(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 11 月 26 日 (26.11.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/233022 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)

(21) 国际申请号: PCT/CN2019/118685

(22) 国际申请日: 2019 年 11 月 15 日 (15.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910425959.2 2019年5月21日 (21.05.2019) CN

(71) 申请人: 平安科技（深圳）有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518033 (CN)。

(72) 发明人: 王延辉 (WANG, Yanhui); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518033 (CN)。

张驰 (ZHANG, Chi); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518033 (CN)。

(74) 代理人: 北京市京大律师事务所 (BEIJING JINGDA LAW FIRM); 中国北京市海淀区海淀中街16号7层2单元703, Beijing 100080 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(54) **Title:** VULNERABILITY DETECTION METHOD AND APPARATUS, COMPUTER DEVICE, AND STORAGE MEDIUM

(54) **发明名称**: 漏洞检测方法、装置、计算机设备和存储介质

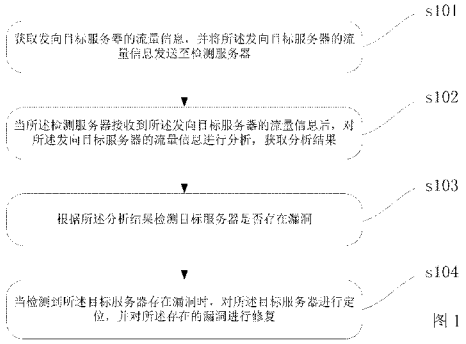

图 1

S101 Obtain traffic information sent to a target server, and send to a detection server said traffic information
S102 Upon receiving said traffic information, the detection server analyzes said traffic information to obtain an analysis result
S103 Detect whether vulnerability exists in the target server according to the analysis result
S104 If yes, locate the target server and fix the existing vulnerability

(57) **Abstract:** The present application relates to the field of information security. Disclosed are a vulnerability detection method and apparatus, a computer device, and a storage medium. The method comprises: obtaining traffic information sent to a target server, and sending to a detection server said traffic information; upon receiving said traffic information, the detection server analyzes said traffic information to obtain an analysis result; detect whether vulnerability exists in the target server according to the analysis result; and if yes, locate the target server and fix the existing vulnerability. In the present application, traffic information is obtained and sent to a detection server to perform analysis, so as to obtain a vulnerability detection result according to the analysis result, such that vulnerability detection can be effectively performed in different scenarios, and the detection efficiency is improved.

(57) **摘要**: 本申请涉及信息安全领域，本申请公开了一种漏洞检测的方法、装置、计算机设备和存储介质，所述方法包括：获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器；当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果；根据所述分析结果检测目标服务器是否存在漏洞；当检测到所述目标服务器存在漏洞时，对所述目标服务器进行定位，并对所述存在的漏洞进行修复。本申请通过获取流量信息，将所述流量信息发送至检测服务器进行分析，并根据分析结果获得漏洞检测结果，可以有效的对不同场景进行漏洞检测，提高检测效率。

WO 2020/233022 A1

[见续页]

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

漏洞检测方法、装置、计算机设备和存储介质

本申请要求于2019年05月21日提交中国专利局、申请号为201910425959.2、发明名称为“漏洞检测方法、装置、设备和存储介质”的中国专利申请的优先权，其全部内容通过引用结合在申请中。

技术领域

本申请涉及信息安全领域，特别涉及一种漏洞检测的方法、装置、计算机设备和存储介质。

背景技术

网站漏洞，随着B/S模式被广泛的应用，用这种模式编写Web应用程序的程序员也越来越多。发明人发现，由于开发人员的水平和经验参差不齐，相当一部分的开发人员在编写代码的时候，没有对用户的输入数据或者是页面中所携带的信息(如Cookie)进行必要的合法性判断，导致了攻击者可以利用这个编程漏洞来入侵数据库或者攻击Web应用程序的使用者，由此获得一些重要的数据和利益。

网站漏洞检测通常是指基于漏洞数据库，通过扫描等手段，对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用的漏洞的一种安全检测（渗透攻击）行为。

对于常规的漏洞扫描系统，对于web网站主要基于爬虫，在登录后页面以模拟登录或者填写cookie方式获取；当前主要问题有：目前网站都有防爬系统，模拟登录越来越难，cookie方式不是完全适用；此外，对于爬虫的全面性也一直是一个难点,支持web网站，但是对于手机app的网络连接无法检测。

发明内容

本申请的目的在于针对现有技术的不足，提供一种漏洞检测的方法、装置、计算机设备和存储介质，通过获取流量信息，将所述流量信息发送至检测服务器进行分析，并根据分析结果获得漏洞检测结果，可以有效的对不同场景进行漏洞检测，提高检测效率。

为达到上述目的，本申请的技术方案提供一种漏洞检测的方法、装置、计算机设备和存储介质。

本申请公开了一种漏洞检测的方法，包括以下步骤：

获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器；

当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果；

根据所述分析结果检测目标服务器是否存在漏洞；

当检测到所述目标服务器存在漏洞时，对所述目标服务器进行定位，并对所述存在的漏洞进行修复。

较佳地，所述获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器，包括：

在浏览器中设置插件，将所述插件与所述检测服务器进行关联，并通过所述浏览器中的插件获取访问各站点的超文本传输协议 HTTP 请求信息；

将所述超文本传输协议 HTTP 请求信息发送至与所述浏览器中的插件关联的检测服务器。

较佳地，所述获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器，包括：

设置超文本传输协议 HTTP 代理服务器，通过所述超文本传输协议 HTTP 代理服务器将浏览器的网络代理端口指向代理系统，将所述代理系统与所述检测服务器进行关联；

当获取到网络流量信息时，通过所述代理系统将所述网络流量信息发送至与所述代理系统关联的检测服务器。

较佳地，所述当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果，包括：

当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行解析，获得解析数据；

对所述解析数据进行漏洞检测，获得漏洞检测结果。

较佳地，所述对所述发向目标服务器的流量信息进行解析，获得解析数据，包括：

对所述发向目标服务器的流量信息中的统一资源定位符 URL 进行解析，获得各站点域名信息及关联域名信息；

根据所述统一资源定位符 URL 或所述域名信息获取关联互联网协议 IP 信息；

在所述发向目标服务器的流量信息中获取应用功能文件，对所述应用功能文件对应的统一资源定位符 URL 进行解析，获得超文本传输协议 HTTP 请求参数信息。

较佳地，所述对所述解析数据进行漏洞检测，获得漏洞检测结果，包括：

将所述解析数据发送至待检测队列，对所述待检测队列中解析数据的统一资源定位符 URL 依次进行检测；

当检测到所述统一资源定位符 URL 是周期性检测任务且所述统一资源定位符 URL 对应的文件没有更改时，调用上一次的漏洞检测结果作为本次漏洞检测

结果，否则对所述统一资源定位符 URL 进行万维网 web 指纹识别，获得漏洞检测结果。

较佳地，所述对所述统一资源定位符 URL 进行万维网 web 指纹识别，获得漏洞检测结果，包括：

当对所述统一资源定位符 URL 进行万维网 web 指纹识别后，如果获得对应网站的指纹信息，则根据所述指纹信息进行漏洞检测，获得漏洞检测结果，所述指纹信息包括：操作系统类型、万维网 web 服务器、数据库类型及万维网 web 应用脚本语言；

当对所述统一资源定位符 URL 进行万维网 web 指纹识别后，如果未获得对应网站的指纹信息，则调用漏洞检测终端提供的检测工具进行检测，获得漏洞检测结果。

本申请还公开了一种漏洞检测的装置，所述装置包括：

信息发送模块：设置为获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器；

数据分析模块：设置为当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果；

检测模块：设置为根据所述分析结果检测目标服务器是否存在漏洞；

漏洞修复模块：设置为当检测到所述目标服务器存在漏洞时，对所述目标服务器进行定位，并对所述存在的漏洞进行修复。

本申请还公开了一种计算机设备，所述计算机设备包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被一个或多个所述处理器执行时，使得一个或多个所述处理器执行上述所述漏洞检测方法的步骤。

本申请还公开了一种计算机可读存储介质，所述存储介质可被处理器读写，所述存储介质存储有计算机指令，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行上述所述漏洞检测方法的步骤。

本申请的有益效果是：本申请通过获取流量信息，将所述流量信息发送至检测服务器进行分析，并根据分析结果获得漏洞检测结果，可以有效的对不同场景进行漏洞检测，提高检测效率。

附图说明

图 1 为本申请第一个实施例的一种漏洞检测的方法的流程示意图；

图 2 为本申请第二个实施例的一种漏洞检测的方法的流程示意图；

图 3 为本申请第三个实施例的一种漏洞检测的方法的流程示意图；

图 4 为本申请第四个实施例的一种漏洞检测的方法的流程示意图；

图 5 为本申请第五个实施例的一种漏洞检测的方法的流程示意图；

图 6 为本申请第六个实施例的一种漏洞检测的方法的流程示意图；

图 7 为本申请第七个实施例的一种漏洞检测的方法的流程示意图；

图 8 为本申请实施例的一种漏洞检测装置结构示意图。

具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

本技术领域技术人员可以理解，除非特意声明，这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是，本申请的说明书中使用的措辞“包括”是指存在所述特征、整数、步骤、操作、元件和/或组件，但是并不排除存在或添加一个或多个其他特征、整数、步骤、操作、元件、组件和/或它们的组。

本申请第一个实施例的一种漏洞检测的方法流程如图 1 所示，本实施例包括以下步骤：

步骤 s101，获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器；

具体的，所述流量信息包括对目标服务器的 HTTP（超文本传输协议）请求，其中，HTTP 请求包括 HTTP GET 请求和 HTTP POST 请求；对所述目标服务器发起 HTTP（超文本传输协议）请求的可以是浏览器、手机或者 APP 应用。

具体的，无论是浏览器、手机或者 APP 应用，在向目标服务器发起 HTTP（超文本传输协议）请求时，可将所述 HTTP（超文本传输协议）请求信息进行采集并发送给检测服务器进行分析，用以进行漏洞检测。

步骤 s102，当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果；

具体的，当所述检测服务器接收到所述发向目标服务器的流量信息后，即收到 HTTP（超文本传输协议）请求等信息后，可对所述发向目标服务器的流量信息进行分析，获取分析结果，所述分析过程可以分为解析阶段和漏洞检测阶段，其中，解析阶段用于对所述发向目标服务器的流量信息进行解析，获取解析数据；漏洞检测阶段用于对解析的数据进行漏洞检测，发现目标服务器中的漏洞。

步骤 s103，根据所述分析结果检测目标服务器是否存在漏洞；

具体的，当对流量信息进行分析并获取到漏洞检测结果后，可根据所述漏洞检测结果判断目标服务器是否存在漏洞；其中，漏洞检测结果包括：文件 URL（统一资源定位符）漏洞扫描结果及应用功能文件 URL（统一资源定位符）漏洞

检测结果；所述文件 URL（统一资源定位符）漏洞扫描结果通过调用漏洞检测终端提供的扫描工具对 URL（统一资源定位符）对应的文件进行漏洞扫描获得，所述应用功能文件 URL（统一资源定位符）漏洞检测结果可通过调用 SQL 注入、XSS 攻击及越权漏洞检测等漏洞检测工具获得。

具体的，当检测到各文件的 URL（统一资源定位符）漏洞扫描无异常以及应用功能文件 URL（统一资源定位符）的 SQL 注入、XSS 攻击及越权漏洞检测结果正常时可判定目标服务器不存在漏洞；当检测到各文件的 URL（统一资源定位符）漏洞扫描有异常或应用功能文件 URL（统一资源定位符）的 SQL 注入、XSS 攻击及越权漏洞检测结果异常时可判定目标服务器存在漏洞。

步骤 s104，当检测到所述目标服务器存在漏洞时，对所述目标服务器进行定位，并对所述存在的漏洞进行修复。

具体的，当检测到所述目标服务器存在漏洞时，可根据目标服务器的 URL（统一资源定位符）所对应的域名信息或者 IP（互联网协议）信息，定位目标服务器的位置，然后通过攻击所述目标服务器定位出目标服务器中的安全漏洞，所述攻击可通过向目标服务器发起 HTTP（超文本传输协议）请求，并获得 HTTP（超文本传输协议）响应进行。

本实施例中，通过获取流量信息，将所述流量信息发送至检测服务器进行分析，并根据分析结果获得漏洞检测结果，可以有效的对不同场景进行漏洞检测，提高检测效率。

图 2 为本申请第二个实施例的一种漏洞检测的方法流程示意图，如图所示，所述步骤 s101，获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器，包括：

步骤 s201，在浏览器中设置插件，将所述插件与所述检测服务器进行关联，并通过所述浏览器中的插件获取访问各站点的超文本传输协议 HTTP 请求信息；

具体的，可在浏览器中安装自制插件，通过所述自制插件可获取各站点的流量信息，所述流量信息包括 HTTP（超文本传输协议）请求信息，例如：在 chrome 浏览器中安装 chrome 插件，通过所述 chrome 插件将检测服务器与 chrome 浏览器进行关联，然后通过所述 chrome 插件从 chrome 浏览器中获取各站点的流量信息，并将获取到的所述流量信息发送至所述检测服务器。

步骤 s202，将所述超文本传输协议 HTTP 请求信息发送至与所述浏览器中的插件关联的检测服务器。

具体的，当通过所述浏览器中的插件获取到所述 HTTP（超文本传输协议）请求信息后，可通过所述浏览器中的插件与检测服务器之间的关联关系找到对应的检测服务器，并将所述 HTTP（超文本传输协议）请求信息发送至与所述浏

览器中的插件关联的检测服务器。

本实施例中，通过在浏览器中设置插件，并通过插件将流量信息发送给检测服务器进行漏洞检测，可以提高漏洞检测的效率。

图 3 为本申请第三个实施例的一种漏洞检测的方法流程示意图，如图所示，所述步骤 s101，获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器，包括：

步骤 s301，设置超文本传输协议 HTTP 代理服务器，通过所述超文本传输协议 HTTP 代理服务器将浏览器的网络代理端口指向代理系统，将所述代理系统与所述检测服务器进行关联；

具体的，可先设置 HTTP（超文本传输协议）代理服务器，通过所述超文本传输协议 HTTP 代理服务器将浏览器的网络代理端口指向代理系统，将所述代理系统与所述检测服务器进行关联，例如：通过所述 HTTP（超文本传输协议）代理服务器可将检测服务器与浏览器、手机以及 APP 应用的网络代理端口进行关联。

步骤 s302，当获取到网络流量信息时，通过所述代理系统将所述网络流量信息发送至与所述代理系统关联的检测服务器。

具体的，当通过代理端口获取到各站点的网络流量信息时，可通过代理系统与检测服务器之间的关联关系找到对应的检测服务器，所述网络流量信息也包括 HTTP（超文本传输协议）请求信息，然后将所述 HTTP（超文本传输协议）请求信息发送至与所述代理系统关联的检测服务器。

本实施例中，通过代理服务器将流量信息发送给检测服务器进行漏洞检测，可以提高漏洞检测的效率。

图 4 为本申请第四个实施例的一种漏洞检测的方法流程示意图，如图所示，所述步骤 s102，当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果，包括：

步骤 s401，当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行解析，获得解析数据；

具体的，当所述检测服务器接收到所述发向目标服务器的流量信息后，可对所述发向目标服务器的流量信息进行数据解析处理，获取所述发向目标服务器的流量信息中所包含的文件的 URL（统一资源定位符）和 IP（互联网协议）信息。

步骤 s402，对所述解析数据进行漏洞检测，获得漏洞检测结果。

具体的，根据所述解析后的数据进行漏洞检测，获得漏洞检测结果，所述漏洞检测包括对文件 URL（统一资源定位符）进行漏洞扫描及对应用功能文件

URL（统一资源定位符）进行漏洞检测，并由此获得文件URL（统一资源定位符）漏洞扫描结果及应用功能文件URL（统一资源定位符）漏洞检测结果。

本实施例中，通过检测服务器对流量信息解析后进行漏洞检测，可以有效获取漏洞检测结果，提高检测效率。

图5为本申请第五个实施例的一种漏洞检测的方法流程示意图，如图所示，所述步骤s401，对所述发向目标服务器的流量信息进行解析，获得解析数据，包括：

步骤s501，对所述发向目标服务器的流量信息中的统一资源定位符URL进行解析，获得各站点域名信息及关联域名信息；

具体的，URL是统一资源定位符，是对可以从互联网上得到的资源的位置和访问方法的一种简洁的表示，是互联网上标准资源的地址，互联网上的每个文件都有一个唯一的URL，它包含的信息指出文件的位置以及浏览器应该怎么处理它，标准的URL包含域名、端口号、资源位置、参数以及锚点等信息。

具体的，当获取到流量信息中的URL（统一资源定位符）后，可对所述流量信息中的URL（统一资源定位符）进行解析，获得各站点域名信息及关联域名信息，由于域名信息是URL（统一资源定位符）的一部分，因此很容易从URL（统一资源定位符）中解析出域名信息。

步骤s502，根据所述统一资源定位符URL或所述域名信息获取关联互联网协议IP信息；

具体的，由于URL（统一资源定位符）中可能直接包含IP（互联网协议）信息，那么可以直接从URL（统一资源定位符）获取IP（互联网协议）信息；如果URL（统一资源定位符）中包含的是域名信息，由于域名信息和IP（互联网协议）信息表示的是同一个信息，IP（互联网协议）信息用数字表示，用来唯一标识互联网上计算机的逻辑地址，但是不好记忆，如192.168.1.1.，因此通常将IP（互联网协议）信息转换为域名信息，而域名信息都是字符表示，容易记忆，如www.baidu.com；因此可通过对域名信息的解析获得IP（互联网协议）信息。

步骤s503，在所述发向目标服务器的流量信息中获取应用功能文件，对所述应用功能文件对应的统一资源定位符URL进行解析，获得超文本传输协议HTTP请求参数信息。

具体的，首先可在所述发向目标服务器的流量信息中筛选出应用功能的文件，然后对每个应用功能文件对应的URL（统一资源定位符）进行解析，获得其中包含的超文本传输协议HTTP请求参数信息。

本实施例中，通过对流量信息的解析，获得流量信息中包含的URL和IP信

息，根据 URL 和 IP 信息可进行漏洞检测，可有效提高检测效率。

图 6 为本申请第六个实施例的一种漏洞检测的方法流程示意图，如图所示，所述步骤 s402，对所述解析数据进行漏洞检测，获得漏洞检测结果，包括：

步骤 s601，将所述解析数据发送至待检测队列，对所述待检测队列中解析数据的统一资源定位符 URL 依次进行检测；

具体的，当对流量数据进行解析获取到 URL（统一资源定位符）后，可将 URL（统一资源定位符）信息放入待检测队列，所述待检测队列包含多个检测任务，所述检测任务按时间顺序进行排列，并按时间顺序依次进行检测。

具体的，所述对 URL（统一资源定位符）的检测包括：对 URL（统一资源定位符）进行周期性检测任务的检测以及对所述 URL（统一资源定位符）对应的文件是否有更改的检测。

步骤 s602，当检测到所述统一资源定位符 URL 是周期性检测任务且所述统一资源定位符 URL 对应的文件没有更改时，调用上一次的漏洞检测结果作为本次漏洞检测结果，否则对所述统一资源定位符 URL 进行万维网 web 指纹识别，获得漏洞检测结果。

具体的，当检测到所述 URL（统一资源定位符）是周期性检测任务且所述 URL（统一资源定位符）对应的文件没有更改时，可调用上一次的漏洞检测结果作为本次漏洞检测结果；其中，每次进行漏洞检测之后都可将漏洞检测结果进行存储。

具体的，判断所述 URL（统一资源定位符）对应的文件是否有更改包括：每次在检测所述 URL（统一资源定位符）时记录当前 URL（统一资源定位符）对应文件的 md5 值，当再次检测所述 URL（统一资源定位符）对应的文件时，判断所述 URL（统一资源定位符）对应的文件的 md5 值和上次检测时记录的 md5 值是否相同，若相同，则所述 URL（统一资源定位符）对应的文件无更改，若不相同，则所述 URL（统一资源定位符）对应的文件有更改。

具体的，如果检测到所述 URL（统一资源定位符）不是周期性检测任务或者所述 URL（统一资源定位符）对应的文件有更改时，可对所述统一资源定位符 URL 进行万维网 web 指纹识别，并由此获得漏洞检测结果。

本实施例中，通过对 URL 对应的检测任务进行识别以及对 URL 对应的文件进行检测，可以有效获取检测结果，提高检测效率。

图 7 为本申请第七个实施例的一种漏洞检测的方法流程示意图，如图所示，所述步骤 s602，对所述统一资源定位符 URL 进行万维网 web 指纹识别，获得漏洞检测结果，包括：

步骤 s701，当对所述统一资源定位符 URL 进行万维网 web 指纹识别后，如

果获得对应网站的指纹信息，则根据所述指纹信息进行漏洞检测，获得漏洞检测结果，所述指纹信息包括：操作系统类型、万维网 web 服务器、数据库类型及万维网 web 应用脚本语言；

具体的，可对所述 URL（统一资源定位符）进行 web（万维网）指纹识别，如果通过所述 web（万维网）指纹识别后获取对应网站的指纹信息，那么可调用与所述指纹信息相对应的扫描依据进行漏洞检测，获得漏洞检测结果，所述指纹信息包括操作系统类型、使用的 web（万维网）服务器、数据库类型和 web（万维网）应用的脚本语言。

步骤 s702，当对所述统一资源定位符 URL 进行万维网 web 指纹识别后，如果未获得对应网站的指纹信息，则调用漏洞检测终端提供的检测工具进行检测，获得漏洞检测结果。

具体的，当对所述 URL（统一资源定位符）进行 web（万维网）指纹识别后，如果未获得对应网站的指纹信息，那么可调用漏洞检测终端提供的所有的扫描工具对其 URL（统一资源定位符）对应的文件进行漏洞扫描，根据扫描结果确定其 URL（统一资源定位符）对应的文件是否存在漏洞，获得漏洞检测结果。

具体的，还可收集各应用功能所包含的各文件对应的 URL（统一资源定位符），调用针对应用功能的检测工具对对应的 URL（统一资源定位符）进行漏洞检测；例如，调用专门针对 SQL 注入、XSS 攻击和越权漏洞的检测工具对各应用功能进行自动化的 SQL 注入、XSS 攻击、越权漏洞的检测，获得漏洞检测结果。

本实施例中，通过对 URL 进行 web 指纹识别，并根据指纹识别结果进行工具检测，可以有效提高漏洞检测效率。

本申请实施例的一种漏洞检测的装置结构如图 8 所示，包括：

信息发送模块 801、数据分析模块 802、检测模块 803 及漏洞修复模块 804；其中，信息发送模块 801 与数据分析模块 802 相连，数据分析模块 802 与检测模块 803 相连，检测模块 803 与漏洞修复模块 804 相连；信息发送模块 801 设置为获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器；数据分析模块 802 设置为当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果；检测模块 803 设置为根据所述分析结果检测目标服务器是否存在漏洞；漏洞修复模块 804 设置为当检测到所述目标服务器存在漏洞时，对所述目标服务器进行定位，并对所述存在的漏洞进行修复。

本申请实施例还公开了一种计算机设备，所述计算机设备包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被一个或多个所述处理器执行时，使得一个或多个所述处理器执行上述各实施例中所述漏

洞检测方法中的步骤。

本申请实施例还公开了一种计算机可读存储介质，所述存储介质可被处理器读写，所述存储器存储有计算机可读指令，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行上述各实施例中所述漏洞检测方法中的步骤。其中，该计算机存储介质可以为非易失性存储介质，也可以为易失性存储介质，具体本申请不做限定。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，该计算机程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，前述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）等非易失性存储介质，或随机存储记忆体（Random Access Memory，RAM）等。

以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

权 利 要 求 书

1、一种漏洞检测的方法，包括以下步骤：

获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器；

当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果；

根据所述分析结果检测目标服务器是否存在漏洞；

当检测到所述目标服务器存在漏洞时，对所述目标服务器进行定位，并对所述存在的漏洞进行修复。

2、如权利要求 1 所述的漏洞检测的方法，所述获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器，包括：

在浏览器中设置插件，将所述插件与所述检测服务器进行关联，并通过所述浏览器中的插件获取访问各站点的超文本传输协议 HTTP 请求信息；

将所述超文本传输协议 HTTP 请求信息发送至与所述浏览器中的插件关联的检测服务器。

3、如权利要求 1 所述的漏洞检测的方法，所述获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器，包括：

设置超文本传输协议 HTTP 代理服务器，通过所述超文本传输协议 HTTP 代理服务器将浏览器的网络代理端口指向代理系统，将所述代理系统与所述检测服务器进行关联；

当获取到网络流量信息时，通过所述代理系统将所述网络流量信息发送至与所述代理系统关联的检测服务器。

4、如权利要求 1 所述的漏洞检测的方法，所述当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果，包括：

当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行解析，获得解析数据；

对所述解析数据进行漏洞检测，获得漏洞检测结果。

5、如权利要求 4 所述的漏洞检测的方法，所述对所述发向目标服务器的流量信息进行解析，获得解析数据，包括：

对所述发向目标服务器的流量信息中的统一资源定位符 URL 进行解析，获得各站点域名信息及关联域名信息；

根据所述统一资源定位符 URL 或所述域名信息获取关联互联网协议 IP 信息；

在所述发向目标服务器的流量信息中获取应用功能文件，对所述应用功能

文件对应的统一资源定位符 URL 进行解析，获得超文本传输协议 HTTP 请求参数信息。

6、如权利要求 4 所述的漏洞检测的方法，所述对所述解析数据进行漏洞检测，获得漏洞检测结果，包括：

将所述解析数据发送至待检测队列，对所述待检测队列中解析数据的统一资源定位符 URL 依次进行检测；

当检测到所述统一资源定位符 URL 是周期性检测任务且所述统一资源定位符 URL 对应的文件没有更改时，调用上一次的漏洞检测结果作为本次漏洞检测结果，否则对所述统一资源定位符 URL 进行万维网 web 指纹识别，获得漏洞检测结果。

7、如权利要求 6 所述的漏洞检测的方法，所述对所述统一资源定位符 URL 进行万维网 web 指纹识别，获得漏洞检测结果，包括：

当对所述统一资源定位符 URL 进行万维网 web 指纹识别后，如果获得对应网站的指纹信息，则根据所述指纹信息进行漏洞检测，获得漏洞检测结果，所述指纹信息包括：操作系统类型、万维网 web 服务器、数据库类型及万维网 web 应用脚本语言；

当对所述统一资源定位符 URL 进行万维网 web 指纹识别后，如果未获得对应网站的指纹信息，则调用漏洞检测终端提供的检测工具进行检测，获得漏洞检测结果。

8、一种漏洞检测的装置，所述装置包括：

信息发送模块：设置为获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器；

数据分析模块：设置为当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果；

检测模块：设置为根据所述分析结果检测目标服务器是否存在漏洞；

漏洞修复模块：设置为当检测到所述目标服务器存在漏洞时，对所述目标服务器进行定位，并对所述存在的漏洞进行修复。

9、一种计算机设备，所述计算机设备包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被一个或多个所述处理器执行时，使得一个或多个所述处理器执行如下所述漏洞检测方法的步骤：

获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器；

当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果；

根据所述分析结果检测目标服务器是否存在漏洞；

当检测到所述目标服务器存在漏洞时，对所述目标服务器进行定位，并对所述存在的漏洞进行修复。

10、如权利要求 9 所述的计算机设备，所述计算机可读指令被一个或多个所述处理器执行时，使得一个或多个所述处理器执行所述获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器的步骤时，还执行如下步骤：

在浏览器中设置插件，将所述插件与所述检测服务器进行关联，并通过所述浏览器中的插件获取访问各站点的超文本传输协议 HTTP 请求信息；

将所述超文本传输协议 HTTP 请求信息发送至与所述浏览器中的插件关联的检测服务器。

11、如权利要求 9 所述的计算机设备，所述计算机可读指令被一个或多个所述处理器执行时，使得一个或多个所述处理器执行所述获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器的步骤时，还执行如下步骤：

设置超文本传输协议 HTTP 代理服务器，通过所述超文本传输协议 HTTP 代理服务器将浏览器的网络代理端口指向代理系统，将所述代理系统与所述检测服务器进行关联；

当获取到网络流量信息时，通过所述代理系统将所述网络流量信息发送至与所述代理系统关联的检测服务器。

12、如权利要求 9 所述的计算机设备，所述计算机可读指令被一个或多个所述处理器执行时，使得一个或多个所述处理器执行所述当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果的步骤时，还执行如下步骤：

当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行解析，获得解析数据；

对所述解析数据进行漏洞检测，获得漏洞检测结果。

13、如权利要求 12 所述的计算机设备，所述计算机可读指令被一个或多个所述处理器执行时，使得一个或多个所述处理器执行所述发向目标服务器的流量信息进行解析，获得解析数据的步骤时，还执行如下步骤：

对所述发向目标服务器的流量信息中的统一资源定位符 URL 进行解析，获得各站点域名信息及关联域名信息；

根据所述统一资源定位符 URL 或所述域名信息获取关联互联网协议 IP 信息；

在所述发向目标服务器的流量信息中获取应用功能文件，对所述应用功能文件对应的统一资源定位符 URL 进行解析，获得超文本传输协议 HTTP 请求参数信息。

14、如权利要求 12 所述的计算机设备，所述计算机可读指令被一个或多个所述处理器执行时，使得一个或多个所述处理器执行所述解析数据进行漏洞检测，获得漏洞检测结果的步骤时，还执行如下步骤：

将所述解析数据发送至待检测队列，对所述待检测队列中解析数据的统一资源定位符 URL 依次进行检测；

当检测到所述统一资源定位符 URL 是周期性检测任务且所述统一资源定位符 URL 对应的文件没有更改时，调用上一次的漏洞检测结果作为本次漏洞检测结果，否则对所述统一资源定位符 URL 进行万维网 web 指纹识别，获得漏洞检测结果。

15、一种计算机可读存储介质，所述存储介质可被处理器读写，所述存储介质存储有计算机可读指令，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行如下所述漏洞检测方法的步骤：

获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器；

当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果；

根据所述分析结果检测目标服务器是否存在漏洞；

当检测到所述目标服务器存在漏洞时，对所述目标服务器进行定位，并对所述存在的漏洞进行修复。

16、如权利要求 15 所述的计算机存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行所述获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器的步骤时，还还执行如下步骤：

在浏览器中设置插件，将所述插件与所述检测服务器进行关联，并通过所述浏览器中的插件获取访问各站点的超文本传输协议 HTTP 请求信息；

将所述超文本传输协议 HTTP 请求信息发送至与所述浏览器中的插件关联的检测服务器。

17、如权利要求 15 所述的计算机存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行所述获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器的步骤时，还执行如下步骤：

设置超文本传输协议 HTTP 代理服务器，通过所述超文本传输协议 HTTP 代理服务器将浏览器的网络代理端口指向代理系统，将所述代理系统与所述检测服务器进行关联；

当获取到网络流量信息时，通过所述代理系统将所述网络流量信息发送至与所述代理系统关联的检测服务器。

18、如权利要求 15 所述的计算机存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行所述当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果的步骤时，还执行如下步骤：

当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行解析，获得解析数据；

对所述解析数据进行漏洞检测，获得漏洞检测结果。

19、如权利要求 18 所述的计算机存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行所述对所述发向目标服务器的流量信息进行解析，获得解析数据的步骤时，还执行如下步骤：

对所述发向目标服务器的流量信息中的统一资源定位符 URL 进行解析，获得各站点域名信息及关联域名信息；

根据所述统一资源定位符 URL 或所述域名信息获取关联互联网协议 IP 信息；

在所述发向目标服务器的流量信息中获取应用功能文件，对所述应用功能文件对应的统一资源定位符 URL 进行解析，获得超文本传输协议 HTTP 请求参数信息。

20、如权利要求 18 所述的计算机可读存储介质，所述计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行所述对所述解析数据进行漏洞检测，获得漏洞检测结果的步骤时，还执行如下步骤：

将所述解析数据发送至待检测队列，对所述待检测队列中解析数据的统一资源定位符 URL 依次进行检测；

当检测到所述统一资源定位符 URL 是周期性检测任务且所述统一资源定位符 URL 对应的文件没有更改时，调用上一次的漏洞检测结果作为本次漏洞检测结果，否则对所述统一资源定位符 URL 进行万维网 web 指纹识别，获得漏洞检测结果。

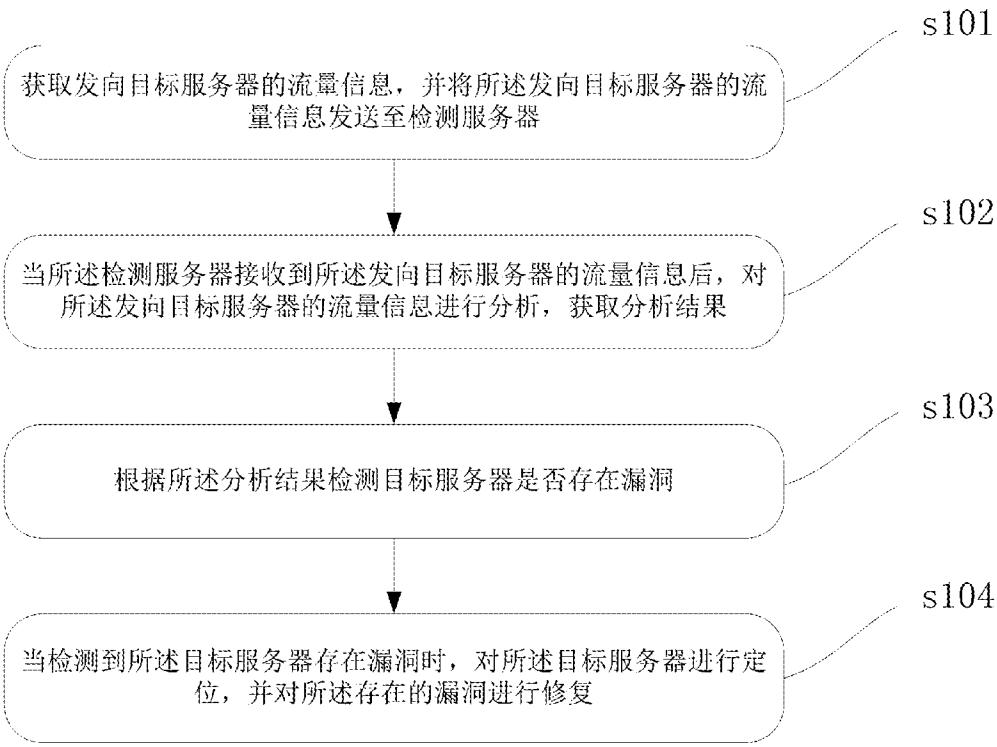
s101
获取发向目标服务器的流量信息，并将所述发向目标服务器的流量信息发送至检测服务器
s102
当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行分析，获取分析结果
s103
根据所述分析结果检测目标服务器是否存在漏洞
s104
当检测到所述目标服务器存在漏洞时，对所述目标服务器进行定位，并对所述存在的漏洞进行修复

图 1

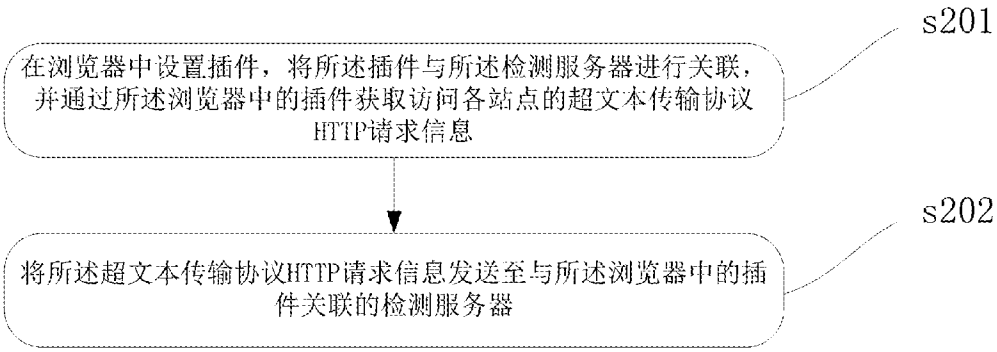
s201
在浏览器中设置插件，将所述插件与所述检测服务器进行关联，并通过所述浏览器中的插件获取访问各站点的超文本传输协议HTTP请求信息
s202
将所述超文本传输协议HTTP请求信息发送至与所述浏览器中的插件关联的检测服务器

图 2

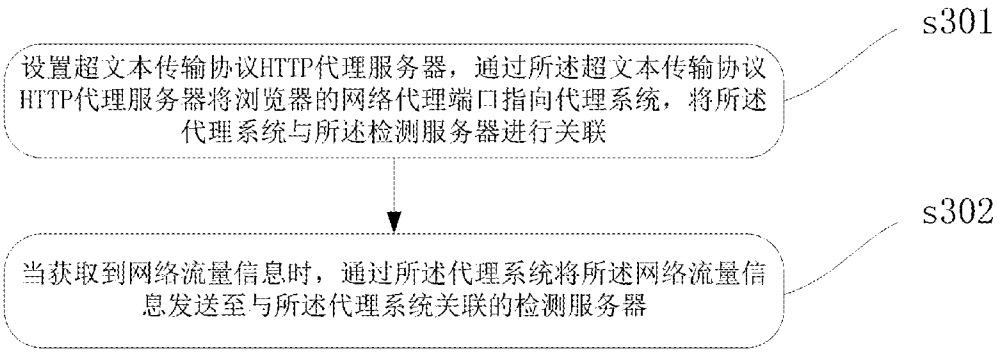
s301
设置超文本传输协议HTTP代理服务器，通过所述超文本传输协议HTTP代理服务器将浏览器的网络代理端口指向代理系统，将所述代理系统与所述检测服务器进行关联
s302
当获取到网络流量信息时，通过所述代理系统将所述网络流量信息发送至与所述代理系统关联的检测服务器

图 3

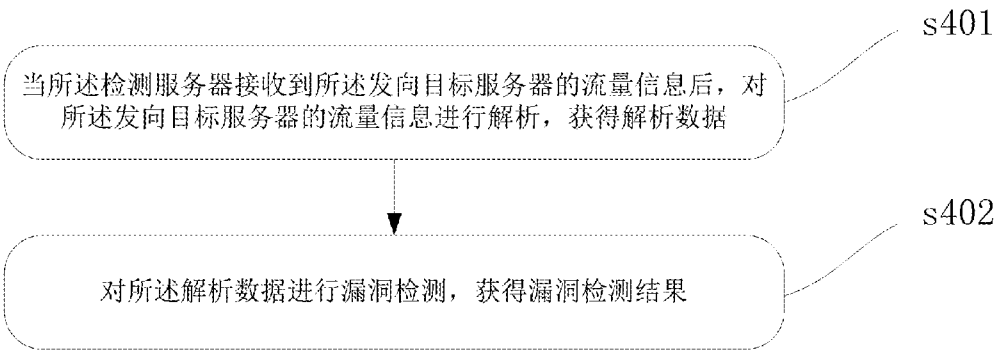
s401
当所述检测服务器接收到所述发向目标服务器的流量信息后，对所述发向目标服务器的流量信息进行解析，获得解析数据
s402
对所述解析数据进行漏洞检测，获得漏洞检测结果

图 4

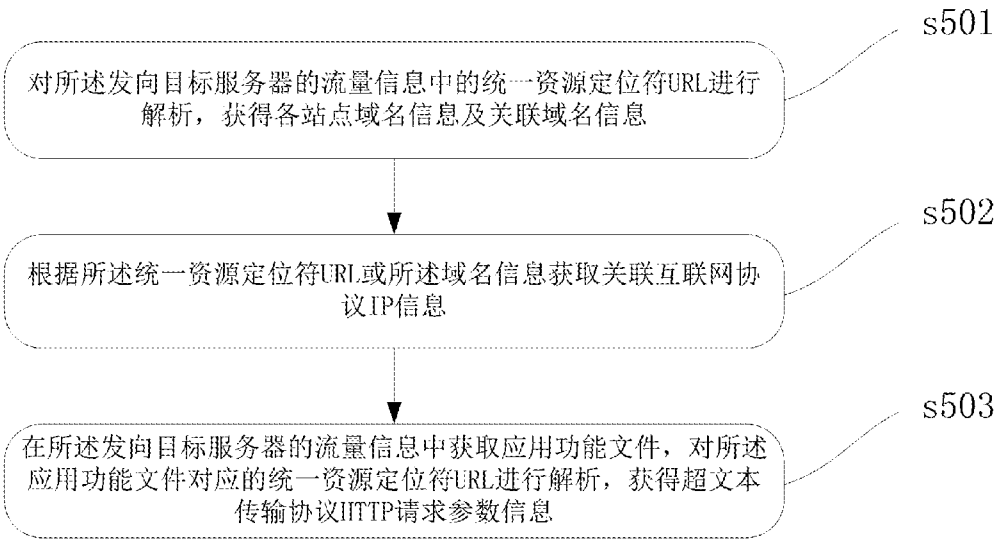
s501
对所述发向目标服务器的流量信息中的统一资源定位符URL进行解析，获得各站点域名信息及关联域名信息
s502
根据所述统一资源定位符URL或所述域名信息获取关联互联网协议IP信息
s503
在所述发向目标服务器的流量信息中获取应用功能文件，对所述应用功能文件对应的统一资源定位符URL进行解析，获得超文本传输协议HTTP请求参数信息

图 5

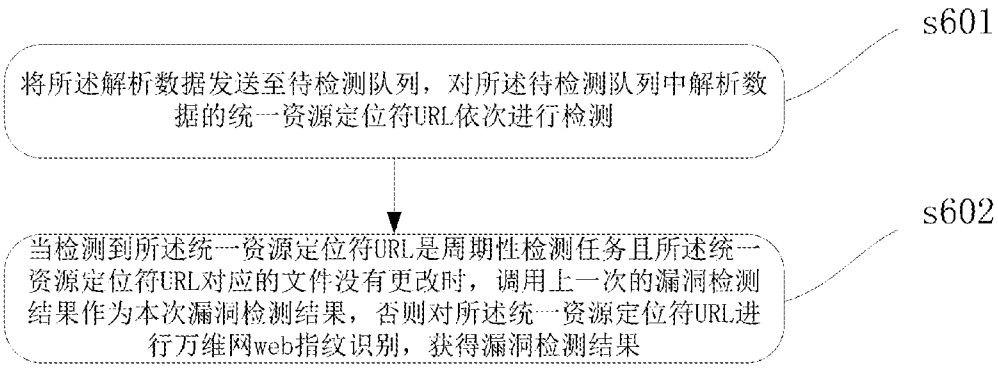
s601
将所述解析数据发送至待检测队列，对所述待检测队列中解析数据的统一资源定位符URL依次进行检测
s602
当检测到所述统一资源定位符URL是周期性检测任务且所述统一资源定位符URL对应的文件没有更改时，调用上一次的漏洞检测结果作为本次漏洞检测结果，否则对所述统一资源定位符URL进行万维网web指纹识别，获得漏洞检测结果

图 6

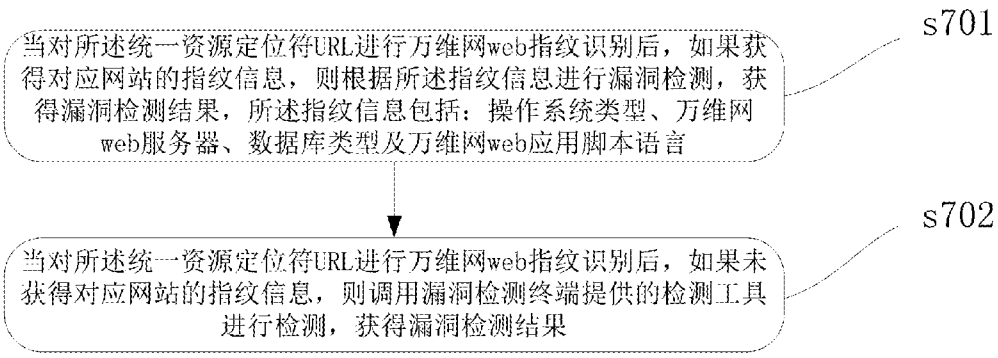
s701
当对所述统一资源定位符URL进行万维网web指纹识别后，如果获得对应网站的指纹信息，则根据所述指纹信息进行漏洞检测，获得漏洞检测结果，所述指纹信息包括：操作系统类型、万维网web服务器、数据库类型及万维网web应用脚本语言
s702
当对所述统一资源定位符URL进行万维网web指纹识别后，如果未获得对应网站的指纹信息，则调用漏洞检测终端提供的检测工具进行检测，获得漏洞检测结果

图 7

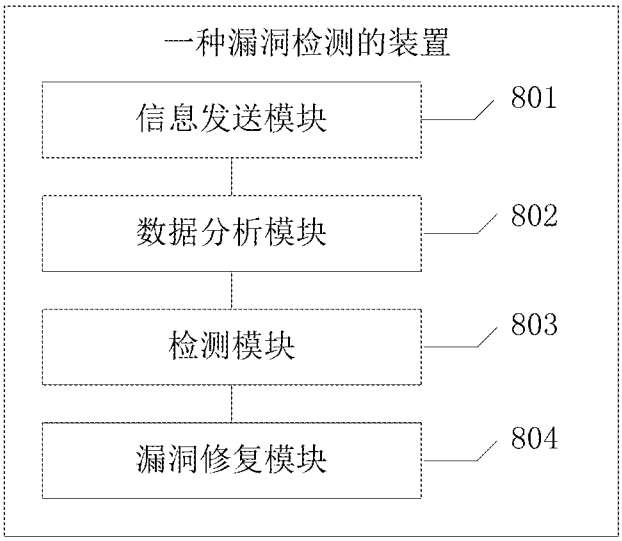
一种漏洞检测的装置
信息发送模块
801
数据分析模块
802
检测模块
803
漏洞修复模块
804

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/118685

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 29/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC: 漏洞, 检测, 扫描, 流量, HTTP, 请求, 分析, 解析, 插件, 代理, 网页, 指纹, 识别, 应用功能, 文件, URL, vulnerability, detect+, scan+, post, get, analysis, parse, plug in, agent, proxy, web, fingerprint, identif+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110324311 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 11 October 2019 (2019-10-11) claims 1-10	1-20
X	CN 104378389 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 25 February 2015 (2015-02-25) description, paragraphs 82-143, figures 1-5	1, 4, 8, 9, 12, 15, 18
Y	CN 104378389 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 25 February 2015 (2015-02-25) description, paragraphs 82-143, figures 1-5	2-3, 5-7, 10-11, 13-14, 16-17, 19-20
Y	CN 108040045 A (BAIDU ONLINE NETWORK TECHNOLOGY BEIJING CO., LTD.) 15 May 2018 (2018-05-15) description, paragraphs 34-35	2, 3, 10, 11, 16, 17
Y	CN 105141647 A (CHINA UNIONPAY CO., LTD.) 09 December 2015 (2015-12-09) description, paragraphs 9, 11	5, 13, 19
Y	CN 108063759 A (XI'AN JIAOTONG JUMP NETWORK TECHNOLOGY CO., LTD.) 22 May 2018 (2018-05-22) description, paragraphs 4-11	6, 7, 14, 20

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 January 2020	**23 January 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 108667770 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 16 October 2018 (2018-10-16) entire document	1-20
A	US 2017270303 A1 (CHECKMARX LTD.) 21 September 2017 (2017-09-21) entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/118685

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110324311 A	11 October 2019	None	
CN 104378389 A	25 February 2015	CN 104378389 B	28 September 2016
CN 108040045 A	15 May 2018	None	
CN 105141647 A	09 December 2015	CN 105141647 B	21 September 2018
CN 108063759 A	22 May 2018	None	
CN 108667770 A	16 October 2018	None	
US 2017270303 A1	21 September 2017	US 10387656 B2	20 August 2019

国际检索报告

国际申请号
PCT/CN2019/118685

A. 主题的分类

H04L 29/06(2006.01)i; H04L 29/08(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNKI,CNPAT,WPI,EPODOC:漏洞，检测，扫描，流量，HTTP，请求，分析，解析，插件，代理，网页，指纹，识别，应用功能，文件，URL，vulnerability, detect+, scan+, post, get, analysis, parse, plug in, agent, proxy, web, fingerprint, identif+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 110324311 A (平安科技深圳有限公司) 2019年 10月 11日 (2019-10-11) 权利要求1-10	1-20
X	CN 104378389 A (北京奇虎科技有限公司等) 2015年 2月 25日 (2015-02-25) 说明书第82-143段，图1-5	1，4，8，9，12，15，18
Y	CN 104378389 A (北京奇虎科技有限公司等) 2015年 2月 25日 (2015-02-25) 说明书第82-143段，图1-5	2-3，5-7，10-11，13-14，16-17，19-20
Y	CN 108040045 A (百度在线网络技术北京有限公司) 2018年 5月 15日 (2018-05-15) 说明书第34-35段	2，3，10，11，16，17
Y	CN 105141647 A (中国银联股份有限公司) 2015年 12月 9日 (2015-12-09) 说明书第9、11段	5，13，19
Y	CN 108063759 A (西安交大捷普网络科技有限公司) 2018年 5月 22日 (2018-05-22) 说明书第4-11段	6，7，14，20
A	CN 108667770 A (腾讯科技深圳有限公司) 2018年 10月 16日 (2018-10-16) 全文	1-20

☑ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 1月 8日	2020年 1月 23日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 董振兴 电话号码 01053961757

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	US 2017270303 A1 (CHECKMARX LTD.) 2017年 9月 21日 (2017-09-21) 全文	1-20

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/118685

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 110324311 A	2019年 10月 11日	无	
CN 104378389 A	2015年 2月 25日	CN 104378389 B	2016年 9月 28日
CN 108040045 A	2018年 5月 15日	无	
CN 105141647 A	2015年 12月 9日	CN 105141647 B	2018年 9月 21日
CN 108063759 A	2018年 5月 22日	无	
CN 108667770 A	2018年 10月 16日	无	
US 2017270303 A1	2017年 9月 21日	US 10387656 B2	2019年 8月 20日