(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 104065645 A
(43)申请公布日 2014.09.24

(21)申请号 201410230520.1

(22)申请日 2014.05.28

(71)申请人 北京知道创宇信息技术有限公司
地址 100044 北京市海淀区蓝靛厂南路 55 号金威大厦 803 室

(72)发明人 练晓谦

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 马永利 李浩

(51)Int.Cl.
*H04L 29/06*(2006.01)
*G06F 21/57*(2013.01)

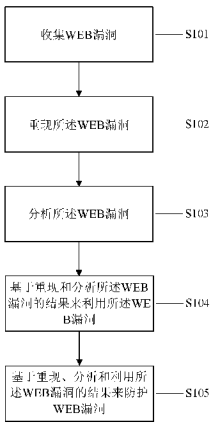
权利要求书2页 说明书11页 附图3页

(54)发明名称

用于防护 WEB 漏洞的方法和设备

(57)摘要

本发明公开了用于防护 WEB 漏洞的方法和设备。一种用于防护 WEB 漏洞的方法,所述方法包括:收集 WEB 漏洞;重现所述 WEB 漏洞;分析所述 WEB 漏洞;基于重现和分析所述 WEB 漏洞的结果来利用所述 WEB 漏洞;基于重现、分析和利用所述 WEB 漏洞的结果来防护 WEB 漏洞。




CN 104065645 A

1. 一种用于防护 WEB 漏洞的方法，所述方法包括：

收集 WEB 漏洞；

重现所述 WEB 漏洞；

分析所述 WEB 漏洞；

基于重现和分析所述 WEB 漏洞的结果来利用所述 WEB 漏洞；以及

基于重现、分析和利用所述 WEB 漏洞的结果来防护 WEB 漏洞。

2. 根据权利要求 1 所述的方法，进一步包括在收集所述 WEB 漏洞之后基于筛选标准对所收集的所述 WEB 漏洞进行筛选。

3. 根据权利要求 2 所述的方法，其中所述筛选标准包括以下至少一个：所述 WEB 漏洞的新旧程度、所述 WEB 漏洞的影响范围、利用所述 WEB 漏洞的难易程度、所述 WEB 漏洞的危害程度。

4. 根据权利要求 1 所述的方法，其中所述收集所述 WEB 漏洞进一步包括通过网络从 WEB 漏洞源收集所述 WEB 漏洞。

5. 根据权利要求 4 所述的方法，其中所述 WEB 漏洞源包括以下至少一个：WEB 漏洞公布网站和数据库、社区交互网站、新闻门户网站。

6. 根据权利要求 1 所述的方法，其中所述重现所述 WEB 漏洞进一步包括利用虚拟机和相关程序构建靶场环境来重新所述 WEB 漏洞。

7. 根据权利要求 1 所述的方法，其中所述分析所述 WEB 漏洞进一步包括根据所述 WEB 漏洞触发点通过源代码审计技术、分析参数传递过程来获取对所述 WEB 漏洞的根源的描述和所述 WEB 的形成原理。

8. 根据权利要求 1 所述的方法，其中所述利用所述 WEB 漏洞进一步包括生成概念验证 POC 程序来实现 WEB 漏洞利用。

9. 根据权利要求 8 所述的方法，其中所述 WEB 漏洞利用包括以下至少一个：读取数据库内容、读取文件内容、上传后门、代码执行。

10. 根据权利要求 1 至 9 中任一项所述的方法，其中所述防护 WEB 漏洞进一步包括以下至少一个：形成对所述 WEB 漏洞的根源的描述、生成针对所述 WEB 漏洞的修复方案、生成针对所述 WEB 漏洞的检测方案、生成针对所述 WEB 漏洞的防御方案。

11. 根据权利要求 10 所述的方法，进一步包括将针对所述 WEB 漏洞的检测方案转换为用于安全扫描器的扫描规则、将针对所述 WEB 漏洞的防御方案转换为用于安全防火墙的防御规则。

12. 一种用于防护 WEB 漏洞的设备，所述设备包括：

收集装置，用于收集 WEB 漏洞；

重现装置，用于重现所述 WEB 漏洞；

分析装置，用于分析所述 WEB 漏洞；

利用装置，用于基于重现和分析所述 WEB 漏洞的结果来利用所述 WEB 漏洞；

防护装置，用于基于重现、分析和利用所述 WEB 漏洞的结果来防护 WEB 漏洞。

13. 根据权利要求 12 所述的设备，进一步包括筛选装置，用于在收集所述 WEB 漏洞之后基于筛选标准对所收集的所述 WEB 漏洞进行筛选。

14. 根据权利要求 13 所述的设备，其中所述筛选标准包括以下至少一个：所述 WEB 漏

洞的新旧程度、所述 WEB 漏洞的影响范围、利用所述 WEB 漏洞的难易程度、所述 WEB 漏洞的危害程度。

15. 根据权利要求 12 所述的设备，其中所述收集装置进一步包括网络收集装置，用于通过网络从 WEB 漏洞源收集所述 WEB 漏洞。

16. 根据权利要求 15 所述的设备，其中所述 WEB 漏洞源包括以下至少一个 :WEB 漏洞公布网站和数据库、社区交互网站、新闻门户网站。

17. 根据权利要求 12 所述的设备，其中所述重现装置进一步包括构建装置，用于利用虚拟机和相关程序构建靶场环境来重现所述 WEB 漏洞。

18. 根据权利要求 12 所述的设备，其中所述分析装置进一步包括审计装置，用于根据所述 WEB 漏洞触发点通过源代码审计技术、分析参数传递过程来获取对所述 WEB 漏洞的根源的描述和所述 WEB 的形成原理。

19. 根据权利要求 12 所述的设备，其中所述利用装置进一步包括生成装置，用于生成概念验证 POC 程序来实现 WEB 漏洞利用。

20. 根据权利要求 19 所述的设备，其中所述 WEB 漏洞利用包括以下至少一个 :读取数据库内容、读取文件内容、上传后门、代码执行。

21. 根据权利要求 12 至 20 中任一项所述的设备，其中所述防护装置进一步包括以下至少一个 :形成装置，用于形成对所述 WEB 漏洞的根源的描述 ;修复方案生成装置，用于生成针对所述 WEB 漏洞的修复方案 ;检测方法生成装置，生成针对所述 WEB 漏洞的检测方案 ;防御方法生成装置，用于生成针对所述 WEB 漏洞的防御方案。

22. 根据权利要求 21 所述的设备，进一步包括转换装置，用于将针对所述 WEB 漏洞的检测方案转换为用于安全扫描器的扫描规则、将针对所述 WEB 漏洞的防御方案转换为用于安全防火墙的防御规则。

# 用于防护 WEB 漏洞的方法和设备

## 技术领域

[0001] 本发明总体上涉及网络安全，具体地涉及一种用于防护 WEB 漏洞的方法和设备。

## 背景技术

[0002] 随着网络和计算机技术的日益发展，使用网络的人员增多，网络安全环境日益恶化。网络和软件技术的逐渐复杂化为各种网络攻击和黑客行为提供了肥沃的土壤。网络上层出不穷的攻击和不停产生的漏洞使网络使用者不胜其烦，尤其是其中与网络接触频繁 WEB 开发者、各种网站的管理员等深受其害。

[0003] 在各种网络危害中，WEB 漏洞的危害程度很大。具体而言，WEB 漏洞是指 WEB 应用、WEB 框架、WEB 语言和 WEB 服务器等存在的安全隐患。常见的 WEB 漏洞有 SQL 注入漏洞、XSS 漏洞、文件包含漏洞、代码执行漏洞和文件解析漏洞等。攻击者利用 WEB 漏洞可以实现以下恶意操作 :获取网站数据库数据、网站上传后门、网页挂马和植入暗链等。WEB 漏洞的危害之所以严重是因为 WEB 应用使用的操作系统和第三方应用程序中的所有程序错误或者可以被利用的漏洞都是 WEB 漏洞的来源。甚至错误配置也可产生漏洞，并且包含有不安全的默认设置或管理员没有进行安全配置的应用程序也会产生漏洞。例如，WEB 服务器被配置成可以让任何用户从系统上的任何目录路径通过，这样可能会导致泄露存储在 WEB 服务器上的一些敏感信息，如口令、源代码或客户信息等。

[0004] 针对上述 WEB 漏洞，常用的检测和防御工具是 WEB 安全扫描器和 WEB 安全防火墙。WEB 安全扫描器是指针对 WEB 服务器进行扫描检测，以发现其存在安全隐患的设备。WEB 安全防火墙是指为 WEB 服务器提供安全防护的设备。

[0005] 然而，虽然具有检测和防御工具，但是如果不能有效地为其设置扫描和防御规则，往往对于 WEB 漏洞的防护还是无能为力。而设置检测和防御规则必须在对漏洞进行分析并得到其原理之后才能得到更新。这就使规则的更新和对漏洞的防护严重依赖于对漏洞的研究分析结果。只有分析结果越细致、越快速以及越全面才能为 WEB 漏洞的防护提供越有利的条件。现在为了防护 WEB 漏洞而进行的 WEB 安全研究包括 WEB 漏洞收集、WEB 漏洞重现、WEB 漏洞分析和 WEB 漏洞利用，最终形成对 WEB 漏洞的描述信息 :WEB 漏洞名称、WEB 漏洞适用版本、WEB 漏洞描述和 WEB 漏洞利用方法等。而通过这个流程产生的 WEB 漏洞防护是不够全面的，因为现有的 WEB 安全研究方案缺少了对 WEB 漏洞的研究的综合利用，也就是不能将对 WEB 漏洞的重现、分析和利用的结果转换成用于防护漏洞的最终方案。换言之，在现有技术中，对 WEB 漏洞做出的重现、分析以及利用仅仅是为了研究该 WEB 漏洞的特性，而得到的结果并没有被充分利用，这是不利于 WEB 漏洞防护的。并且在现有技术中，WEB 漏洞分析环节不够深入透彻，只形成对漏洞的一个简单描述。

[0006] 因此，在现有 WEB 漏洞防护方法中，对漏洞的分析研究仅仅停留在表面，对漏洞成因的描述也只有片言只语，仅仅是表面上的分析，不够深入，不能指出漏洞的根源所在，这样简单的漏洞分析对后续的防护起不到任何的作用。对比之下，在根据本发明的 WEB 漏洞防护方法中，对 WEB 漏洞的分析更加透彻，能够指出漏洞产生的根源所在，分析出漏洞触发

的整个过程；通过深入详细的漏洞分析，最终给出针对性的修复方案、扫描方法以及防御方法，这对 WEB 漏洞防护具有积极的意义。

[0007] 此外，现有的 WEB 漏洞防护方法缺少对 WEB 漏洞的综合分析和转换环节，仅仅是对单个 WEB 漏洞的分析研究，不能将 WEB 安全研究分析的成果转化为 WEB 安全扫描器和 WEB 安全防火墙的规则。在根据本发明的 WEB 漏洞防护方法中，可以及时地将针对 WEB 漏洞的重现、分析和利用成果转换成 WEB 漏洞扫描规则和 WEB 漏洞防御规则，供 WEB 安全扫描器和 WEB 安全防火墙使用，这极大的提高了 WEB 安全扫描和 WEB 安全防御的及时性和准确性。换言之，根据本发明的技术方案充分利用了对 WEB 漏洞的分析、重现和利用的成果，其成果的基础上发展出 WEB 漏洞防护的有效方案并能够全方位地覆盖 WEB 漏洞从产生到危害的各个环节。

## 发明内容

[0008] 因此，本发明的目的在于针对日益恶化的网络安全环境提供一种用于及时、准确以及全面地防护 WEB 漏洞的方法和设备。

[0009] 在本发明的第一方面中，本发明提供一种用于防护 WEB 漏洞的方法。所述方法包括：收集 WEB 漏洞；重现所述 WEB 漏洞；分析所述 WEB 漏洞；基于重现和分析所述 WEB 漏洞的结果来利用所述 WEB 漏洞；基于重现、分析和利用所述 WEB 漏洞的结果来防护 WEB 漏洞。

[0010] 在本发明的一个优选实施例中，所述方法进一步包括在收集所述 WEB 漏洞之后基于筛选标准对所收集的所述 WEB 漏洞进行筛选。

[0011] 在本发明的一个优选实施例中，在所述方法中，所述筛选标准包括以下至少一个：所述 WEB 漏洞的新旧程度、所述 WEB 漏洞的影响范围、利用所述 WEB 漏洞的难易程度、所述 WEB 漏洞的危害程度。

[0012] 在本发明的一个优选实施例中，在所述方法中，所述收集所述 WEB 漏洞进一步包括通过网络从 WEB 漏洞源收集所述 WEB 漏洞。

[0013] 在本发明的一个优选实施例中，在所述方法中，所述 WEB 漏洞源包括以下至少一个：WEB 漏洞公布网站和数据库、社区交互网站、新闻门户网站。

[0014] 在本发明的一个优选实施例中，在所述方法中，所述重现所述 WEB 漏洞进一步包括利用虚拟机和相关程序构建靶场环境来重新所述 WEB 漏洞。

[0015] 在本发明的一个优选实施例中，在所述方法中，所述分析所述 WEB 漏洞进一步包括根据所述 WEB 漏洞触发点通过源代码审计技术、分析参数传递过程来获取所述 WEB 漏洞的根源和所述 WEB 的形成原理。

[0016] 在本发明的一个优选实施例中，在所述方法中，所述利用所述 WEB 漏洞进一步包括生成概念验证 POC 程序来实现 WEB 漏洞利用。

[0017] 在本发明的一个优选实施例中，在所述方法中，WEB 漏洞利用包括以下至少一个：读取数据库内容、读取文件内容、上传后门、代码执行。

[0018] 在本发明的一个优选实施例中，在所述方法中，所述防护 WEB 漏洞进一步包括以下至少一个：形成对所述 WEB 漏洞的根源的描述、生成针对所述 WEB 漏洞的修复方案、生成针对所述 WEB 漏洞的检测方法、生成针对所述 WEB 漏洞的防御方法。

[0019] 在本发明的一个优选实施例中，所述方法进一步包括将针对所述 WEB 漏洞的检测

方法转换为用于安全扫描器的扫描规则、将针对所述 WEB 漏洞的防御方法转换为用于安全防火墙的防御规则。

[0020] 在本发明的第二方面中，提供一种用于防护 WEB 漏洞的设备。所述设备包括：收集装置，用于收集 WEB 漏洞；重现装置，用于重现所述 WEB 漏洞；分析装置，用于分析所述 WEB 漏洞；利用装置，用于基于重现和分析所述 WEB 漏洞的结果来利用所述 WEB 漏洞；防护装置，用于基于重现、分析和利用所述 WEB 漏洞的结果来防护 WEB 漏洞。

[0021] 在本发明的一个优选实施例中，所述设备进一步包括筛选装置，用于在收集所述 WEB 漏洞之后基于筛选标准对所收集的所述 WEB 漏洞进行筛选。

[0022] 在本发明的一个优选实施例中，在所述设备中，所述筛选标准包括以下至少一个：所述 WEB 漏洞的新旧程度、所述 WEB 漏洞的影响范围、利用所述 WEB 漏洞的难易程度、所述 WEB 漏洞的危害程度。

[0023] 在本发明的一个优选实施例中，在所述设备中，所述收集装置进一步包括网络收集装置，用于通过网络从 WEB 漏洞源收集所述 WEB 漏洞。

[0024] 在本发明的一个优选实施例中，在所述设备中，所述 WEB 漏洞源包括以下至少一个：WEB 漏洞公布网站和数据库、社区交互网站、新闻门户网站。

[0025] 在本发明的一个优选实施例中，在所述设备中，所述重现装置进一步包括构建装置，用于利用虚拟机和相关程序构建靶场环境来重现所述 WEB 漏洞。

[0026] 在本发明的一个优选实施例中，在所述设备中，所述分析装置进一步包括审计装置，用于根据所述 WEB 漏洞触发点通过源代码审计技术、分析参数传递过程来获取所述 WEB 漏洞的根源和所述 WEB 的形成原理。

[0027] 在本发明的一个优选实施例中，在所述设备中，所述利用装置进一步包括生成装置，用于生成概念验证 POC 程序来实现 WEB 漏洞利用。

[0028] 在本发明的一个优选实施例中，在所述设备中，所述 WEB 漏洞利用包括以下至少一个：读取数据库内容、读取文件内容、上传后门、代码执行。

[0029] 在本发明的一个优选实施例中，在所述设备中，所述防护装置进一步包括以下至少一个：形成装置，用于形成对所述 WEB 漏洞的根源的描述；修复方案生成装置，用于生成针对所述 WEB 漏洞的修复方案；检测方法生成装置，生成针对所述 WEB 漏洞的检测方法；防御方法生成装置，用于生成针对所述 WEB 漏洞的防御方法。

[0030] 在本发明的一个优选实施例中，所述设备进一步包括转换装置，用于将针对所述 WEB 漏洞的检测方法转换为用于安全扫描器的扫描规则、将针对所述 WEB 漏洞的防御方法转换为用于安全防火墙的防御规则。

[0031] 从以上本发明的各个方面可以看出，根据本发明的方法和设备相对于现有技术具有以下优势：

根据本发明的用于防护 WEB 漏洞的方法和设备实现了对 WEB 漏洞的直观重现和本质分析，提供了修复方案，并为 WEB 安全扫描器和 WEB 安全防火墙提供了规则，极大的提高了扫描和防御的及时性和准确性。并且，在根据本发明的方法和设备中，对于 WEB 漏洞的分析更加透彻，能够指出漏洞产生的根源所在，分析出漏洞触发的整个过程；通过深入详细的漏洞分析，可以方便的给出针对性的修复方案、扫描方法以及防御方法，由此极大地增强了 WEB 安全性。

## 附图说明

[0032] 下面参考结合附图所进行的下列描述，以便更透彻地理解本公开内容，在附图中：

图 1 是根据本发明实施例的用于防护 WEB 漏洞的方法的流程图。

[0033] 图 2 是详细示出了利用 WEB 漏洞重现、WEB 漏洞分析和 WEB 漏洞利用的结果来进行 WEB 漏洞防护的框图。

[0034] 图 3 是根据本发明实施例的用于防护 WEB 漏洞的设备的框图。

## 具体实施方式

[0035] 下面将详细描述本发明的具体实施例，在附图中示出了本发明的实施例。然而，可以以许多不同形式来体现本发明，并且不应将其理解为局限于本文阐述的实施例。相反，提供这些实施例使得本公开将是透彻和完整的，并将向本领域的技术人员全面传达本发明的范围。相同的附图标记自始至终指示相同的元素。

[0036] 应理解的是，虽然术语“第一”、“第二”等在本文中可以用来描述各种元素，但这些元素不应受到这些术语的限制。这些术语仅用来将一个元素与另一个区别开。

[0037] 本文所使用的术语仅仅是出于描述特定实施例的目的，并且并不意图限制本发明。除非上下文明确指明，本文所使用的单数形式“一个”、“一种”和“该”意图也包括复数形式。还应理解的是当在本文中使用时，术语“包括”和 / 或“包含”指定所述特征、整体、步骤、操作、元素和 / 或组件的存在，但是不排除一个或多个其他特征、整体、步骤、操作、元素、组件和 / 或其群组的存在或添加。

[0038] 除非另外定义，本文所使用的所有术语（包括技术和科学术语）具有与本发明所属领域的普通技术人员一般理解的相同的意义。还应理解的是应将本文所使用的术语解释为具有与其在本说明书和相关领域的上下文中的意义一致的意义，并且不应以理想化或过度形式化的意义来进行解释，除非在本文中明确地这样定义。

[0039] 在以下描述中，除非明确指出，术语“WEB 漏洞”和“漏洞”可以互换使用，它们都表示 WEB 漏洞这个含义。

[0040] 下面结合附图对本发明的实施例进行描述。

[0041] 在附图 1 中，示出根据本发明实施例的用于防护 WEB 漏洞的方法的流程图。

[0042] 在该流程图中，步骤 S101 是收集 WEB 漏洞的步骤。对 WEB 漏洞的收集是实现整个 WEB 漏洞防护方法的基础。只有掌握了 WEB 漏洞的整体情况，才能有针对性的进行防护。收集过程本身就是对 WEB 漏洞流行的内在规律进行了解的过程。例如，在根据本发明的收集过程中，发现某种漏洞的数量近期突然呈现爆炸式增长，那么就此可以得出近期需要重点防护该种漏洞且产生该种漏洞的条件可能最近被披露或被发现、甚至于得到 WEB 漏洞发展的某种宏观趋势的结论。这个结论看似简单，但是可以为后续步骤给出指导性方向。所以收集 WEB 漏洞的步骤非常重要。

[0043] 根据本发明，收集 WEB 漏洞可以采用自动方式和人工方式。在采取自动方式时，可以利用 WEB 漏洞自动收集程序、基于 WEB 漏洞特征库来从可以获得或者检测到漏洞的各种漏洞源来收集漏洞。自动收集程序可以利用内建的收集模型（例如，斯坦福大学提出的对象

交换模型)来收集 WEB 漏洞。自动收集方式毫无疑问是高效率和准确的,采用自动收集方式可以应对大的漏洞收集工作量,所以一般而言对于 WEB 漏洞的收集都采用自动收集方式。

[0044] 然而,自动收集方式也有可能存在某些缺点,例如程序有可能不能有针对性地收集某类漏洞,对新漏洞的出现情况无法了解等等。这时候就可以采用人工收集的方式,而且人工收集可以更加灵活地应对漏洞发生情况。例如,在对某类突然爆发的漏洞初步分析后,有针对性的收集某个或某些漏洞来进一步分析,而不是像自动收集程序那样不予区分地无差别收集。这在某些情况下无疑也可以提高漏洞收集的效率、及时性和准确性。

[0045] 在一个实施例中,在收集 WEB 漏洞之后或者在收集 WEB 漏洞过程之中,还可以包括基于筛选标准对所收集的 WEB 漏洞进行筛选的步骤。这一筛选步骤也可以采用自动方式和人工方式。添加筛选所收集的 WEB 漏洞的步骤具有的最重要优点就是加强针对性。因为对一些 WEB 应用的开发者和网站管理员而言,防护最近流行程度高、危害程度严重的 WEB 漏洞显然要比仅仅是常规地防护一些常见的 WEB 漏洞更加重要。

[0046] 因此,在一个实施例中,在筛选过程中,筛选标准可以包括以下至少一个 :WEB 漏洞的新旧程度、WEB 漏洞的影响范围、利用 WEB 漏洞的难易程度、WEB 漏洞的危害程度。

[0047] 很显然,在同一类 WEB 漏洞中,新产生的 WEB 漏洞往往要比之前产生的 WEB 漏洞更具有分析价值,也更需要防护。所以在筛选时,可以按照 WEB 漏洞的新旧程度来进行筛选。当然,也许很久以前的 WEB 漏洞在新的环境中产生了新的危害,那么它对于分析程序和人员来说也可能具有比新产生的 WEB 漏洞更大的价值,那么也可以将其筛选出来。总而言之,可以将 WEB 漏洞的新旧程度作为筛选标准之一而加以利用。类似地,利用筛选标准 -WEB 漏洞的影响范围可以筛选出不同影响范围的 WEB 漏洞。例如,对全球产生影响、只影响国内、甚至只影响某个局域网或某个 WEB 应用等。同样,筛选标准 - 利用 WEB 漏洞的难易程度可以筛选出利用难易程度不同的 WEB 漏洞。例如,某些 WEB 漏洞更容易被利用,那么就可以优先加以分析和防护,而不易利用的 WEB 漏洞就可以放在后面再行分析。此外,较为重要的筛选标准就是 WEB 漏洞的危害程度。这一筛选标准可以筛选出危害程度不同的 WEB 漏洞。例如,仅仅破坏某个 WEB 应用的 WEB 漏洞显然要比动辄就破坏整个系统、甚至于破坏整个网络的 WEB 漏洞危害程度低。

[0048] 通过使用上述这些筛选标准来收集或者指导后续的分析步骤,可以使 WEB 漏洞防护方法以某种优先级来分析处理符合不同标准的 WEB 漏洞,进而实现高效、准确的 WEB 漏洞防护。

[0049] 在一个实施例中,在收集方式上,自动收集程序和人工收集都可以通过网络从 WEB 漏洞源收集所述 WEB 漏洞。但是这两种收集方式也可以使用其他途径来收集漏洞。例如,负责人工收集的人员可以听取或者阅读某些 WEB 漏洞描述来实现对 WEB 漏洞的收集,在这种情况下可以使用各种通信交流手段来收集 WEB 漏洞。

[0050] 然而,在一个实施例中,通过网络来收集 WEB 漏洞显然是一种高效的方式,而且网络上的 WEB 漏洞源也更加丰富和准确。WEB 漏洞源可以包括以下至少一个 :WEB 漏洞公布网站和数据库、社区交互网站、新闻门户网站。例如,漏洞收集人员或者自动收集程序可以浏览、搜索 WEB 漏洞发布网站和数据库,其包括但不限于国家信息安全漏洞共享平台 -www.cnvd.org.cn、中国国家信息安全漏洞库 -www.cnnvd.org.cn、著名的乌云网站 -www.wooyun.org、www.securityfocus.com、www.exploit-db.com 等。漏洞收集人员或者自动收

集程序还可以通过新浪微博、腾讯微博、twitter 等社交网站来收集 WEB 漏洞。甚至还可以通过一些新闻门户网站(例如,www.sohu.com、www.163.com 等)、任意其他网上站点、甚至于一些独立的服务器来收集 WEB 漏洞。

[0051] 在一个实施例中,在从这些漏洞源收集 WEB 漏洞的过程中,可以采用 SQL 语言查询漏洞数据库的方式、可以采取解析 XML 语言获取其中数据的方式、可以采取网络爬虫的方式、甚至于可以采取人工阅读某些信息的方式来收集 WEB 漏洞。总而言之,可以采用一切获取信息的手段来收集 WEB 漏洞。

[0052] 在完成了收集 WEB 漏洞的步骤之后,就要对所收集的 WEB 漏洞进行重现。如图 1 中的步骤 S102 所示。在一个实施例中,重现 WEB 漏洞可以包括利用虚拟机和相关程序构建靶场环境来重现所述 WEB 漏洞。重现 WEB 漏洞的意义在于可以弄清和复查触发该 WEB 漏洞的各种条件,其包括 WEB 漏洞的产生环境和直接触发条件。

[0053] 为了重现 WEB 漏洞,需要搭建靶场环境,通常为虚拟机环境。可以参考漏洞公布信息,针对不同的 WEB 漏洞,在靶场环境中使用特定的 WEB 服务器操作系统、WEB 容器、WEB 语言、数据库、WEB 应用、WEB 框架、WEB 插件或者 WEB 浏览器。最后可以再次参考漏洞公布信息,构建漏洞触发的特定条件,重现该 WEB 漏洞。在搭建靶场环境的过程中,要特别注意的是需要使用存在漏洞的版本,并且确保其没有被打补丁。若根据漏洞公布信息中的方法来重现漏洞没有成功,则可以考虑该漏洞的触发是否依赖于其他特定的条件。

[0054] 针对每个 WEB 安全漏洞,例如可以创建一个 vmware 虚拟机,在该虚拟机中安装触发该漏洞所需要的各特定的操作系统和 WEB 程序。例如,操作系统(windows、linux 等)、WEB 容器(iis、apache、tomcat 等)、WEB 语言(asp、php、jsp 等)、数据库(mysql、oracle、mssql 等)、WEB 应用(Discuz、Wordpress 等)、WEB 框架(django、thinkphp 等)、WEB 插件(Buddypress、TimThumb 等)、WEB 浏览器(IE、firefox、chrome 等)。

[0055] 在搭建靶场环境的基础上,参考漏洞发布信息,获取触发该漏洞所需要的特定条件和触发流程,例如访问某个 url,或者上传某个文件等。结合 vmware 虚拟机和漏洞触发条件,我们可以重现该 WEB 漏洞。

[0056] 例如,在从网上收集了公布的一个针对 Discuz 论坛程序(版本 2.0)的 SQL 注入漏洞之后如下重现该漏洞。首先新建一个 vmware 虚拟机,在该虚拟机中安装 linux 操作系统、apache 服务器、php 语言、mysql 数据库、Discuz 论坛程序(版本 2.0,未打补丁)。安装完成之后,执行使用任意浏览器访问这个 Discuz 论坛的一个特定 url 的操作,该操作的结果是显示出该论坛数据库的内容。这就实现了该 SQL 注入漏洞的重现。

[0057] 在重现 WEB 漏洞的步骤中,可以得知 WEB 漏洞的触发点,进而进入漏洞 WEB 漏洞的分析步骤。如图 1 中的步骤 S103 所示。漏洞分析环节是整个 WEB 漏洞防护方法的核心步骤。通过该 WEB 漏洞分析环节,可以获得 WEB 漏洞的产生根源。漏洞重现步骤仅仅重现了 WEB 漏洞的表面现象,但是漏洞分析步骤是一个由表到里进行分析的步骤,是一个追根究底、推本溯源的步骤。

[0058] 在一个实施例中,分析 WEB 漏洞可以包括根据 WEB 漏洞触发点通过源代码审计技术、分析参数传递过程来获取所述 WEB 漏洞的根源和所述 WEB 的形成原理。一般而言,漏洞分析方法一般可以包括补丁对比、端点调试、程序关联关系、数据传递跟踪、程序流程跟踪等等。WEB 漏洞的根源可以包括输入未验证、输出未验证、权限未验证、逻辑错误等等。

[0059] 例如，在这个 WEB 漏洞分析步骤中，可以在源码层次上对 WEB 漏洞进行分析：若有官方补丁发布，则可以对比补丁，定位到漏洞点，并根据数据传递流程和程序执行流程，找到漏洞的触发点；若没有官方补丁，参考漏洞公布的相关信息，分析程序间的文件关联关系，追踪程序的执行流程和数据的传递过程，结合给程序下断点进行调试的方法，找出漏洞的根源所在，并说明在何种条件下，程序在何种运行流程时，会导致漏洞的触发。

[0060] 以下面的 WEB 漏洞分析示例来进行进一步的说明。仍就某个针对 Discuz 论坛程序（版本 2.0）的 SQL 注入漏洞进行说明。该漏洞触发点是访问某个特定 url。我们针对版本 2.0 的 Discuz 论坛程序进行源代码审计，分析该特定 url 中的特殊输入参数，分析过程接收该参数后，如何经过多次的参数传递和参数处理流程，将用户的输入放进 SQL 查询语句中，并将 SQL 查询语句的结果展现在输出页面上。至此，输出页面上呈现的结果提供了漏洞根源所在以及漏洞形成原理。

[0061] 在进行了上述的漏洞分析和漏洞重现步骤之后，基于重现和分析 WEB 漏洞的结果来利用所述漏洞。如图 1 的步骤 S104 所示。具体而言，漏洞利用步骤可以在得到 WEB 漏洞根源的所在以及该 WEB 漏洞的触发流程的基础上，具体且详细地利用某种手段来更透彻地分析漏洞，也即漏洞利用步骤是更深入了解 WEB 漏洞的一个必不可少的步骤。利用 WEB 漏洞的目的在于更进一步地了解该 WEB 漏洞的运行原理，验证在分析步骤中得到的漏洞根源是否正确以及其危害程度的大小，从而可以更有针对性地来进行防护。

[0062] 在一个实施例中，利用 WEB 漏洞的步骤可以包括生成概念验证 POC 程序来实现 WEB 漏洞利用。POC（Proof of Concept）程序、即 POC 验证程序的主要功能就是针对漏洞的形成原理和触发方法来进行程序验证，从而在重现 WEB 漏洞的靶场环境中利用分析结果真实具体地看到该漏洞产生的结果和可能产生的危害。简言之，就是针对特定的漏洞原理，编写特定的 POC 程序，实现特定的目标。

[0063] 在一个实施例中，WEB 漏洞利用可以包括以下至少一个：读取数据库内容、读取文件内容、上传后门、代码执行等。这些手段通常都是用于针对 WEB 漏洞进行攻击的手段。换言之，就是恶意攻击者利用 WEB 漏洞所能实现的功能。所以，只有通过 POC 程序实现了这些针对 WEB 漏洞的既定目标，才能具体且真实地了解该漏洞的内部实现细节或方法，从而为防护提供多方面的信息。

[0064] 现仍以上述论坛 SQL 注入漏洞来简要解释 WEB 漏洞利用的过程。例如，针对该 SQL 注入漏洞，编写 POC 程序。结合 Vmware 虚拟机的靶场环境，利用 POC 程序可以获取该网站的数据库内容。针对代码执行漏洞，编写 POC 程序。结合 Vmware 虚拟机的靶场环境，利用该 POC 程序可以获取网站的 Webshell 后门。

[0065] 以上对 WEB 漏洞的重现、分析和利用目的都在于寻求对 WEB 漏洞的透彻理解，以便为防护该 WEB 漏洞提供必要的信息。在掌握了这些信息之后，根据本发明的方法可以基于重现、分析和利用所述 WEB 漏洞的结果来防护 WEB 漏洞，如图 1 的步骤 S105 所示。

[0066] 如图 1 所示的本发明的 WEB 漏洞防护方法，本领域技术人员应该理解，其中所示步骤的为示例性的，实际中也可以不按照所示顺序执行。或者，可以添加或者省略步骤。例如，在已有 WEB 漏洞基础上执行本发明就可以省略收集步骤。

[0067] 现在，将结合图 2 详细描述 WEB 漏洞的防护方法。图 2 是详细示出了利用 WEB 漏洞重现、WEB 漏洞分析和 WEB 漏洞利用的结果来进行 WEB 漏洞防护的框图。

[0068] 在根据本发明的方法的实施例中并如图 2 所示，对 WEB 漏洞的方法 200 可以包括以下至少一个：如框 201 所示，形成对 WEB 漏洞的根源的描述、如框 202 所示，生成针对 WEB 漏洞的修复方案、如框 203 所示，生成针对 WEB 漏洞的检测方案、如框 204 所示，生成针对 WEB 漏洞的防御方案。

[0069] 上述这些 WEB 漏洞防护方面可以单独使用也可以组合使用，并且这些方面可以提供对 WEB 漏洞全方位的防护，即，为 WEB 漏洞的产生源头 - 开发人员开始一直到 WEB 漏洞的受害者 - 可能包括网站管理员(站长)、WEB 应用人员等、直至为防护 WEB 漏洞的防火墙和扫描器提供全面的应对方案。这在现有技术的 WEB 漏洞防护方法中是没有的。因为现有技术的方法仅仅是对单个 WEB 漏洞的分析研究，且不能将 WEB 分析研究的成果应用于 WEB 漏洞的产生 - 传播 - 封堵的整个链条。根据本发明的方法因此相对于现有技术的方法具有防护全面、具有更好的及时性和准确性的优势。

[0070] 下面，具体地阐述这些防护步骤。之所以采用这四个防护方面，是因为可以为 WEB 漏洞危害链条上的所有人员和程序提供全面的应对方案。如图所示，其最终可以应用于 WEB 开发人员 210、网站站长、管理员 220、WEB 安全扫描器 230 以及 WEB 安全防火墙 240。本领域技术人员应该理解，该附图仅为示例性而非限制性的。并且，所产生的最终防护方案可以以各种形式提供给需要的各种人员或设备，而不限于图中所示的 210 至 240 这四个方面。

[0071] 在经过 WEB 漏洞重现、分析和利用之后，对 WEB 漏洞的根源或触发流程等都有了很透彻的了解。但是这些了解仅仅停留在程序运行结果方面，例如上述在网页上呈现的数据库内容、POC 程序的运行结果等。而 WEB 开发人员对此可能并不了解，也就无法在程序设计和开发的阶段来预防 WEB 漏洞的形成。所以，根据本发明的 WEB 漏洞防护方法在获得 WEB 漏洞的根源等信息之后，可以形成对 WEB 漏洞的根源的各种有用描述。这些描述所采用的方式包括但不限于：人员能够以自然阅读方式获取的自然语言描述方式、以各种格式形成的机器可读格式，例如 XML 语言形成的描述以及可以由 WEB 漏洞防护人员或机器可获得的任何其他描述方式。而且，提供这些描述的方式也可以多种多样。例如，通过网页提供、通过各种通信软件或硬件以消息形式提供、以语音方式的自然语言提供以及以可以使人员或机器获得信息的任何其他方式提供。

[0072] 这种描述显然可以使 WEB 开发者在设计开发 WEB 应用时，不要再犯类似的错误，也就是从源头防止了 WEB 漏洞的产生。这种方式显然是效率最高的方式，也是本发明的优势之一。而且这些根源描述也并非只有 WEB 开发者可以利用，任何程序或硬件的开发者都可以从中获取自己需要的信息以防止漏洞的发生。

[0073] 其次，根据本发明的 WEB 漏洞防护方法可以形成生成针对 WEB 漏洞的修复方案。

[0074] 当 WEB 漏洞开始在网络上蔓延时，各种防护软件有可能还未针对该漏洞进行更新。所以，在 WEB 漏洞发展的初期进行防护也具有重大意义。而在这种突然出现的威胁面前，各种网站的管理员、站长等往往束手无策。因为他们对造成危害的 WEB 漏洞一无所知，并且因此也就没有任何防护措施。然而，根据本发明的防护方法在 WEB 漏洞危害的初期阶段就可以提供针对该 WEB 漏洞的修复方案以便向受到危害的各种人员迅速提供支援，也有可能将 WEB 漏洞的危害性降至最低。例如，该修复方案可以是对 WEB 漏洞进行手工操作修复的描述，也可以是一个程序补丁等。这种修复方案有可能可以快速地被网站站长、管理员加以利用而不必等待防火墙等软件的更新。但是，出于应急的目的，此类修复方式有可能仅

针对当前流行的主要危害方式提供修复。换言之，修复方案可能无法提供全面的防御。因此，根据本发明的方法还提供后续的方案来进一步完善防护步骤。

[0075] 以上两个方面可以为各种人员提供针对 WEB 漏洞的紧急应对方式，适合在 WEB 威胁出现之后的短时间内进行及时地防护。

[0076] 此外，根据本发明的方法还可以生成针对 WEB 漏洞的检测方案和针对 WEB 漏洞的防御方案。这两种方案可以针对 WEB 漏洞提供更全面的防护。针对 WEB 漏洞生成检测方案的目的在于提供全面检测存在的 WEB 漏洞的方案。由于有些 WEB 漏洞在没有被触发之前处于潜伏状态并且因此暂时没有表现出危害性，这时如果不将其检测出来，那么其就有可能成为潜在的威胁并且在意想不到的时候爆发。所以，提供对 WEB 漏洞的全面检测方案是十分有必要的。

[0077] 类似地，提供针对 WEB 漏洞的全面防御方案也是有必要的。因为，如上所述，修复方案可能仅提供针对某种具体触发方式的修复，而无法全面防御。所以可能稍后提供的全面防御方案将可以提供对 WEB 漏洞的全面防御以防止利用该 WEB 漏洞所能实现的任何攻击和危害后果。

[0078] 在一个实施例中，根据本发明的方法还可以包括将针对 WEB 漏洞的检测方案转换为用于安全扫描器的扫描规则、将针对 WEB 漏洞的防御方案转换为用于安全防火墙的防御规则。

[0079] 毕竟，对于 WEB 漏洞的防护仅仅依靠人工方式是不够的，WEB 安全防火墙和扫描器可以提供更加快捷、自动和全面的防护。所以将检测方案和防御方案转换为 WEB 安全防火墙和扫描器的扫描和防御规则是更有效率地防护 WEB 漏洞的方式。

[0080] 下面以具体示例来说明根据本发明的 WEB 漏洞防护方法。本领域技术人员应该明白，本发明所示示例均是说明性而非限制性的。

[0081] 例如，针对某个 WEB 应用程序的 SQL 注入漏洞，经过 WEB 漏洞重现、分析和利用，发现漏洞根源在于程序对于用户输入的 id 参数没有进行有效过滤。程序中的 SQL 查询语句例如为“select title,content from paper where id = $id”，其中需要限制$id参数的输入为数字型参数。但是由于程序员的粗心，并没有对 $id 参数进行限制，导致用户可以对 $id 参数任意赋值，从而导致了 SQL 注入漏洞的产生。当恶意用户访问形如”http://www.xxx.com/xxx.php?id=1 union select username,password from admin”的 url 链接时，程序中接收到的 $id 参数为“1 union select username,password from admin”，其不是数字型的，从而导致返回页面中将会出现网站管理员的用户名和密码。

[0082] 针对这个 SQL 注入漏洞进行防护体现在以下四个方面：

1. 形成对漏洞根源的描述并提供给该 WEB 应用的程序员：没有对 $id 参数进行有效过滤和限制，从而导致了恶意用户可以对 $id 参数任意赋值。WEB 应用开发者在收到该描述之后，可以从该案例中吸取经验教训，避免出现对用户输入不加以限制的错误。

[0083] 2. 针对漏洞根源，提出漏洞修复方案：在程序中对 $id 参数进行过滤限制，仅允许为数字型的 $id 参数进入到程序中。该修复方案可以供网站站长使用，从而避免网站遭受攻击。

[0084] 3. 从漏洞检测的角度对漏洞提出检测方案并转换为安全扫描器规则。可以在扫描器中加入以下的检测规则：分别访问“xxx.php?id=1 and 1=1”和“xxx.php?id=1 and 1=2”

两个 url，两个返回页面内容不一样，则说明该网站存在 SQL 注入漏洞。

[0085] 4. 从漏洞防御的角度对漏洞提出防御方案并转换为安全防火墙规则。可以在防火墙中加入以下的防御规则：当用户提交 url 形如”xxx.php?id=1 union select name,password from admin”时，判断 id 参数为非数字型，且包含了 union / select 等关键字符串，则阻止用户的该次请求。

[0086] 综上所述，根据本发明的用于防护 WEB 漏洞的方法可以对 WEB 漏洞形成全面、及时和准确的防护。并且，本领域技术人员应该理解，本发明的方法不仅可以用于防护 WEB 漏洞，也可以用于防护网络上的其他漏洞和危害。而且，在描述本发明的方法中所述的步骤顺序也不是限制性的，某些步骤可以不以描述的顺序进行或者省略某些步骤。例如，如果预先对某个 WEB 漏洞的原理有一定的了解，那么可以不进行漏洞重现步骤而直接跳到分析和利用步骤以节约时间。

[0087] 下面结合图 3 描述根据本发明的用于防护 WEB 漏洞的设备。图 3 是根据本发明实施例的用于防护 WEB 漏洞的设备的框图。

[0088] 在图 3 中，所述设备 300 可以包括：收集装置 301，可以用于收集 WEB 漏洞；重现装置 302，可以用于重现所述 WEB 漏洞；分析装置 303，可以用于分析所述 WEB 漏洞；利用装置 304，可以用于基于重现和分析所述 WEB 漏洞的结果来利用所述 WEB 漏洞；防护装置 305，可以用于基于重现、分析和利用所述 WEB 漏洞的结果来防护 WEB 漏洞。

[0089] 优选地，该设备可以进一步包括筛选装置，用于在收集所述 WEB 漏洞之后基于筛选标准对所收集的所述 WEB 漏洞进行筛选。

[0090] 并且，优选地，所述筛选标准可以包括以下至少一个：所述 WEB 漏洞的新旧程度、所述 WEB 漏洞的影响范围、利用所述 WEB 漏洞的难易程度、所述 WEB 漏洞的危害程度。

[0091] 优选地，在该设备中，所述收集装置可以进一步包括网络收集装置，用于通过网络从 WEB 漏洞源收集所述 WEB 漏洞。

[0092] 优选地，在该设备中，所述 WEB 漏洞源可以包括以下至少一个：WEB 漏洞公布网站和数据库、社区交互网站、新闻门户网站。

[0093] 优选地，在该设备中，所述重现装置可以进一步包括构建装置，用于利用虚拟机和相关程序构建靶场环境来重现所述 WEB 漏洞。

[0094] 优选地，在该设备中，所述分析装置可以进一步包括审计装置，用于根据所述 WEB 漏洞触发点通过源代码审计技术、分析参数传递过程来获取对所述 WEB 漏洞的根源的描述和所述 WEB 的形成原理。

[0095] 优选地，在该设备中，所述利用装置可以进一步包括生成装置，用于生成概念验证 POC 程序来实现 WEB 漏洞利用。

[0096] 优选地，在该设备中，所述 WEB 漏洞可以利用包括以下至少一个：读取数据库内容、读取文件内容、上传后门、代码执行。

[0097] 优选地，在该设备中，所述防护装置可以进一步包括以下至少一个：形成装置，用于形成对所述 WEB 漏洞的根源的描述；修复方案生成装置，用于生成针对所述 WEB 漏洞的修复方案；检测方法生成装置，生成针对所述 WEB 漏洞的检测方案；防御方法生成装置，用于生成针对所述 WEB 漏洞的防御方案。

[0098] 优选地，该设备可以进一步包括转换装置，用于将针对所述 WEB 漏洞的检测方案

转换为用于安全扫描器的扫描规则、将针对所述 WEB 漏洞的防御方案转换为用于安全防火墙的防御规则。

[0099] 综上所示，根据本发明的用于防护 WEB 漏洞的方法可以针对 WEB 漏洞形成发展的整个链条进行全面的防护。并且可以为涉及 WEB 漏洞的各种人员和程序都提供应对防护方案，使对 WEB 漏洞的防护变得及时、全面、高效和准确。

[0100] 虽然上述已经结合附图描述了本发明的具体实施例，但是本领域技术人员在不脱离本发明的精神和范围的情况下，可以对本发明进行各种改变、修改和等效替代。这些改变、修改和等效替代都意为落入随附的权利要求所限定的精神和范围之内。

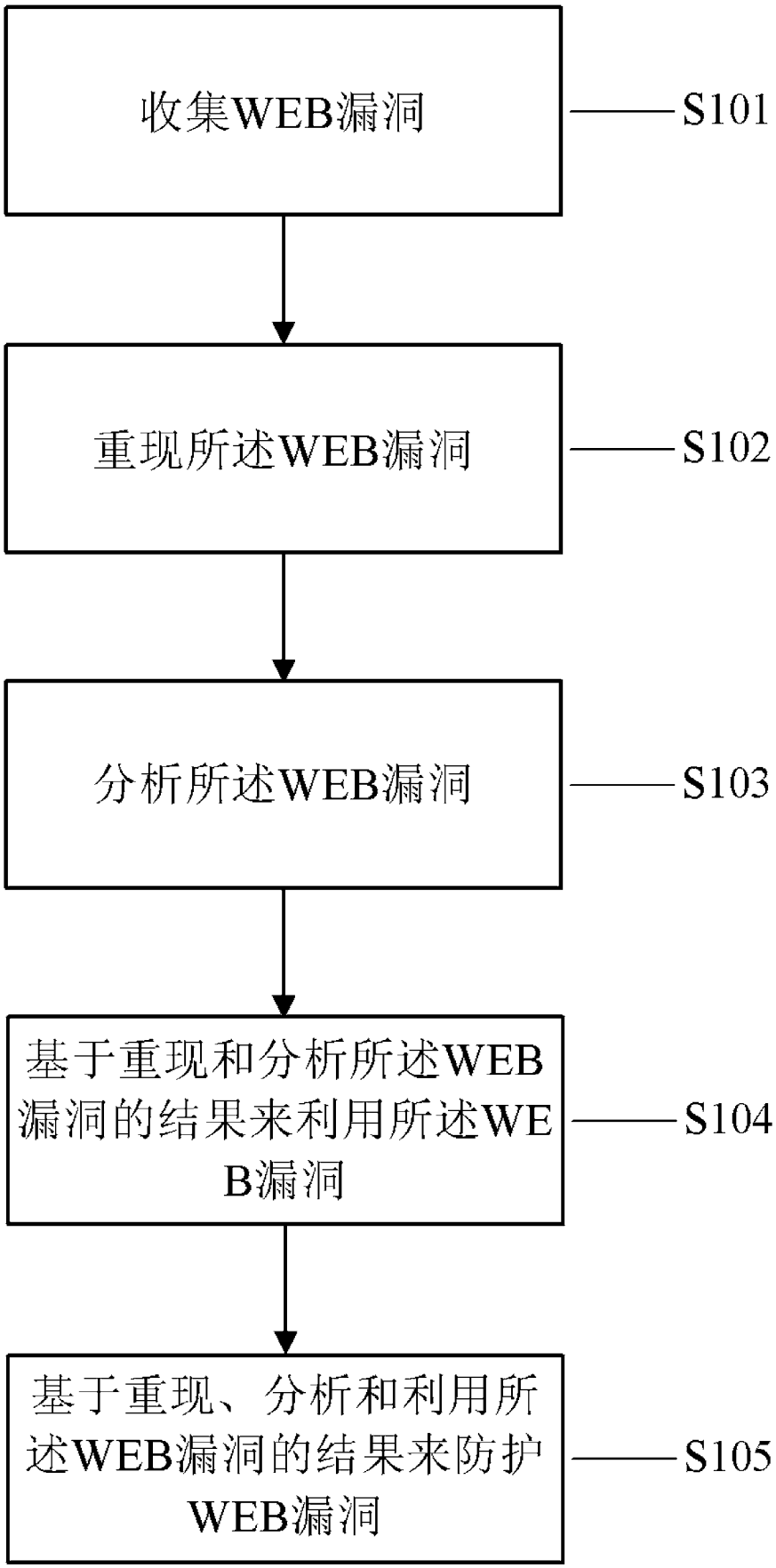

收集WEB漏洞
S101
重现所述WEB漏洞
S102
分析所述WEB漏洞
S103
基于重现和分析所述WEB漏洞的结果来利用所述WEB漏洞
S104
基于重现、分析和利用所述WEB漏洞的结果来防护WEB漏洞
S105

图 1

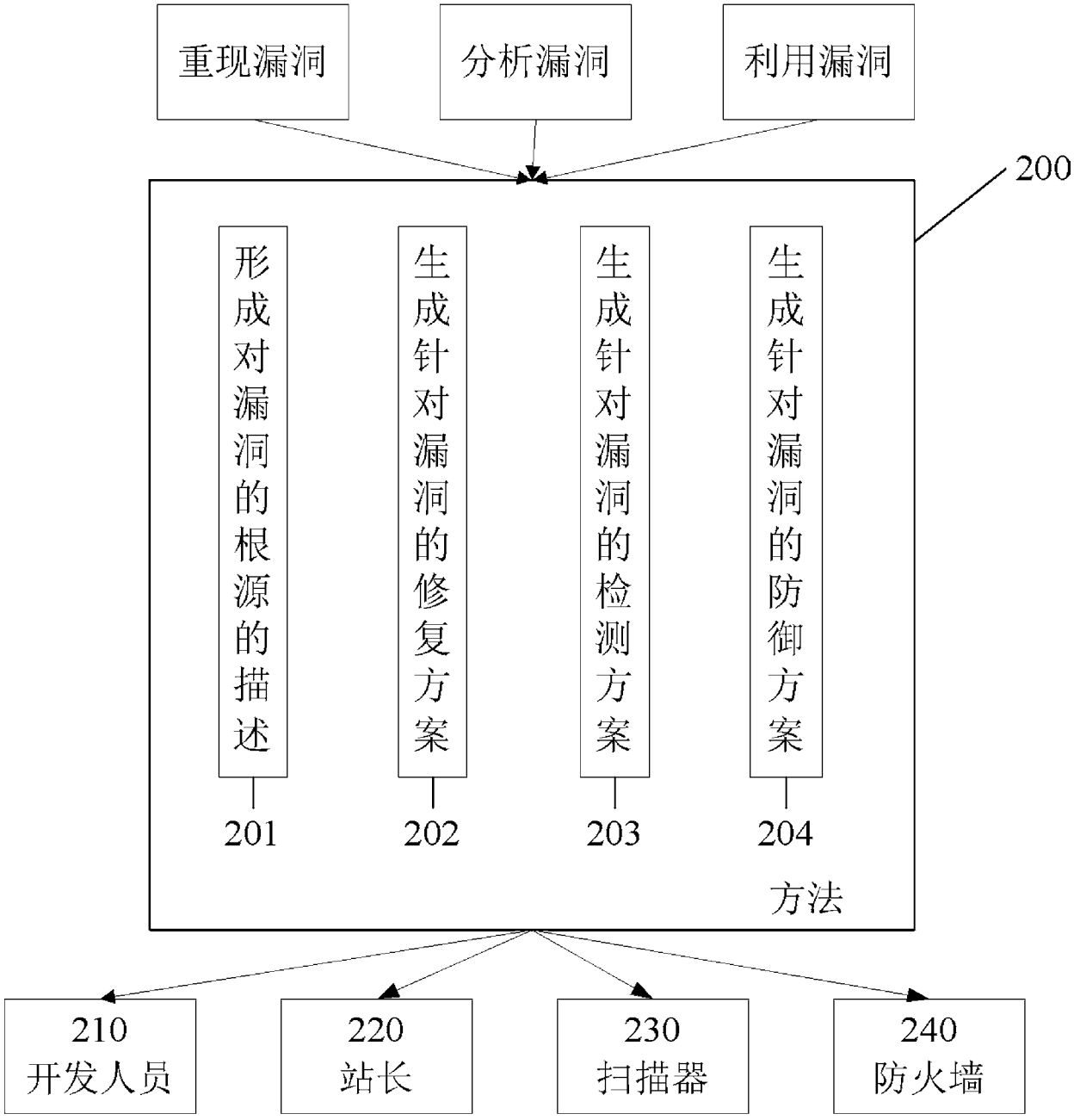

重现漏洞
分析漏洞
利用漏洞
200
形成对漏洞的根源的描述
生成针对漏洞的修复方案
生成针对漏洞的检测方案
生成针对漏洞的防御方案
201
202
203
204
方法
210
开发人员
220
站长
230
扫描器
240
防火墙

图 2

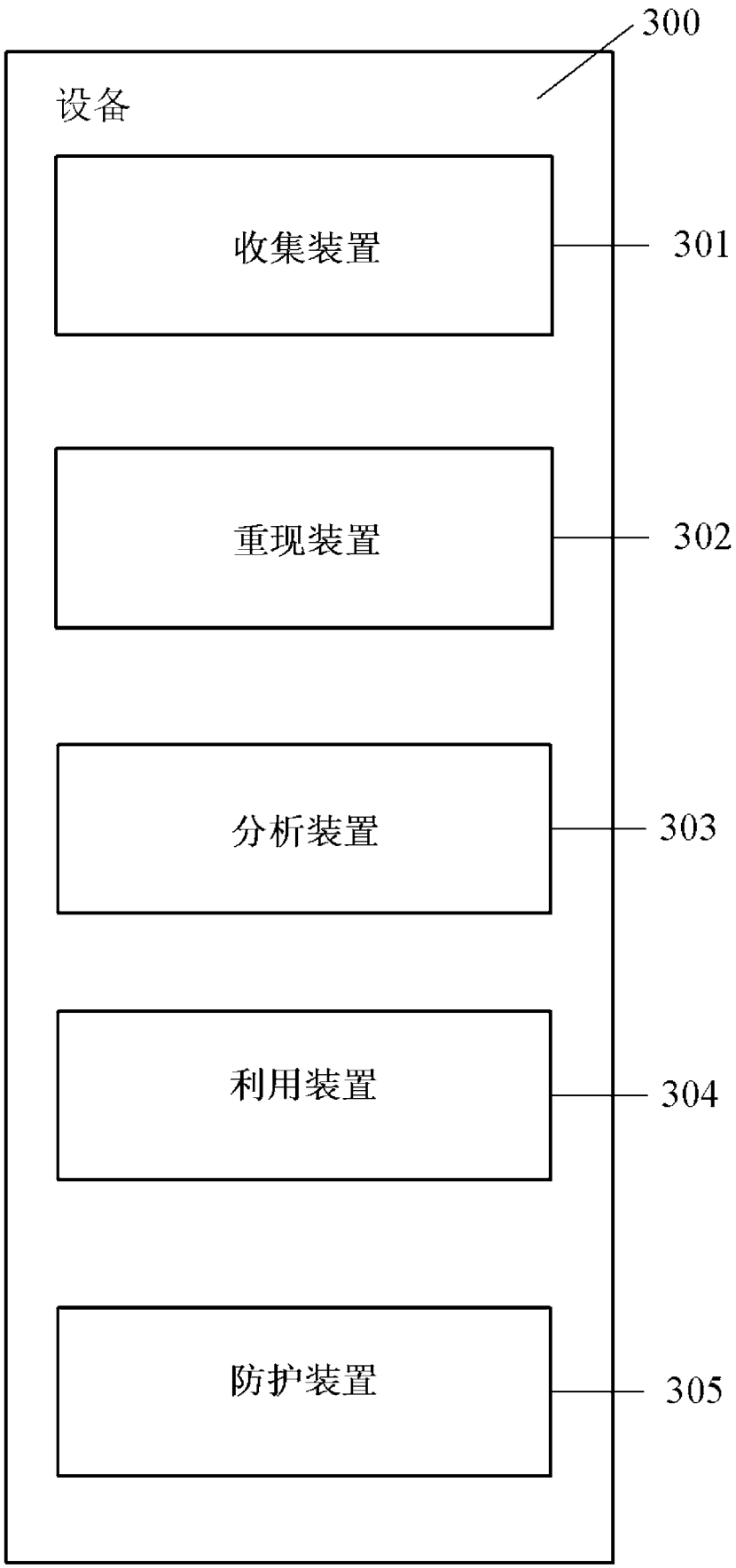



图 3