库中获取所述关键字对应的关键字字符串;以及执行所述关键字字符串,将所述关键字字符串转换成所述关键字代码,以确定待被测试的接口中的关键字对应的关键字代码;在执行所述关键字字符串将所述关键字字符串转换成所述关键字代码之前,该方法还包括:判断所获取的关键字字符串是否是恶意代码字符串,其中,所述执行所述关键字字符串将所述关键字字符串转换成所述关键字代码的条件为所获取的关键字符串不是恶意代码字符串;所述预设关键字数据库基于以下内容被创建:接收被编写的编写关键字代码转换的编写关键字字符串;判断所述编写关键字字符串是否是所述恶意代码字符串;在所述编写关键字字符串不是所述恶意代码字符串的情况下,执行所述编写关键字字符串,以将所述编写关键字字符串转换成对应的编写关键字代码;将所述编写关键字代码的运行范围限制在第二预设安全沙箱内;在所述第二预设安全沙箱内运行所述编写关键字代码时,验证所述编写关键字代码是否符合所述预设语法规范;以及在所述编写关键字代码符合所述预设语法规范的情况下,将所述编写关键字字符串存储在数据库中,以构建所述预设关键字数据库。本文中的电子设备可以是服务器、PC、PAD、手机等。

[0057] 本申请还提供了一种计算机程序产品,当在数据处理设备上执行时,适于执行初始化有如下方法步骤的程序:确定待被测试的接口中的关键字对应的关键字代码;将所获取的关键字代码的运行范围限制在第一预设安全沙箱内;在所述第一预设安全沙箱内运行所获取的关键字代码时,验证所获取的关键字代码是否符合预设语法规范;以及在所获取的关键字代码不符合预设语法规范的情况下,结束所获取的关键字代码的运行;所述确定待被测试的接口中的关键字对应的关键字代码包括:从预设关键字数据库中获取所述关键字对应的关键字字符串;以及执行所述关键字字符串,将所述关键字字符串转换成所述关键字代码,以确定待被测试的接口中的关键字对应的关键字代码;在执行所述关键字字符

串将所述关键字字符串转换成所述关键字代码之前,该方法还包括:判断所获取的关键字字符串是否是恶意代码字符串,其中,所述执行所述关键字字符串将所述关键字字符串转换成所述关键字代码的条件为所获取的关键字符串不是恶意代码字符串;所述预设关键字数据库基于以下内容被创建:接收被编写的编写关键字代码转换的编写关键字字符串;判断所述编写关键字字符串是否是所述恶意代码字符串;在所述编写关键字字符串不是所述恶意代码字符串的情况下,执行所述编写关键字字符串,以将所述编写关键字字符串转换成对应的编写关键字代码;将所述编写关键字代码的运行范围限制在第二预设安全沙箱内;在所述第二预设安全沙箱内运行所述编写关键字代码时,验证所述编写关键字代码是否符合所述预设语法规范;以及在所述编写关键字代码符合所述预设语法规范的情况下,将所述编写关键字字符串存储在数据库中,以构建所述预设关键字数据库。

[0058] 本领域内的技术人员应明白,本申请的实施例可提供为方法、系统、或计算机程序产品。因此,本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0059] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0060] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0061] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0062] 在一个典型的配置中,计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0063] 存储器可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM)。存储器是计算机可读介质的示例。

[0064] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、

数字多功能光盘(DVD)或其他光学存储、磁盒式磁带,磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体(transitory media),如调制的数据信号和载波。

[0065] 还需要说明的是,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0066] 以上仅为本申请的实施例而已,并不用于限制本申请。对于本领域技术人员来说,本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等,均应包含在本申请的权利要求范围之内。

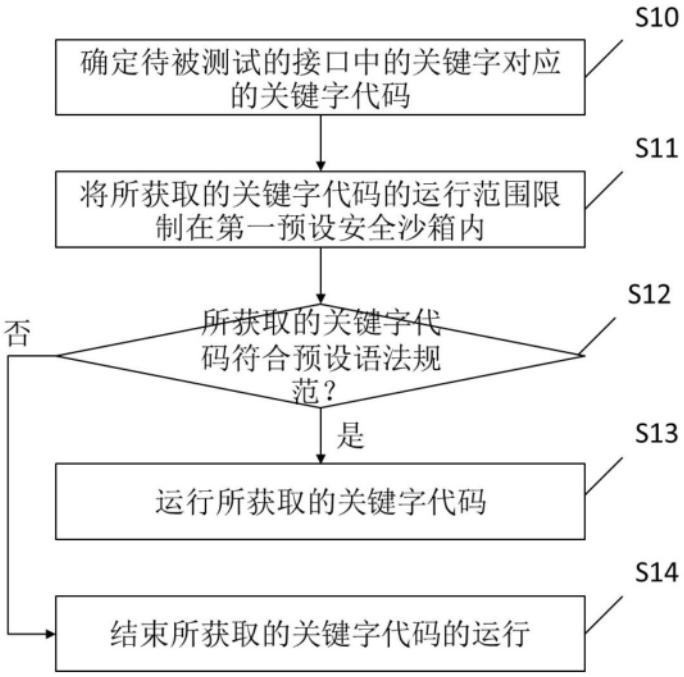

S10
确定待被测试的接口中的关键字对应的关键字代码
S11
将所获取的关键字代码的运行范围限制在第一预设安全沙箱内
S12
所获取的关键字代码符合预设语法规范？
否
是
S13
运行所获取的关键字代码
S14
结束所获取的关键字代码的运行

图1

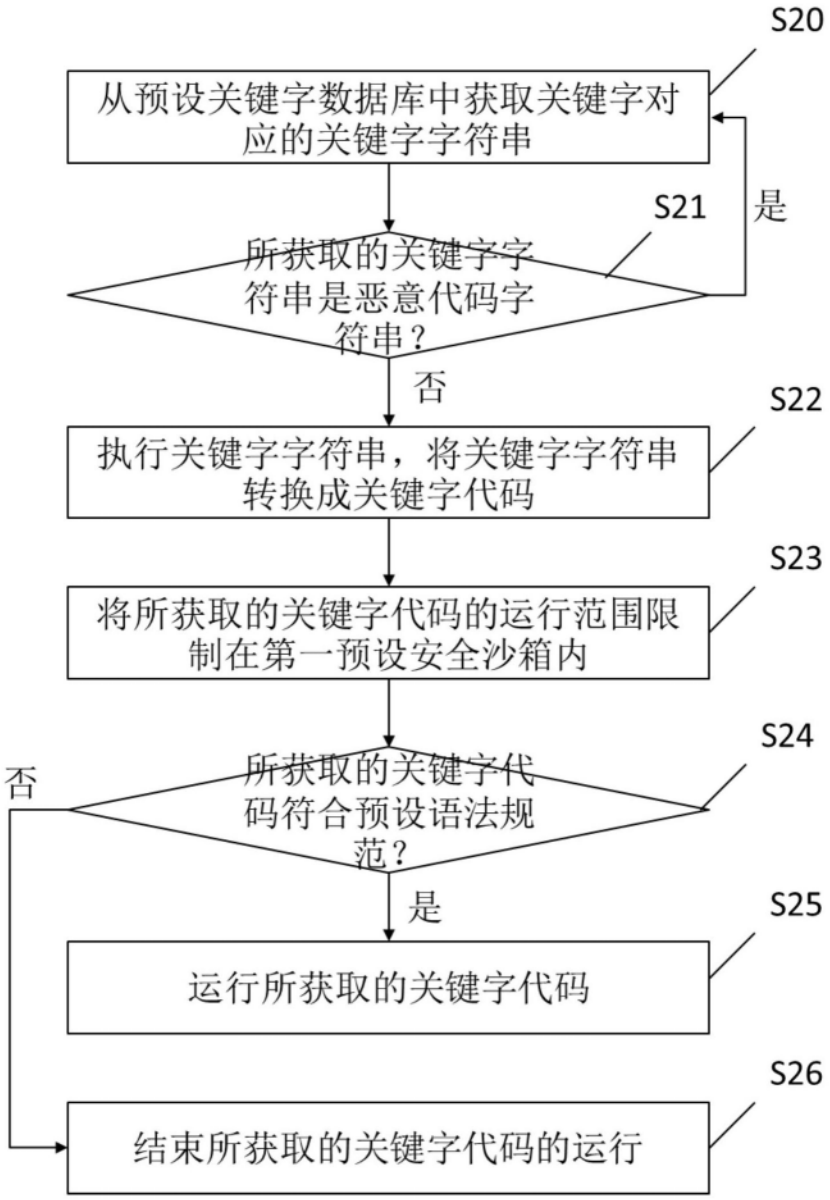

S20
从预设关键字数据库中获取关键字对应的关键字字符串
S21
所获取的关键字字符串是恶意代码字符串？
是
否
S22
执行关键字字符串，将关键字字符串转换成关键字代码
S23
将所获取的关键字代码的运行范围限制在第一预设安全沙箱内
S24
所获取的关键字代码符合预设语法规范？
否
是
S25
运行所获取的关键字代码
S26
结束所获取的关键字代码的运行

图2

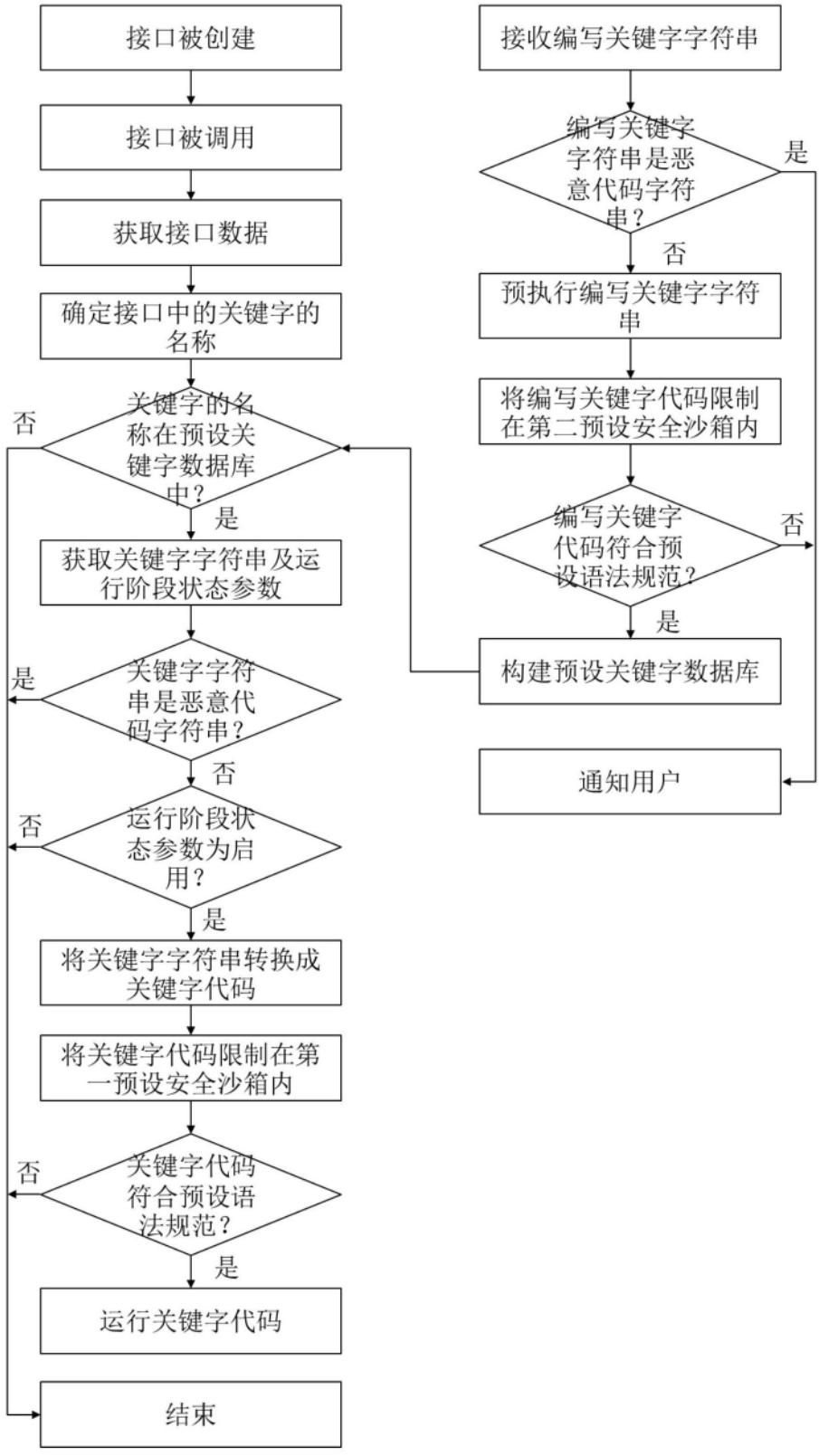

接口被创建
接口被调用
获取接口数据
确定接口中的关键字的名称
关键字的名称在预设关键字数据库中？
否
是
获取关键字字符串及运行阶段状态参数
关键字字符串是恶意代码字符串？
是
否
运行阶段状态参数为启用？
否
是
将关键字字符串转换成关键字代码
将关键字代码限制在第一预设安全沙箱内
关键字代码符合预设语法规范？
否
是
运行关键字代码
结束
接收编写关键字字符串
编写关键字字符串是恶意代码字符串？
是
否
预执行编写关键字字符串
将编写关键字代码限制在第二预设安全沙箱内
编写关键字代码符合预设语法规范？
否
是
构建预设关键字数据库
通知用户

图3

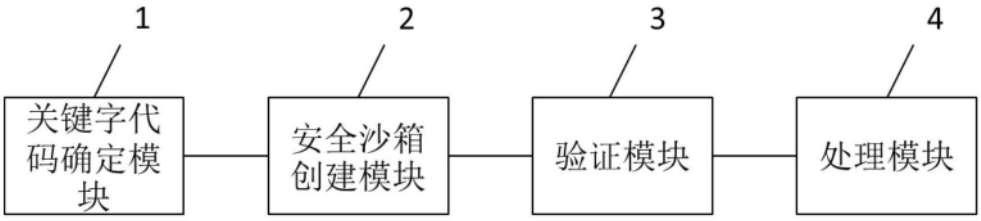


图4