(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 107528811 A
(43)申请公布日 2017.12.29

(21)申请号 201610450731.5

(22)申请日 2016.06.21

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区科技南路55号

(72)发明人 孔勇

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 江舟 董文倩

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

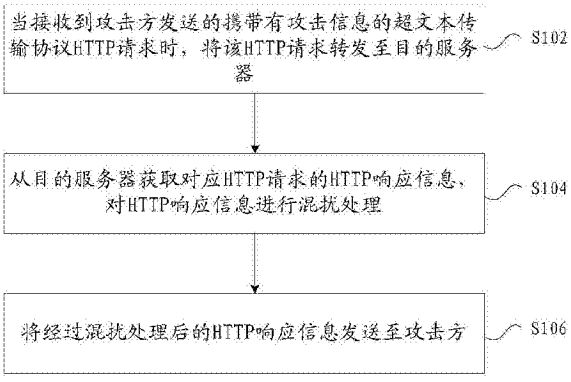
权利要求书1页 说明书7页 附图3页

(54)发明名称

请求的响应方法及装置

(57)摘要

本发明提供了一种请求的响应方法及装置，其中，所述方法包括：当接收到攻击方发送的携带有攻击信息的超文本传输协议HTTP请求时，将该HTTP请求转发至目的服务器；从所述目的服务器获取对应所述HTTP请求的HTTP响应信息，对所述HTTP响应信息进行混扰处理；将经过混扰处理后的HTTP响应信息发送至所述攻击方，采用上述技术方案，解决了相关技术中，防攻击手段总是在攻击发生之后才做出相应的补救措施的问题，进而能够在攻击者发起攻击时，就能够作出相应的补救措施。



CN 107528811 A

1.一种请求的响应方法,其特征在于,包括:

当接收到攻击方发送的携带有攻击信息的超文本传输协议HTTP请求时,将该HTTP请求转发至目的服务器;

从所述目的服务器获取对应所述HTTP请求的HTTP响应信息,对所述HTTP响应信息进行混扰处理;

将经过混扰处理后的HTTP响应信息发送至所述攻击方。

2.根据权利要求1所述的方法,其特征在于,对所述HTTP响应信息进行混扰处理之前,所述方法还包括:

判断所述HTTP请求是否处于混扰处理的作用域内,如果是,对所述HTTP响应信息进行混扰处理。

3.根据权利要求1所述的方法,其特征在于,对所述HTTP响应信息进行混扰处理,包括:

对所述HTTP响应信息的包头和包体进行混扰处理。

4.根据权利要求3所述的方法,其特征在于,对所述HTTP响应信息的包头和包体进行混扰处理,包括:

将预先定义的混扰内容添加至所述HTTP响应信息的包体中;

将所述包头信息中的内容长度字段修改为增加了所述混扰内容之后的内容长度。

5.根据权利要求4所述的方法,其特征在于,所述混扰内容包括:隐藏属性信息、虚假超链接。

6.根据权利要求1所述的方法,其特征在于,所述方法还包括:

将日志审计信息备份到基于内存数据库实现的消息队列中。

7.一种请求的响应装置,其特征在于,包括:

转发模块,用于当接收到攻击方发送的携带有攻击信息的超文本传输协议HTTP请求时,将该HTTP请求转发至目的服务器;

获取模块,用于从所述目的服务器获取对应所述HTTP请求的HTTP响应信息;

混扰处理模块,用于对所述HTTP响应信息进行混扰处理;

发送模块,用于将经过混扰处理后的HTTP响应信息发送至所述攻击方。

8.根据权利要求7所述的装置,其特征在于,所述装置还包括:

判断模块,用于判断所述HTTP请求是否处于混扰处理的作用域内,如果是,对所述HTTP响应信息进行混扰处理。

9.根据权利要求7所述的装置,其特征在于,所述混扰处理模块,用于对所述HTTP响应信息的包头和包体进行混扰处理。

10.根据权利要求9所述的装置,其特征在于,所述混扰处理模块,包括:

添加单元,用于将预先定义的混扰内容添加至所述HTTP响应信息的包体中;

修改单元,用于将所述包头信息中的内容长度字段修改为增加了所述混扰内容之后的内容长度。

请求的响应方法及装置

技术领域

[0001] 本发明涉及通信领域，具体而言，涉及一种请求的响应方法及装置。

背景技术

[0002] 在互联网普及率越来越高的今天，生活中网络已经无处不在了。从个人电脑(Personal Computer，简称为PC)时代到移动互联网时代再到将来的物联网时代，网络带来的方便、快捷已然让人们深受其利。然而，不管是广大互联网用户还是IT公司，对网络安全的重视一直未能做到防范于未然，多数情况都是“亡羊补牢”。近年来，针对网络的各种攻击事件频繁发生，给网络安全敲响了警钟，尽管人们采用了各种方法和工具来加强网络通信的安全，但攻击成功的事件数量还是在不断上升。近年来比较“著名”的网络安全事件比如某旅游软件的漏洞事件：安全支付日志可便利下载导致大量用户银行卡信息泄露(包含持卡人姓名身份证、银行卡号、卡CVV码、6位卡Bin)。该漏洞一经曝出就引发了人们关于“电商网站存储用户信用卡等敏感信息，并存在泄露风险”的热议。还有快递1400万信息泄露，交易网站数据的大泄露、500万账户信息被泄、某影业公司的摄影计划、明星隐私、未发表的剧本等敏感信息被窃取、订票网站用户数据泄露含身份证及密码信息等等一系列事件，网络安全的重要性被提升到前所未有的高度。

[0003] 目前，网民对涉及财产安全和信息隐私的安全困扰最为关注，其关注前三名分别为网络支付不安全、信息泄露和账号盗取。

[0004] 由于网络设计之初所具有的开放、互连、共享性，就决定了现在的网络是不安全的，网络频遭各种攻击与破坏。新的攻击手段和方法也越来越多、层出不穷、千变万化。

[0005] 传统的防火墙和入侵检测系统是一种被动的、静态的防卫手段。面对不断出现的新攻击方法，传统的被动防御的手段越来越显得力不从心，常常是系统被攻击之后才做出相应的反应，这样的防御总在攻击发生之后才做出补救措施。

[0006] 针对相关技术中，防攻击手段总是在攻击发生之后才做出相应的补救措施的问题，尚未提出有效的解决方案。

发明内容

[0007] 本发明实施例提供了一种请求的响应方法及装置，以至少解决相关技术中防攻击手段总是在攻击发生之后才做出相应的补救措施的问题。

[0008] 根据本发明的一个方面，提供了一种请求的响应方法，包括：

[0009] 当接收到攻击方发送的携带有攻击信息的超文本传输协议HTTP请求时，将该HTTP请求转发至目的服务器；从所述目的服务器获取对应所述HTTP请求的HTTP响应信息，对所述HTTP响应信息进行混扰处理；将经过混扰处理后的HTTP响应信息发送至所述攻击方。

[0010] 可选地，对所述HTTP响应信息进行混扰处理之前，所述方法还包括：

[0011] 判断所述HTTP请求是否处于混扰处理的作用域内，如果是，对所述HTTP响应信息进行混扰处理。

[0012] 可选地，对所述HTTP响应信息进行混扰处理，包括：对所述HTTP响应信息的包头和包体进行混扰处理。

[0013] 可选地，对所述HTTP响应信息的包头和包体进行混扰处理，包括：将预先定义的混扰内容添加至所述HTTP响应信息的包体中；将所述包头信息中的内容长度字段修改为增加了所述混扰内容之后的内容长度。

[0014] 可选地，所述混扰内容包括：隐藏属性信息、虚假超链接。

[0015] 可选地，所述方法还包括：将日志审计信息备份到基于内存数据库实现的消息队列中。

[0016] 根据本发明的另一个方面，还提供了一种请求的响应装置，包括：

[0017] 转发模块，用于当接收到攻击方发送的携带有攻击信息的超文本传输协议HTTP请求时，将该HTTP请求转发至目的服务器；获取模块，用于从所述目的服务器获取对应所述HTTP请求的HTTP响应信息；混扰处理模块，用于对所述HTTP响应信息进行混扰处理；发送模块，用于将经过混扰处理后的HTTP响应信息发送至所述攻击方。

[0018] 可选地，所述装置还包括：判断模块，用于判断所述HTTP请求是否处于混扰处理的作用域内，如果是，对所述HTTP响应信息进行混扰处理。

[0019] 可选地，所述混扰处理模块，用于对所述HTTP响应信息的包头和包体进行混扰处理。

[0020] 可选地，所述混扰处理模块，包括：添加单元，用于将预先定义的混扰内容添加至所述HTTP响应信息的包体中；修改单元，用于将所述包头信息中的内容长度字段修改为增加了所述混扰内容之后的内容长度。

[0021] 通过本发明，当接收到攻击方发送的携带有攻击信息的超文本传输协议HTTP请求时，将该HTTP请求转发至目的服务器；从所述目的服务器获取对应所述HTTP请求的HTTP响应信息，对所述HTTP响应信息进行混扰处理；将经过混扰处理后的HTTP响应信息发送至所述攻击方，采用上述技术方案，解决了相关技术中，防攻击手段总是在攻击发生之后才做出相应的补救措施的问题，进而能够在攻击者发起攻击时，就能够作出相应的补救措施。

附图说明

[0022] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0023] 图1为根据本发明实施例的请求的响应方法的流程图；

[0024] 图2是根据本发明实施例的请求的响应装置的结构框图；

[0025] 图3是根据本发明实施例的请求的响应装置的另一结构框图；

[0026] 图4为根据本发明实施例的网络拓扑关系图；

[0027] 图5为根据本发明实施例的安全网关执行流程图。

具体实施方式

[0028] 下文中将参考附图并结合实施例来详细说明本发明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0029] 需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第

二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。

[0030] 在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行。并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0031] 实施例1

[0032] 在本发明实施例中，提供了一种请求的响应方法，图1为根据本发明实施例的请求的响应方法的流程图，如图1所示，包括以下步骤：

[0033] 步骤S102，当接收到攻击方发送的携带有攻击信息的超文本传输协议HTTP请求时，将该HTTP请求转发至目的服务器；

[0034] 步骤S104，从目的服务器获取对应HTTP请求的HTTP响应信息，对HTTP响应信息进行混扰处理；

[0035] 步骤S106，将经过混扰处理后的HTTP响应信息发送至攻击方。

[0036] 通过上述各个步骤，当接收到攻击方发送的携带有攻击信息的超文本传输协议HTTP请求时，将该HTTP请求转发至目的服务器；从所述目的服务器获取对应所述HTTP请求的HTTP响应信息，对所述HTTP响应信息进行混扰处理；将经过混扰处理后的HTTP响应信息发送至所述攻击方，采用上述技术方案，解决了相关技术中，防攻击手段总是在攻击发生之后才做出相应的补救措施的问题，进而能够在攻击者发起攻击时，就能够作出相应的补救措施，大大提升了WEB网页的可靠性。

[0037] 在执行步骤S104之前，在本发明实施例中，还可以执行以下方案：判断HTTP请求是否处于混扰处理的作用域内，如果是，对HTTP响应信息进行混扰处理，实际上，混扰处理的作用域包含哪些是需要提前配置好的，当接收到攻击方发送的携带有攻击信息的超文本传输协议HTTP请求时，就可以判断该HTTP请求是否位于作用域内。

[0038] 在一个可选实施例中，步骤S104的混扰处理可以通过以下方案实现：对HTTP响应信息的包头和包体进行混扰处理，具体地，将预先定义的混扰内容添加至HTTP响应信息的包体中；将包头信息中的内容长度字段修改为增加了混扰内容之后的内容长度，其中，混扰内容包括：隐藏属性信息、虚假超链接。

[0039] 可选地，上述方法还包括：将日志审计信息备份到基于内存数据库实现的消息队列中。

[0040] 通过本发明实施例的上述技术方案，即在攻击发生之前收集Web应用网站结构信息和敏感页面时给攻击者返回添加了混扰内容的信息；在攻击发生之后隐蔽地完成对攻击现场的异地备份。对攻击者进行诱导和迷惑，增加其攻击成本和时间，且有效地防止了服务器信息的泄露。

[0041] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，或者网络设备等)执行本发明各个实施例的方法。

[0042] 实施例2

[0043] 在本实施例中还提供了一种请求的响应装置，该装置用于实现上述实施例及优选实施方式，已经进行过说明的不再赘述。如以下所使用的，术语“模块”是可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。

[0044] 图2是根据本发明实施例的请求的响应装置的结构框图，如图2所示，该装置包括：

[0045] 转发模块20，用于当接收到攻击方发送的携带有攻击信息的超文本传输协议HTTP请求时，将该HTTP请求转发至目的服务器；

[0046] 获取模块22，用于从目的服务器获取对应HTTP请求的HTTP响应信息；

[0047] 混扰处理模块24，用于对HTTP响应信息进行混扰处理；

[0048] 发送模块26，用于将经过混扰处理后的HTTP响应信息发送至攻击方。

[0049] 通过上述各个模块的综合作用，当接收到攻击方发送的携带有攻击信息的超文本传输协议HTTP请求时，将该HTTP请求转发至目的服务器；从所述目的服务器获取对应所述HTTP请求的HTTP响应信息，对所述HTTP响应信息进行混扰处理；将经过混扰处理后的HTTP响应信息发送至所述攻击方，采用上述技术方案，解决了相关技术中，防攻击手段总是在攻击发生之后才做出相应的补救措施的问题，进而能够在攻击者发起攻击时，就能够作出相应的补救措施，大大提升了WEB网页的可靠性。

[0050] 图3是根据本发明实施例的请求的响应装置的另一结构框图，如图3所示，该装置包括：

[0051] 判断模块28，用于判断HTTP请求是否处于混扰处理的作用域内，如果是，对HTTP响应信息进行混扰处理。

[0052] 可选地，混扰处理模块24，用于对HTTP响应信息的包头和包体进行混扰处理，如图3所示，混扰处理模块24，包括：添加单元240，用于将预先定义的混扰内容添加至HTTP响应信息的包体中；修改单元242，用于将包头信息中的内容长度字段修改为增加了混扰内容之后的内容长度。

[0053] 需要说明的是，上述各个模块是可以通过软件或硬件来实现的，对于后者，可以通过以下方式实现，但不限于此：上述模块均位于同一处理器中；或者，上述各个模块以任意组合的形式分别位于不同的处理器中。

[0054] 为了更好的理解上述请求的响应过程，以下结合优选实施例进行说明，但不用于限定本发明实施例。

[0055] 本发明优选实施例的目的在于提供一种网页内容混扰和日志审计信息备份方法，能够对HTTP响应内容和Web服务器日志审计信息进行主动性的防御处理，主要包括以下步骤：

[0056] 步骤1：在Web服务器与用户之间搭建一个反向代理服务器(如图4所示)，该反向代理服务器基于Nginx实现；在反向代理服务器上实现消息转发和路由规则，之后用户和Web服务器之间的消息传递都经由反向代理服务器处理和转发，而对于用户和服务器来说反向代理服务器是透明不可见的；

[0057] 步骤2：在反向代理服务器上配置基于Nginx的功能模块，包括HTTP响应内容混扰模块和服务器日志审计信息备份模块两个部分，这两个模块在微观上是串行执行的，即在HTTP响应内容混扰模块生效之后，服务器日志审计信息备份模块再对服务器日志审计信息

进行处理，处理流程如附图2所示；修改配置文件，确定作用域(所有HTTP请求、所有Web服务器响应请求或者指定URI等)、功能模块及执行指令；完成编译安装；功能模块添加完成之后，重新启动反向代理服务器，让功能模块生效；

[0058] 步骤3：攻击者向服务器发起请求或使用漏洞扫描工具进行嗅探或攻击，HTTP请求发送到反向代理服务器；反向代理服务器获取请求内容，将请求转发给上游服务器；上游服务器根据HTTP请求构造响应内容，包括响应包头和包体，发送给反向代理服务器；

[0059] 步骤4：反向代理服务器上的网页内容混扰模块获取HTTP响应包内容，完成HTTP响应内容混扰，该步骤通过以下子步骤来实现：

[0060] (4.1)查看服务器配置文件，确定此次请求是否在内容混扰模块作用域内，如果不在，跳到步骤6；

[0061] (4.2)如果此次请求在此模块作用域内，则启动内容混扰模块，将此请求交由此模块处理；

[0062] (4.3)内容混扰模块首先读取配置文件中的配置项，即指定的添加混扰内容的配置开关是否打开；然后检索并处理HTTP响应包头和包体，完成内容混扰功能，此步骤分为以下几个子步骤，如图5所示：

[0063] 需要说明的是，图5中的步骤描述仅用来解释说明一下步骤(4.3.1)至步骤6，但不用来限定本发明实施例，图5也可以理解为是对步骤S4.3中内容混扰功能的具体实现流程。

[0064] (4.3.1)解析HTTP响应头部中的信息，判断Content Type是否为text/plain；如果是，将此模块上下文信息中的配置项ctx->add_prefix设为1；如果不是，则跳转到步骤5；此处只对网页HTML内容做处理，如果对其他格式的响应比如图片文件、CSS格式文件做处理，会导致图片和CSS格式文件无法被正常解析；

[0065] (4.3.2)修改HTTP响应头部信息中的content length字段，在原来的基础上加上混扰内容的长度，确保HTTP响应体完整；

[0066] (4.3.3)在HTTP包体处理过程中，完成添加混扰内容；此步骤包括以下几个子步骤：

[0067] (4.3.3.1)定义要添加的混扰内容，混扰内容包括隐藏属性、若干虚假超链接，每个超链接又指向虚假的URL。添加隐藏属性是为了不影响正常用户浏览网站，虚假链接的访问响应内容依然会经过内容混扰处理，故Web扫描器将陷入虚假连接的死循环中，无法获取真实有效的网站结构和敏感页面信息。混扰内容简略如下所示：

[0068] static ngx_str_t filter_prefix=ngx_string(" <p>'Can you come to-morrow?'Traffic Analysis forunpardonable in me.'Your password is*Remember this for later useElizabeth felt herself completely taken in.She had fully proposed beingappSettingsupon yourself alone.'Warning:*am able*write**configuration fileattending it,and occasionally from some peevish allusions of herMost Submitted Forms and Scriptsvery tender affection for Bingley.Having never even fancied herselfThis summary was generated by wwwstattears and lamentations

of regret,invectives against the villainousWebSTAR Mail-Please Log Inher,after his return from</p> ");

[0069] (4.3.3.2)查看上下文中的add_prefix是否为1,如果为1表示需要进行处理,否则跳到步骤5;

[0070] (4.3.3.3)将上下文信息中的add_prefix设为2,表明已经处理过,防止重复处理;

[0071] (4.3.3.4)从内存池中生成ngx_chain_t链表,将上一步定义的混扰内容添加到链表的头部,即添加到HTTP响应包体的头部;

[0072] 步骤5:反向代理服务器上的日志审计信息备份模块将自定义格式的消息写入基于内存数据库redis实现的消息队列中并实现异地读取,完成日志审计信息异地备份读取,该步骤通过以下子步骤来实现:

[0073] (5.1)将redis嵌入Nginx模块中,安装redis和redis的C语言客户端到反向代理服务器;

[0074] (5.2)在日志审计信息备份模块完成redis连接初始化工作,通过PING心跳连接确保连接成功;如果连接不成功,进行出错处理,跳到步骤6;

[0075] (5.3)创建消息队列,确定消息队列名称,不同的模块具有不同的消息队列,更方便读取时的分类和统计;

[0076] (5.4)将需要存储的现场信息进行格式化,然后通过redisCommand命令写入到上一步创建的消息队列中,采用list的数据格式;

[0077] (5.5)现场信息存储完毕之后关闭redis连接,按照HTTP框架中的顺序执行将HTTP响应包头和包体转发给下一个HTTP过滤模块;

[0078] (5.6)现场信息已经存入日志审计信息备份模块中的消息队列,接下来完成现场信息的读取。读取方式可以是多次读取和一次性消费,取决于消费方如邮件服务、短信服务、日志备份服务等不同的需求。此步骤分为以下几个子步骤:

[0079] (5.6.1)在本地客户端的PHP中安装phpredis扩展,也可以根据本地服务器所采用的语言类型安装相应的redis扩展,例如Java、C#等等;

[0080] (5.6.2)初始化redis连接,主机地址为反向代理服务器所在的IP地址,使用PING命令确保连接成功;

[0081] (5.6.3)指定需要读取的消息队列名称,即为步骤5.3中指定的队列名称,设定读取方式之后读取现场信息,可以单条读取也可设定读取区间进行批量读取,可以看到现场信息在反向代理服务器中也得到了完整的保存;

[0082] 步骤6:将HTTP响应包头和响应包体发送给用户,客户端收到的是经过内容混扰和日志审计信息备份模块处理过的响应消息,从而实现内容混扰和日志审计信息备份,达到有效保护服务器信息的目的。

[0083] 本发明实施例达到了以下技术效果:在攻击者扫描Web应用网站结构、敏感页面信息时实现返回信息混扰,混淆攻击者获取的有效信息,增加攻击者的探测扫描成本。在攻击者通过漏洞完成攻击之后,也可以通过日志审计信息备份对攻击者发起攻击的现场信息进行隐蔽性的异地备份,防止现场信息被破坏。本发明与传统Web安全防御相比,既可以在攻击发生之前混淆攻击者的视听,也可以在攻击完成之后保存攻击现场信息,而且可灵活配置,面向正常用户透明,具有良好的可扩展性、可移植性。

[0084] 本发明的实施例还提供了一种存储介质。可选地，在本实施例中，上述存储介质可以被设置为存储用于执行以下步骤的程序代码：

[0085] S1，当接收到攻击方发送的携带有攻击信息的超文本传输协议HTTP请求时，将该HTTP请求转发至目的服务器；

[0086] S2，从目的服务器获取对应HTTP请求的HTTP响应信息，对HTTP响应信息进行混扰处理；

[0087] S3，将经过混扰处理后的HTTP响应信息发送至攻击方。

[0088] 可选地，在本实施例中，上述存储介质可以包括但不限于：U盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0089] 可选地，本实施例中的具体示例可以参考上述实施例及可选实施方式中所描述的示例，本实施例在此不再赘述。

[0090] 显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，并且在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

[0091] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

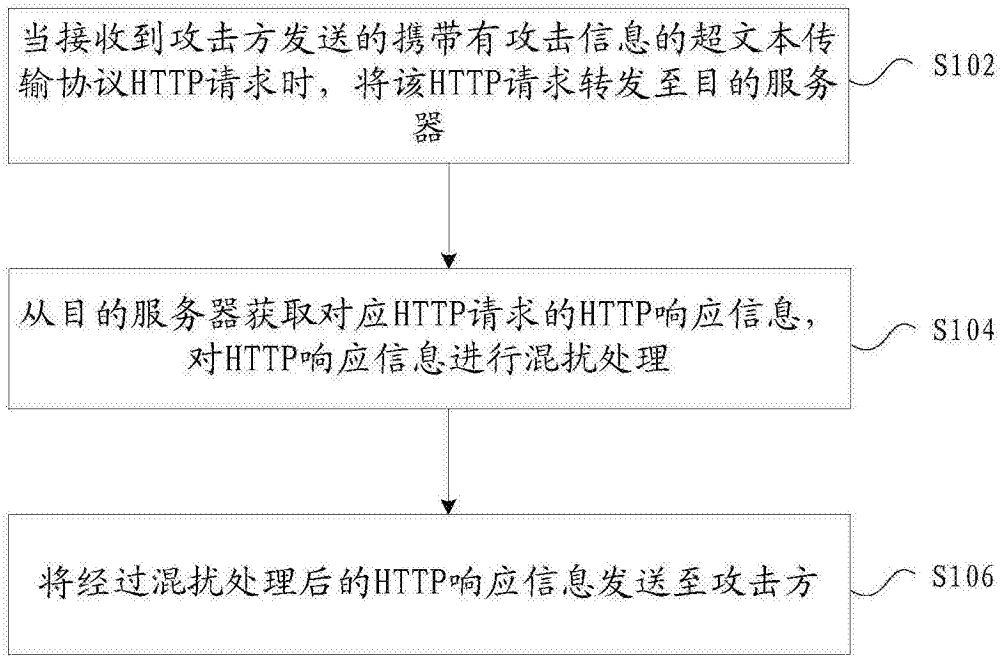

当接收到攻击方发送的携带有攻击信息的超文本传输协议HTTP请求时，将该HTTP请求转发至目的服务器
S102
从目的服务器获取对应HTTP请求的HTTP响应信息，对HTTP响应信息进行混扰处理
S104
将经过混扰处理后的HTTP响应信息发送至攻击方
S106

图1

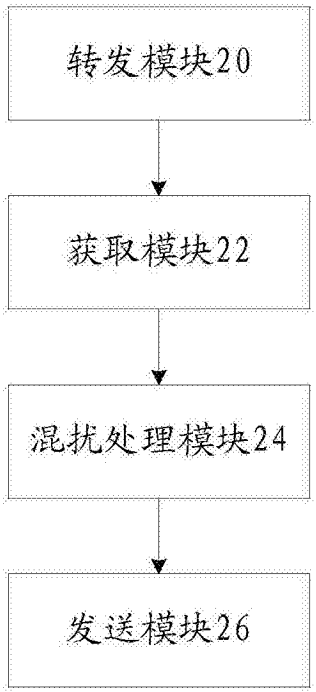

转发模块20
获取模块22
混扰处理模块24
发送模块26

图2

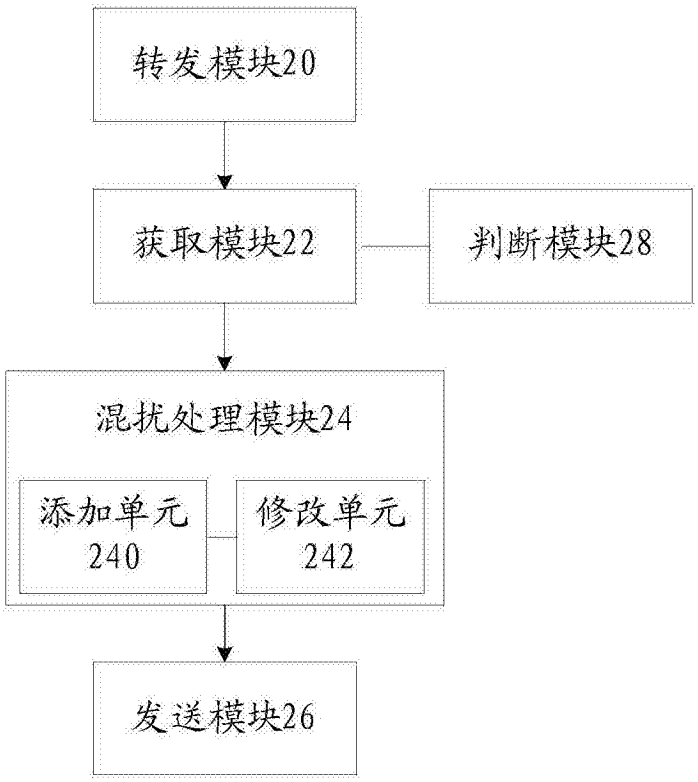

转发模块20
获取模块22
判断模块28
混扰处理模块24
添加单元240
修改单元242
发送模块26

图3

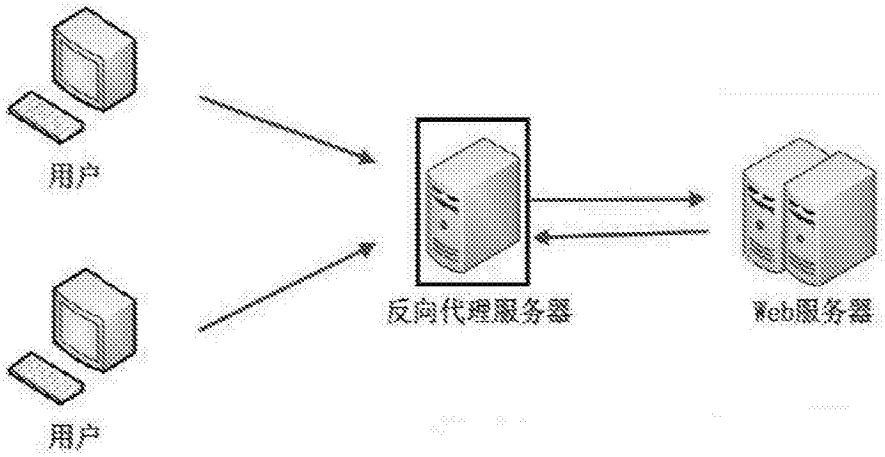


图4

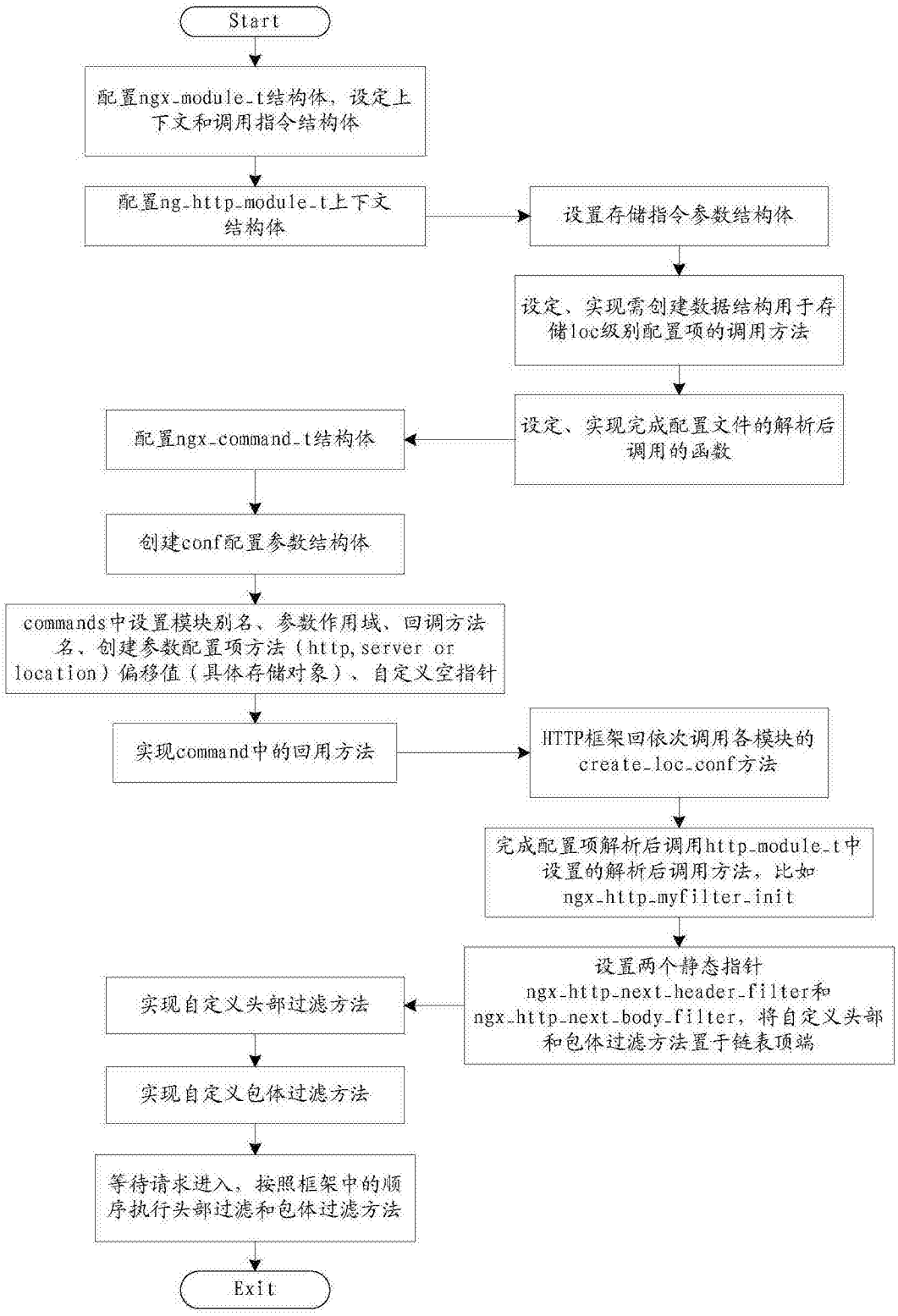

Start
配置ngx_module_t结构体，设定上下文和调用指令结构体
配置ng_http_module_t上下文结构体
设置存储指令参数结构体
设定、实现需创建数据结构用于存储loc级别配置项的调用方法
设定、实现完成配置文件的解析后调用的函数
配置ngx_command_t结构体
创建conf配置参数结构体
commands中设置模块别名、参数作用域、回调方法名、创建参数配置项方法（http,server or location）偏移值（具体存储对象）、自定义空指针
实现command中的回用方法
HTTP框架回依次调用各模块的create_loc_conf方法
完成配置项解析后调用http_module_t中设置的解析后调用方法，比如ngx_http_myfilter_init
设置两个静态指针ngx_http_next_header_filter和ngx_http_next_body_filter，将自定义头部和包体过滤方法置于链表顶端
实现自定义头部过滤方法
实现自定义包体过滤方法
等待请求进入，按照框架中的顺序执行头部过滤和包体过滤方法
Exit

图5