(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111104675 A
(43)申请公布日 2020.05.05

(21)申请号 201911118880.1

(22)申请日 2019.11.15

(71)申请人 泰康保险集团股份有限公司
地址 100031 北京市西城区复兴门内大街156号泰康人寿大厦

(72)发明人 刘刚

(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 张效荣 王志远

(51)Int.Cl.
G06F 21/57(2013.01)

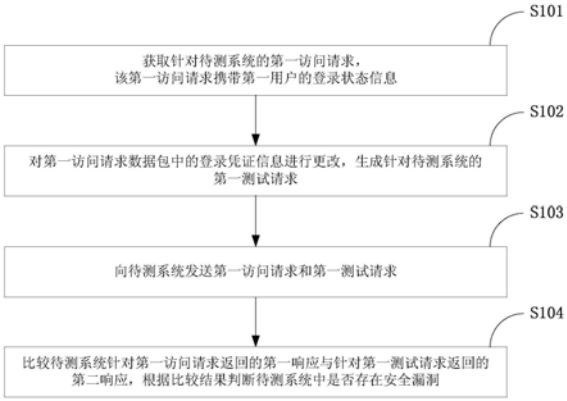
权利要求书2页 说明书8页 附图3页

(54)发明名称

系统安全漏洞的检测方法和装置

(57)摘要

本发明公开了一种系统安全漏洞的检测方法和装置，涉及计算机技术领域。该方法的一具体实施方式包括：获取针对待测系统的第一访问请求，该第一访问请求携带第一用户的登录状态信息；对第一访问请求数据包中的登录凭证信息进行更改，生成针对待测系统的第一测试请求；向待测系统发送第一访问请求和第一测试请求；比较待测系统针对第一访问请求返回的第一响应与针对第一测试请求返回的第二响应，根据比较结果判断待测系统中是否存在安全漏洞。该实施方式能够准确检测待测系统中存在的、因缺少对用户登录凭证进行验证而产生的安全漏洞。



CN 111104675 A

1.一种系统安全漏洞的检测方法,其特征在于,包括:

获取针对待测系统的第一访问请求,该第一访问请求携带第一用户的登录状态信息;

对第一访问请求数据包中的登录凭证信息进行更改,生成针对待测系统的第一测试请求;

向待测系统发送第一访问请求和第一测试请求;以及

比较待测系统针对第一访问请求返回的第一响应与针对第一测试请求返回的第二响应,根据比较结果判断待测系统中是否存在安全漏洞。

2.根据权利要求1所述的方法,其特征在于,所述对第一访问请求数据包中的登录凭证信息进行更改,包括:

将第一访问请求数据包中的登录凭证信息替换为预先存储的第二用户的登录凭证信息;或者

将第一访问请求数据包中的登录凭证信息删除。

3.根据权利要求1所述的方法,其特征在于,所述根据比较结果判断待测系统中是否存在安全漏洞,包括:

在第一响应携带的请求数据与第二响应携带的请求数据相同时,确定待测系统中存在安全漏洞。

4.根据权利要求1所述的方法,其特征在于,所述根据比较结果判断待测系统中是否存在安全漏洞,包括:

在第一响应携带的请求数据与第二响应携带的请求数据的格式相同时,确定待测系统中存在安全漏洞。

5.根据权利要求1所述的方法,其特征在于,所述根据比较结果判断待测系统中是否存在安全漏洞,包括:

在第一响应的数据包大小与第二响应的数据包大小的差值小于预设的第一阈值时,确定待测系统中存在安全漏洞。

6.根据权利要求4所述的方法,其特征在于,所述方法进一步包括:

在第一响应携带的请求数据与第二响应携带的请求数据的格式相同时,获取针对待测系统的第二访问请求,该第二访问请求携带第三用户的登录状态信息;

将第二访问请求数据包中的预设字段的信息替换为预先存储的第四用户的所述字段的信息,生成针对待测系统的第二测试请求;

向待测系统发送第二访问请求和第二测试请求;

比较待测系统针对第二访问请求返回的第三响应与针对第二测试请求返回的第四响应;以及

在第三响应携带的请求数据的格式与第四响应携带的请求数据的格式相同或者第三响应的数据包大小与第四响应的数据包大小差值小于预设的第二阈值时,确定待测系统中存在安全漏洞。

7.根据权利要求6所述的方法,其特征在于,所述字段包括:用户标识和/或当前业务标识。

8.一种系统安全漏洞的检测装置,其特征在于,包括:

请求获取单元,用于获取针对待测系统的第一访问请求,该第一访问请求携带第一用

户的登录状态信息；

请求构造单元，用于对第一访问请求数据包中的登录凭证信息进行更改，生成针对待测系统的第一测试请求；

请求发送单元，用于向待测系统发送第一访问请求和第一测试请求；

测试单元，用于比较待测系统针对第一访问请求返回的第一响应与针对第一测试请求返回的第二响应，根据比较结果判断待测系统中是否存在安全漏洞。

9.一种电子设备，其特征在于，包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序，

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求1-7中任一所述的方法。

10.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述程序被处理器执行时实现如权利要求1-7中任一所述的方法。

系统安全漏洞的检测方法和装置

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种系统安全漏洞的检测方法和装置。

背景技术

[0002] 现有的Web应用系统中往往存在一种或多种安全漏洞，例如由于系统缺少对用户相关权限的验证，没有权限的非法用户能够执行该权限内的业务功能，从而形成巨大的安全隐患。在目前的安全漏洞检测方法中，无论是手工检测还是自动化检测均存在检测准确性低的问题。

发明内容

[0003] 有鉴于此，本发明实施例提供一种系统安全漏洞的检测方法和装置，能够准确检测待测系统中存在的、因缺少对用户登录凭证进行验证而产生的安全漏洞。

[0004] 为实现上述目的，根据本发明的一个方面，提供了一种系统安全漏洞的检测方法。

[0005] 本发明实施例的系统安全漏洞的检测方法包括：获取针对待测系统的第一访问请求，该第一访问请求携带第一用户的登录状态信息；对第一访问请求数据包中的登录凭证信息进行更改，生成针对待测系统的第一测试请求；向待测系统发送第一访问请求和第一测试请求；比较待测系统针对第一访问请求返回的第一响应与针对第一测试请求返回的第二响应，根据比较结果判断待测系统中是否存在安全漏洞。

[0006] 可选地，所述对第一访问请求数据包中的登录凭证信息进行更改，包括：将第一访问请求数据包中的登录凭证信息替换为预先存储的第二用户的登录凭证信息；或者，将第一访问请求数据包中的登录凭证信息删除。

[0007] 可选地，所述根据比较结果判断待测系统中是否存在安全漏洞，包括：在第一响应携带的请求数据与第二响应携带的请求数据相同时，确定待测系统中存在安全漏洞。

[0008] 可选地，所述根据比较结果判断待测系统中是否存在安全漏洞，包括：在第一响应携带的请求数据与第二响应携带的请求数据的格式相同时，确定待测系统中存在安全漏洞。

[0009] 可选地，所述根据比较结果判断待测系统中是否存在安全漏洞，包括：在第一响应的数据包大小与第二响应的数据包大小的差值小于预设的第一阈值时，确定待测系统中存在安全漏洞。

[0010] 可选地，所述方法进一步包括：在第一响应携带的请求数据与第二响应携带的请求数据的格式相同时，获取针对待测系统的第二访问请求，该第二访问请求携带第三用户的登录状态信息；将第二访问请求数据包中的预设字段的信息替换为预先存储的第四用户的所述字段的信息，生成针对待测系统的第二测试请求；向待测系统发送第二访问请求和第二测试请求；比较待测系统针对第二访问请求返回的第三响应与针对第二测试请求返回的第四响应；在第三响应携带的请求数据的格式与第四响应携带的请求数据的格式相同或者第三响应的数据包大小与第四响应的数据包大小差值小于预设的第二阈值时，确定待测

系统中存在安全漏洞。

[0011] 可选地，所述字段包括：用户标识和/或当前业务标识。

[0012] 为实现上述目的，根据本发明的另一方面，提供了一种系统安全漏洞的检测装置。

[0013] 本发明实施例的系统安全漏洞的检测装置可包括：请求获取单元，用于获取针对待测系统的第一访问请求，该第一访问请求携带第一用户的登录状态信息；请求构造单元，用于对第一访问请求数据包中的登录凭证信息进行更改，生成针对待测系统的第一测试请求；请求发送单元，用于向待测系统发送第一访问请求和第一测试请求；测试单元，用于比较待测系统针对第一访问请求返回的第一响应与针对第一测试请求返回的第二响应，根据比较结果判断待测系统中是否存在安全漏洞。

[0014] 为实现上述目的，根据本发明的又一方面，提供了一种电子设备。

[0015] 本发明的一种电子设备包括：一个或多个处理器；存储装置，用于存储一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现本发明所提供的系统安全漏洞的检测方法。

[0016] 为实现上述目的，根据本发明的再一方面，提供了一种计算机可读存储介质。

[0017] 本发明的一种计算机可读存储介质，其上存储有计算机程序，所述程序被处理器执行时实现本发明所提供的系统安全漏洞的检测方法。

[0018] 根据本发明的技术方案，上述发明中的一个实施例具有如下优点或有益效果：通过获取携带正常用户登录状态信息的第一访问请求，将其中的登录凭证信息替换为其他用户的登录凭证信息或者删除从而生成第一测试请求，将二请求发送到待测系统并比较各自的响应信息，在返回数据相同、返回数据格式相同或者响应数据包大小接近时即可判定待检测系统中存在因缺少对登录凭证进行验证而产生的权限访问控制漏洞；在此基础上，还可进一步将正常用户发送的第二访问请求中的预设字段信息更改形成第二测试请求，并以类似的方式比较二请求响应从而检测系统是否存在因缺少对上述字段信息进行验证而产生的权限访问控制漏洞。以上步骤可通过编写测试脚本自动执行，从而具有较高的检测效率。

[0019] 上述的非惯用的可选方式所具有的进一步效果将在下文中结合具体实施方式加以说明。

附图说明

[0020] 附图用于更好地理解本发明，不构成对本发明的不当限定。其中：

[0021] 图1是本发明实施例中系统安全漏洞的检测方法的主要步骤示意图；

[0022] 图2是用于实现本发明实施例中系统安全漏洞的检测方法的架构示意图；

[0023] 图3是本发明实施例中系统安全漏洞的检测装置的组成部分示意图；

[0024] 图4是根据本发明实施例可以应用于其中的示例性系统架构图；

[0025] 图5是用来实现本发明实施例中系统安全漏洞的检测方法的电子设备结构示意图。

具体实施方式

[0026] 以下结合附图对本发明的示范性实施例做出说明，其中包括本发明实施例的各种

细节以助于理解，应当将它们认为仅仅是示范性的。因此，本领域普通技术人员应当认识到，可以对这里描述的实施例做出各种改变和修改，而不会背离本发明的范围和精神。同样，为了清楚和简明，以下的描述中省略了对公知功能和结构的描述。

[0027] 需要指出的是，在不冲突的情况下，本发明的实施例以及实施例中的技术特征可以相互结合。

[0028] 图1是根据本发明实施例中系统安全漏洞的检测方法的主要步骤示意图。

[0029] 如图1所示，本发明实施例的系统安全漏洞的检测方法可具体按照如下步骤执行：

[0030] 步骤S101：获取针对待测系统的第一访问请求，该第一访问请求携带第一用户的登录状态信息。

[0031] 在本步骤，第一用户登录状态信息可以是第一用户的登录信息(例如用户名、密码等)，也可以是表征用户已登录状态的会话标识(即Session ID)或者登录凭证(即Token)。实际应用中，以上登录状态信息可存储在访问请求数据包请求头的Cookie字段中。在本发明实施例中，第一用户包括以下即将介绍的第二用户、第三用户和第四用户(以上四个用户均为不同用户)均为能够正常访问待测系统(即能够接收到待测系统正常响应)的用户。具体应用中，可通过访问请求接入装置截取第一访问请求，也可通过获取第一用户的历史访问信息来构造第一访问请求。在获取第一访问请求之后，可检验第一访问请求在此前的测试过程中是否使用过以及能否被待测系统正常响应，若检验通过说明其为合格请求，可执行后续步骤。

[0032] 步骤S102：对第一访问请求数据包中的登录凭证信息进行更改，生成针对待测系统的第一测试请求。

[0033] 为了验证待测系统是否存在因缺少对用户登录凭证进行验证而产生的安全漏洞，在本步骤中可对正常请求(即第一访问请求)中的用户登录凭证进行更改生成第一测试请求并将二请求向待测系统发送。可以理解，如果待测系统不存在上述安全漏洞，则针对二请求的响应数据包必然存在较大差异；如果待测系统存在上述安全漏洞，则针对二请求的响应数据包可能区别较小甚至完全相同，因此可比较二请求的响应信息从而判断待测系统中是否存在上述安全漏洞。

[0034] 实际应用中，可以在第一访问请求的请求头数据的Cookie字段更改登录凭证信息。具体地，上述更改可以是将第一访问请求中的登录凭证信息替换为预先存储的第二用户的登录凭证信息，也可以是将第一访问请求数据包中的登录凭证信息删除。

[0035] 步骤S103：向待测系统发送第一访问请求和第一测试请求。

[0036] 步骤S104：比较待测系统针对第一访问请求返回的第一响应与针对第一测试请求返回的第二响应，根据比较结果判断待测系统中是否存在安全漏洞。

[0037] 在本步骤中，接收到第一响应与第二响应之后，可进行比较并根据以下策略判断待测系统中是否存在安全漏洞：如果第一响应携带的请求数据(即第一访问请求所请求的数据，例如，第一访问请求的目的是查询订单号时，待测系统返回的订单号信息即为请求数据)与第二响应携带的请求数据相同，则确定待测系统中存在安全漏洞；如果第一响应携带的请求数据与第二响应携带的请求数据的格式相同(例如都是13位数字，该格式可根据需求设置)，则确定待测系统中存在安全漏洞；如果第一响应数据包大小与第二响应数据包大小的差值小于预设的第一阈值(该阈值可根据需求设置，例如500个字节)时，则确定待测系

统中存在安全漏洞。

[0038] 通过以上设置，本发明即可判断待测系统是否存在因缺少对用户登录凭证的验证而产生的安全漏洞。进一步地，在本发明实施例中，可通过以下步骤判断待测系统是否存在因缺少对其它字段信息的验证而产生的安全漏洞，这些字段可以包括：用户标识、用户移动终端(如手机)号码、当前业务标识(例如当用户使用订单号查询订单状态时，订单号即为当前业务标识)。实际应用中，用户标识可存在于请求头的Cookie字段中，用户移动终端号码和当前业务标识可存在于请求正文中。

[0039] 具体地，在通过前述步骤未发现待检测系统的安全漏洞时，可首先获取携带第三用户登录状态信息的针对待测系统的第二访问请求。同样地，在获取第三访问请求之后，可检验第三访问请求在此前的测试过程中是否使用过以及能否被待测系统正常响应，若检验通过说明其为合格请求，可执行后续步骤。此后，可将第二访问请求数据包中的预设字段信息替换为预先存储的第四用户的上述字段信息或者将第二访问请求数据包中的预设字段信息删除，从而生成针对待测系统的第二测试请求。最后，将第二访问请求和第二测试请求向待测系统发送，并比较待测系统针对第二访问请求返回的第三响应与针对第二测试请求返回的第四响应。基于前述原因，可通过以下策略判断待测系统中是否存在因缺少对上述字段信息的验证而产生的安全漏洞。

[0040] 如果第三响应携带的请求数据与第四响应携带的请求数据相同，则确定待测系统中存在安全漏洞；如果第三响应携带的请求数据与第四响应携带的请求数据的格式相同，则确定待测系统中存在安全漏洞；如果第三响应数据包大小与第四响应数据包大小的差值小于预设的第二阈值(该阈值可与第一阈值相同或者不同)时，则确定待测系统中存在安全漏洞。

[0041] 通过上述设置，能够快速、准确地检测待测系统中存在的安全漏洞。图2是用于实现本发明实施例中系统安全漏洞的检测方法的架构示意图，如图2所示，在用于实施上述系统安全漏洞的检测方法的架构中，包括请求接入模块、规则管理维度模块、安全漏洞检测模块、任务处理调度模块以及结果统计输出模块，以下将分别说明每一模块的功能。

[0042] 在本发明实施例中，请求接入模块可用于记录用户终端与待测系统之间的访问请求，所有的请求数据包都经过该模块。该模块对用户终端发送的访问请求执行去重处理，并对请求中携带的参数进行分析。实际应用中，该模块可根据请求方法(如Get方法、Post方法等)、请求协议、请求Host(主机名)和/或请求URL(Uniform Resource Locator，统一资源定位符)执行上述去重处理和分析。可以理解，上文介绍的第一访问请求和第二访问请求可以从请求接入模块中获取。

[0043] 规则管理维护模块可用于维护系统所需的必要数据，这些数据包括用户登录凭证、超文本传输安全协议Https(Hypertext Transfer Protocol Secure)证书、数据匹配规则、数据匹配字段、host优先级等。可以理解，以上Https证书、数据匹配规则、数据匹配字段、host优先级均为执行特定业务所需的数据。需要说明的是，以上步骤中第二用户的登录凭证信息和第四用户的预设字段信息可从规则管理维护模块中获取。

[0044] 安全漏洞识别模块即为执行上文介绍的系统安全漏洞的检测方法的模块，其可从请求接入模块获取第一访问请求和第二访问请求，并从规则管理维护模块中获取第二用户的登录凭证信息和第四用户的预设字段信息从而生成第一测试请求和第二测试请求。

[0045] 任务处理调度模块可用于通过工作节点拉取相应的测试用例并对工作节点进行管理，还可用于分配预设数量的线程处理数据包的请求和响应任务，在当前的空闲线程减少到一定数量时，任务处理调度模块可自动新增线程。

[0046] 结果统计输出模块可用于将检测出的安全漏洞以及相关的请求包数据和响应包数据保存到数据库中便于后续分析，这些数据也可用于后续相关机器学习模型的训练、验证和测试。

[0047] 在本发明实施例的技术方案中，通过获取携带正常用户登录状态信息的第一访问请求，将其中的登录凭证信息替换为其他用户的登录凭证信息或者删除从而生成第一测试请求，将二请求发送到待测系统并比较各自的响应信息，在返回数据相同、返回数据格式相同或者响应数据包大小接近时即可判定待检测系统中存在因缺少对登录凭证进行验证而产生的权限访问控制漏洞；在此基础上，还可进一步将正常用户发送的第二访问请求中的预设字段信息更改形成第二测试请求，并以类似的方式比较二请求响应从而检测系统是否存在因缺少对上述字段信息进行验证而产生的权限访问控制漏洞。以上步骤可通过编写测试脚本自动执行，从而具有较高的检测效率。

[0048] 需要说明的是，对于前述的各方法实施例，为了便于描述，将其表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，某些步骤事实上可以采用其它顺序进行或者同时进行。此外，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是实现本发明所必须的。

[0049] 为便于更好的实施本发明实施例的上述方案，下面还提供用于实施上述方案的相关装置。

[0050] 请参阅图3所示，本发明实施例提供的系统安全漏洞的检测装置300可以包括：请求获取单元301、请求构造单元302、请求发送单元303以及测试单元304。

[0051] 其中，请求获取单元301可用于获取针对待测系统的第一访问请求，该第一访问请求携带第一用户的登录状态信息；请求构造单元302可用于对第一访问请求数据包中的登录凭证信息进行更改，生成针对待测系统的第一测试请求；请求发送单元303可用于向待测系统发送第一访问请求和第一测试请求；测试单元304可用于比较待测系统针对第一访问请求返回的第一响应与针对第一测试请求返回的第二响应，根据比较结果判断待测系统中是否存在安全漏洞。

[0052] 在本发明实施例中，请求构造单元302可进一步用于：将第一访问请求数据包中的登录凭证信息替换为预先存储的第二用户的登录凭证信息；或者，将第一访问请求数据包中的登录凭证信息删除。

[0053] 具体应用中，测试单元304可进一步用于：在第一响应携带的请求数据与第二响应携带的请求数据相同时，确定待测系统中存在安全漏洞。

[0054] 实际应用场景中，测试单元304可进一步用于：在第一响应携带的请求数据与第二响应携带的请求数据的格式相同时，确定待测系统中存在安全漏洞。

[0055] 在一些实施例中，测试单元304可进一步用于：在第一响应的数据包大小与第二响应的数据包大小的差值小于预设的第一阈值时，确定待测系统中存在安全漏洞。

[0056] 作为一个优选方案，所述装置300可进一步包括相关漏洞检测单元，其用于：在第

一响应携带的请求数据与第二响应携带的请求数据的格式相同时，获取针对待测系统的第二访问请求，该第二访问请求携带第三用户的登录状态信息；将第二访问请求数据包中的预设字段的信息替换为预先存储的第四用户的所述字段的信息，生成针对待测系统的第二测试请求；向待测系统发送第二访问请求和第二测试请求；比较待测系统针对第二访问请求返回的第三响应与针对第二测试请求返回的第四响应；在第三响应携带的请求数据的格式与第四响应携带的请求数据的格式相同或者第三响应的数据包大小与第四响应的数据包大小差值小于预设的第二阈值时，确定待测系统中存在安全漏洞。

[0057] 此外，在本发明实施例中，所述字段可包括：用户标识和/或当前业务标识。

[0058] 在本发明实施例的技术方案中，通过获取携带正常用户登录状态信息的第一访问请求，将其中的登录凭证信息替换为其他用户的登录凭证信息或者删除从而生成第一测试请求，将二请求发送到待测系统并比较各自的响应信息，在返回数据相同、返回数据格式相同或者响应数据包大小接近时即可判定待检测系统中存在因缺少对登录凭证进行验证而产生的权限访问控制漏洞；在此基础上，还可进一步将正常用户发送的第二访问请求中的预设字段信息更改形成第二测试请求，并以类似的方式比较二请求响应从而检测系统是否存在因缺少对上述字段信息进行验证而产生的权限访问控制漏洞。以上步骤可通过编写测试脚本自动执行，从而具有较高的检测效率。

[0059] 图4示出了可以应用本发明实施例的系统安全漏洞的检测方法或系统安全漏洞的检测装置的示例性系统架构400。

[0060] 如图4所示，系统架构400可以包括终端设备401、402、403，网络404和服务器405(此架构仅仅是示例，具体架构中包含的组件可以根据申请具体情况调整)。网络404用以在终端设备401、402、403和服务器405之间提供通信链路的介质。网络404可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

[0061] 用户可以使用终端设备401、402、403通过网络404与服务器405交互，以接收或发送消息等。终端设备401、402、403上可以安装有各种通讯客户端应用，例如安全漏洞检测类应用(仅为示例)。

[0062] 终端设备401、402、403可以是具有显示屏并且支持网页浏览的各种电子设备，包括但不限于智能手机、平板电脑、膝上型便携计算机和台式计算机等等。

[0063] 服务器405可以是提供各种服务的服务器，例如对用户利用终端设备401、402、403所操作的安全漏洞检测类应用提供支持的服务器(仅为示例)。服务器405可以对接收到的安全漏洞检测请求等进行处理，并将处理结果(例如检测结果--仅为示例)反馈给终端设备401、402、403。

[0064] 需要说明的是，本发明实施例所提供的系统安全漏洞的检测方法一般由服务器405执行，相应地，系统安全漏洞的检测装置一般设置于服务器405中。

[0065] 应该理解，图4中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和服务器。

[0066] 本发明还提供了一种电子设备。本发明实施例的电子设备包括：一个或多个处理器；存储装置，用于存储一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现本发明所提供的系统安全漏洞的检测方法。

[0067] 下面参考图5，其示出了适于用来实现本发明实施例的电子设备的计算机系统500

的结构示意图。图5示出的电子设备仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0068] 如图5所示，计算机系统500包括中央处理单元(CPU)501，其可以根据存储在只读存储器(ROM)502中的程序或者从存储部分508加载到随机访问存储器(RAM)503中的程序而执行各种适当的动作和处理。在RAM503中，还存储有计算机系统500操作所需的各种程序和数据。CPU501、ROM 502以及RAM 503通过总线504彼此相连。输入/输出(I/O)接口505也连接至总线504。

[0069] 以下部件连接至I/O接口505：包括键盘、鼠标等的输入部分506；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分507；包括硬盘等的存储部分508；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分509。通信部分509经由诸如因特网的网络执行通信处理。驱动器510也根据需要连接至I/O接口505。可拆卸介质511，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器510上，以便从其上读出的计算机程序根据需要被安装入存储部分508。

[0070] 特别地，根据本发明公开的实施例，上文的主要步骤图描述的过程可以被实现为计算机软件程序。例如，本发明实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序包含用于执行主要步骤图所示的方法的程序代码。在上述实施例中，该计算机程序可以通过通信部分509从网络上被下载和安装，和/或从可拆卸介质511被安装。在该计算机程序被中央处理单元501执行时，执行本发明的系统中限定的上述功能。

[0071] 需要说明的是，本发明所示的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本发明中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。在本发明中，计算机可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述任意合适的组合。计算机可读信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于：无线、电线、光缆、RF等等，或者上述的任意合适的组合。

[0072] 附图中的流程图和框图，图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际

上可以基本并行地执行，它们有时也可以按相反的顺序执行，这根据所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0073] 描述于本发明实施例中所涉及到的单元可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的单元也可以设置在处理器中，例如，可以描述为：一种处理器包括请求获取单元、请求构造单元和测试单元。其中，这些单元的名称在某种情况下并不构成对该单元本身的限定，例如，请求获取单元还可以被描述为“向请求构造单元提供第一访问请求的单元”。

[0074] 作为另一方面，本发明还提供了一种计算机可读介质，该计算机可读介质可以是上述实施例中描述的设备中所包含的；也可以是单独存在，而未装配入该设备中的。上述计算机可读介质承载有一个或者多个程序，当上述一个或者多个程序被该设备执行时，使得该设备执行的步骤包括：获取针对待测系统的第一访问请求，该第一访问请求携带第一用户的登录状态信息；对第一访问请求数据包中的登录凭证信息进行更改，生成针对待测系统的第一测试请求；向待测系统发送第一访问请求和第一测试请求；比较待测系统针对第一访问请求返回的第一响应与针对第一测试请求返回的第二响应，根据比较结果判断待测系统中是否存在安全漏洞。

[0075] 在本发明实施例的技术方案中，通过获取携带正常用户登录状态信息的第一访问请求，将其中的登录凭证信息替换为其他用户的登录凭证信息或者删除从而生成第一测试请求，将二请求发送到待测系统并比较各自的响应信息，在返回数据相同、返回数据格式相同或者响应数据包大小接近时即可判定待检测系统中存在因缺少对登录凭证进行验证而产生的权限访问控制漏洞；在此基础上，还可进一步将正常用户发送的第二访问请求中的预设字段信息更改形成第二测试请求，并以类似的方式比较二请求响应从而检测系统是否存在因缺少对上述字段信息进行验证而产生的权限访问控制漏洞。以上步骤可通过编写测试脚本自动执行，从而具有较高的检测效率。

[0076] 上述具体实施方式，并不构成对本发明保护范围的限制。本领域技术人员应该明白的是，取决于设计要求和其他因素，可以发生各种各样的修改、组合、子组合和替代。任何在本发明的精神和原则之内所作的修改、等同替换和改进等，均应包含在本发明保护范围之内。

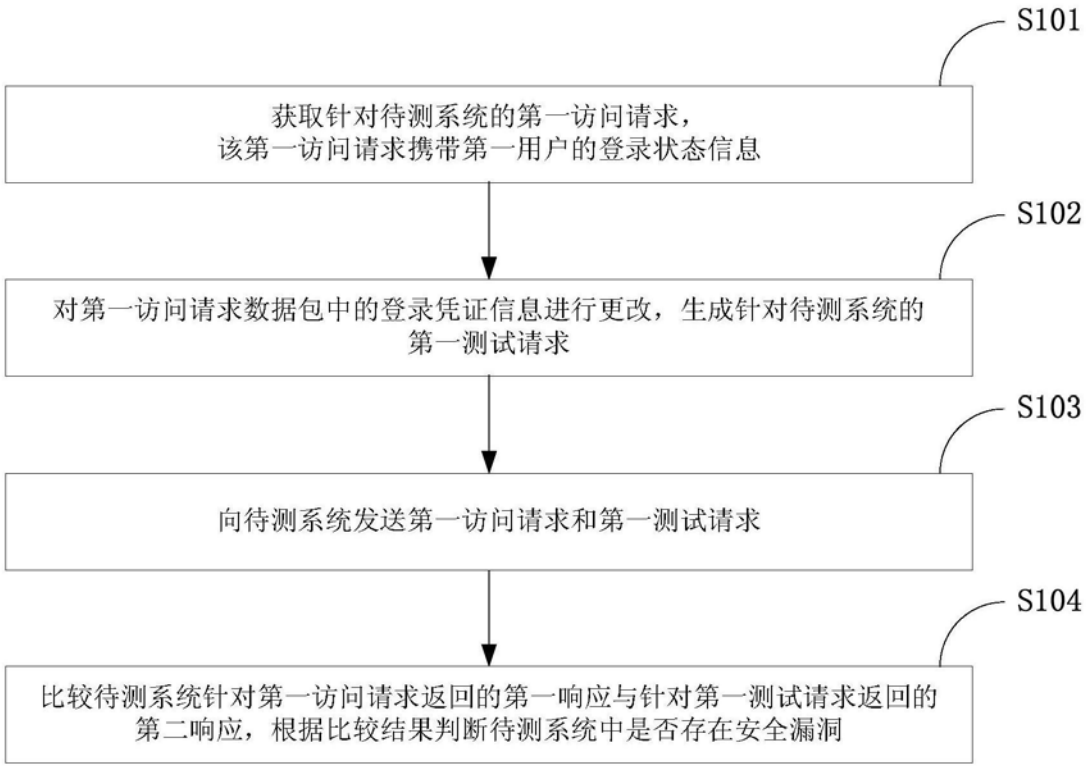

S101
获取针对待测系统的第一访问请求，
该第一访问请求携带第一用户的登录状态信息
S102
对第一访问请求数据包中的登录凭证信息进行更改，生成针对待测系统的
第一测试请求
S103
向待测系统发送第一访问请求和第一测试请求
S104
比较待测系统针对第一访问请求返回的第一响应与针对第一测试请求返回的
第二响应，根据比较结果判断待测系统中是否存在安全漏洞

图1

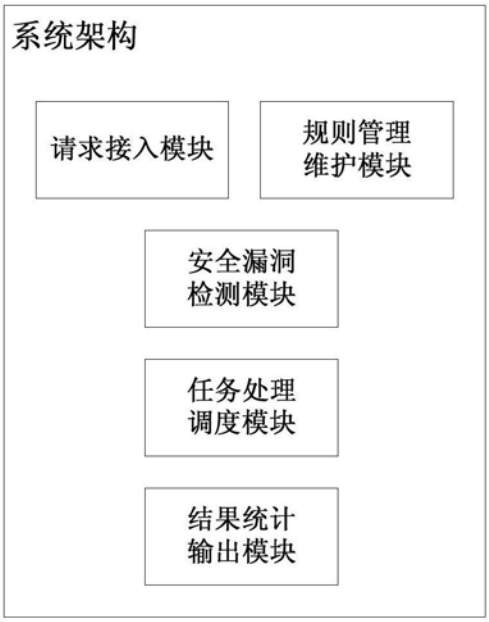

系统架构
请求接入模块
规则管理
维护模块
安全漏洞
检测模块
任务处理
调度模块
结果统计
输出模块

图2

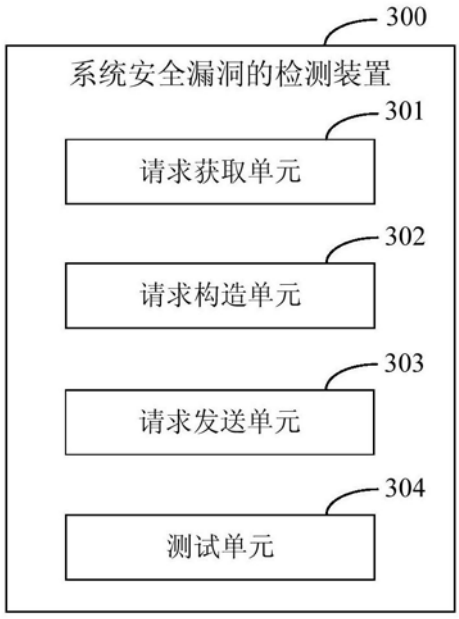

300
系统安全漏洞的检测装置
301
请求获取单元
302
请求构造单元
303
请求发送单元
304
测试单元

图3

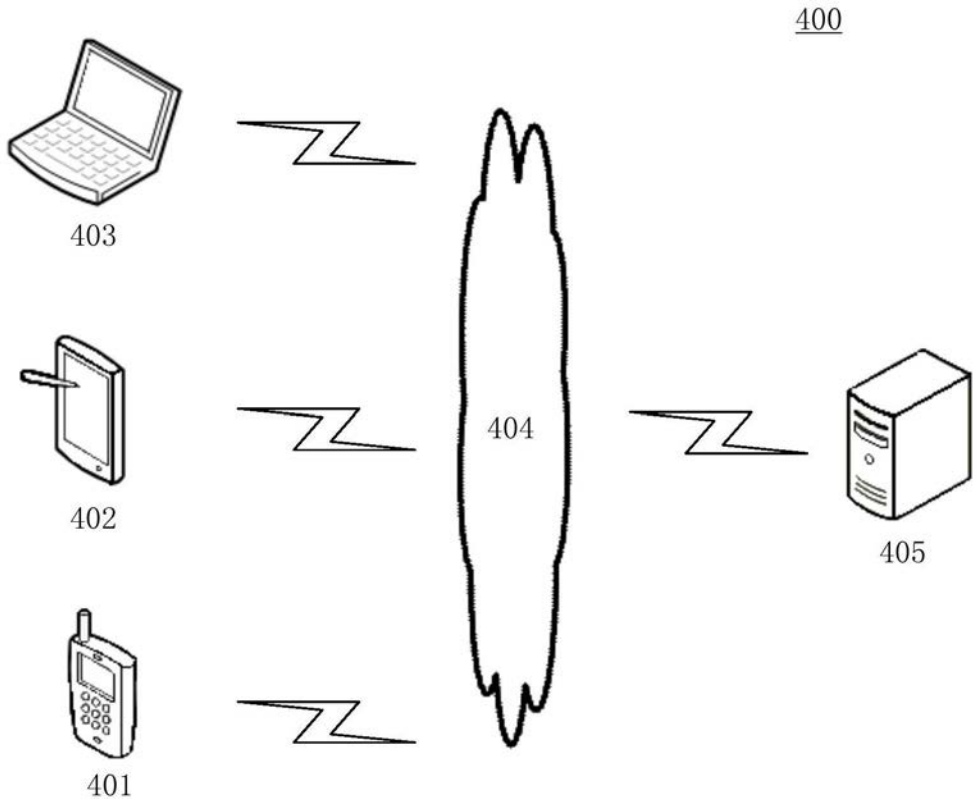

400
403
402
401
404
405

图4

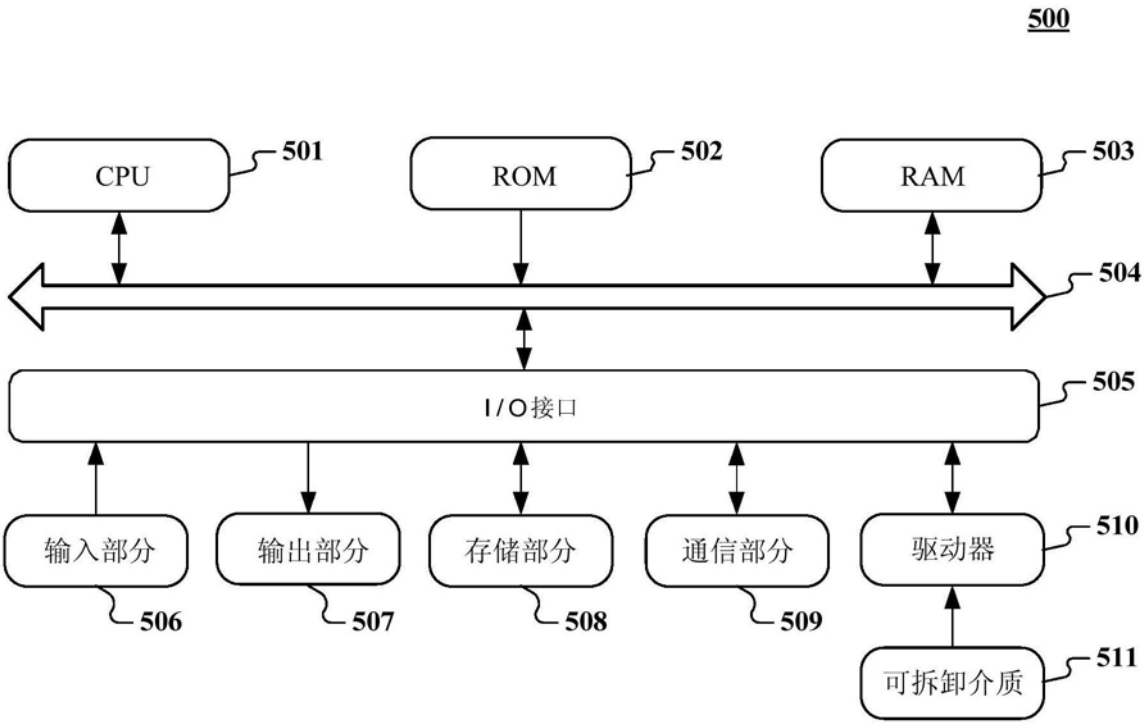

500
CPU
501
ROM
502
RAM
503
504
I/O接口
505
输入部分
506
输出部分
507
存储部分
508
通信部分
509
驱动器
510
可拆卸介质
511

图5