

(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
2018 年 4 月 19 日 (19.04.2018)



(10) 国际公布号
WO 2018/068366 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2016/107349

(22) 国际申请日: 2016 年 11 月 25 日 (25.11.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610897875.5 2016 年 10 月 14 日 (14.10.2016) CN

(71) 申请人: 福建亿榕信息技术有限公司
(FUJIAN YIRONG INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国福建省福州市软件大道 89 号 G 区 20 号楼, Fujian 350000 (CN)。国家电网公司 (STATE GRID CORPORATION OF CHINA) [CN/CN]; 中国北京市西城区西长安街 86 号, Beijing 100031 (CN)。国网信息通信产业集团有限公司 (STATE GRID INFORMATION A

TELECOMMUNICATION GROUP CO., LTD.) [CN/CN]; 中国北京市昌平区未来科技城北区国网智能电网研究院内 C 座 4 层, Beijing 100031 (CN)。国网信通亿力科技有限责任公司 (STATE GRID INFO-TELECOM GREAT POWER SCIENCE AND TECHNOLOGY CO., LTD) [CN/CN]; 中国福建省厦门市软件园二期观日路 36 号 420 室, Fujian 361008 (CN)。

(72) 发明人: 倪时龙 (NI, Shilong); 中国福建省福州市软件大道 89 号 G 区 20 号楼, Fujian 350003 (CN)。林振天 (LIN, Zhentian); 中国福建省福州市软件大道 89 号 G 区 20 号楼, Fujian 350003 (CN)。陈又咏 (CHEN, Youyong); 中国福建省福州市软件大道 89 号 G 区 20 号楼, Fujian 350003 (CN)。陈天宇 (CHEN, Tianyu); 中国福建省福州市软件大道 89 号 G 区 20 号楼, Fujian 350003 (CN)。黄敬林 (HUANG, Jinglin); 中国福建省福州市软件大道 89 号 G 区 20 号楼, Fujian 350003 (CN)。张望华

(54) Title: METHOD FOR PREVENTING XSS ATTACK

(54) 发明名称: 预防 XSS 攻击的方法

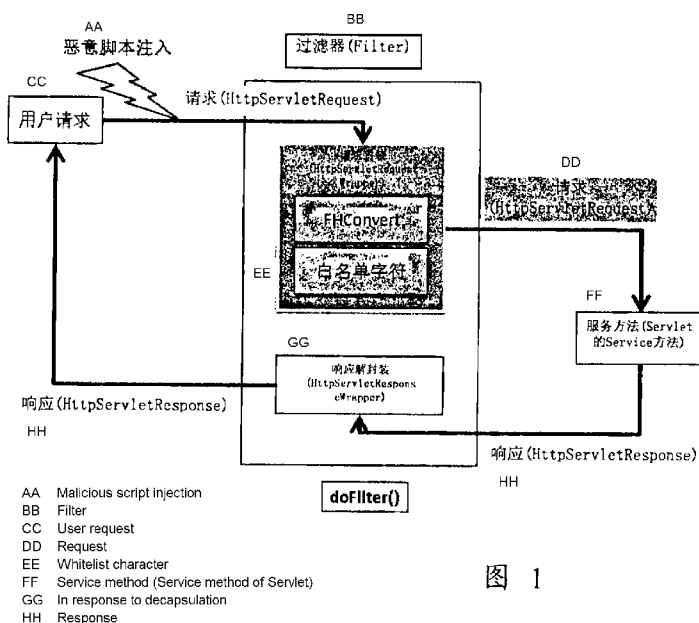


图 1

(57) Abstract: An embodiment of the invention relates to the field of web security, and more particularly, to the field of XSS attacks. Provided in the embodiment of the invention is a method for preventing an XSS attack capable of solving the problem of XSS attacks in certain situations. The method comprises the following steps: configuring an XSS filter for performing, in a filtering function, filtering on a requested parameter sent to a target server by a web page, performing filtering referring to determination of whether the requested parameter comprises a set keyword; if the keyword appears in the requested parameter, replacing the same with a corresponding set character.

(ZHANG, Wanghua); 中国福建省福州市软件大道89号G区20号楼, Fujian 350003 (CN)。

(74) 代理人: 北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY OFFICE); 中国北京市海淀区海淀南路21号中关村知识产权大厦B座2层, 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, JP, KE, KG, 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。

(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))。

(57) 摘要: 本发明实施例属于web安全领域, 特别涉及xss攻击领域。本发明实施例提供一种预防xss攻击的方法解决一些情况下xss攻击的问题。其包括步骤: 配置xssfilter, 使其在过滤函数中对网页向目标服务器发送的请求的参数进行过滤, 所述进行过滤指判断请求的参数中是否包含设定的关键字, 若请求的参数中出现设定的关键字, 则将其替换为对应的设定字符。

预防 xss 攻击的方法

相关申请的交叉引用

本申请基于申请号为 201610897875.5、申请日为 2016 年 10 月 14 日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的
5 全部内容在此引入本申请作为参考。

技术领域

本发明属于 web 安全领域，特别涉及 xss 攻击领域。

背景技术

跨站脚本攻击，又称 xss 攻击，通常指黑客通过 html 注入了篡改网页，
10 插入恶意的脚本，从而在用户浏览网页时，控制用户浏览器的一种攻击，
是 web 安全中的头号大敌，OWASP TOP 10 威胁多次把 xss 列在榜首，xss
破坏力强大，且产生的场景复杂，难以一次性解决。

对于 web 应用，用户通过浏览器访问应用的时候，用户的输入通过 html
表单(form)来实现，最终用户所有的输入以表单（form）的形式发送到 web
15 服务端，xss 攻击就是发生在这个时候，黑客利用技术手段，将恶意脚本，
混淆在用户输入的表单中，导致 xss 攻击。防御 xss 攻击，最主要就是对用
户的输入要进行安全过滤，比如对用户的输入过滤掉<script>、alert、iframe
等关键字，但黑客通过在上述关键字中间加入空格，即可轻松的避开对 script
alert iframe 的过滤，例如将 javascript 写为 java script。

20 在过滤的实现策略上，又有白名单策略和黑名单策略，白名单策略是
通过设置允许用户输入的字符或关键字来控制用户输入，黑名单策略是通
过设置不允许用户输入的字符或关键字来控制用户输入。

这些策略在具体实施的时候，存在这样的缺点：白名单策略，则需要穷举出所有允许用户输入的字符或关键字，只要稍有遗漏，就有可能导致因合法的输入不在白名单中，而影响系统功能；黑名单策略，则需要穷举出所有不允许用户输入的字符或关键字，只要稍有遗漏，就有可能导致非法输入不在黑名单中，引起系统 xss 攻击。

综上所述，不管是采用白名单策略还是黑名单策略，前提都是构造一份完整的没有遗漏的白名单或黑名单，而这在现实中基本上是不太可行的，因为随着系统的不断升级，新的功能不断开发，这个白名单，永远都在不断增加，同样黑客技术也在不断发展，今天认为安全的字符或关键字，在明天有可能就是不安全的了。

发明内容

以下给出对一个或更多个方面的简化概述以力图提供对此类方面的基本理解。此概述不是所有构想到的方面的详尽综览，并且既非旨在指出所有方面的关键性或决定性要素亦非试图界定任何或所有方面的范围。其唯一的目的是，要以简化形式给出一个或更多个方面的一些概念，以作为稍后给出的更加具体的说明之序。

本发明实施例提供一种预防 xss 攻击的方法解决一些情况下 xss 攻击的问题。

为实现上述目的，发明人提供了一种预防 xss 攻击的方法，包括步骤：

配置 xssfilter，使其在过滤函数中对网页向目标服务器发送的请求的参数进行过滤，所述进行过滤指判断请求的参数中是否包含设定的关键字，若请求的参数中出现设定的关键字，则将其替换为对应的设定字符。

进一步，所述设定的关键字指 ASCII 编码中的指除数字、大写字母、小写字母、美元符号外的所有字符，设定的关键字所对应的字符为其对应的全角字符。

进一步，所述的配置 xssfilter 包括步骤：

在 web 应用的配置文件 web.xml 中进行配置使 xssfilter 生效；

通过 xssHttpRequestWrapper 获取请求的参数；

并对请求的参数进行过滤。

- 5 进一步，所述方法还包含设置关键字白名单，在对请求的参数进行过滤时，对关键字白名单中的字符不进行替换处理。

进一步，所述设定的关键字至少包括以下一个或多个字符：半角左尖括号、半角右尖括号；半角左尖括号、半角右尖括号分别对应的设定字符为全角左尖括号、全角右尖括号。

- 10 进一步，所述设定的关键字至少包括以下一个或多个字符：半角双竖线和半角等号，半角左尖括号、半角右尖括号分别对应的设定字符为全角双竖线和全角等号

进一步，所述设定的关键字至少包括以下一个或多个字符：半角字符'\"/>

- 15 上述方法设置简单，相比分别在不同的 jsp 函数中对用于请求的每个参数都进行不同的验证（例如现有技术中常用的在 jsp 函数中对用户登入的用户名和密码的参数进行是否是全数值的校验、或全字母的校验），本发明实施例提供的方法不需要逐一设置验证规则，而可以对网页发送的请求的参数进行过滤，其有效的防御 xss 攻击的同时，也降低了工程师的代码量，有
20 效的缩短了开发时间和缩短了开发成本。

相比于通过过滤 script 等关键字字符串，本发明实施例通过过滤字符，黑客无法在过滤字符中注入空格等方式规避，从而有效的避免现有技术中黑客通过在字符串中加入空格等方式规避对 xss 攻击的过滤的问题。

- 25 为能达成前述及相关目的，这一个或更多个方面包括在下文中充分描述并在所附权利要求中特别指出的特征。以下描述和附图详细阐述了这一

个或更多个方面的某些说明性特征。但是，这些特征仅仅是指示了可采用各种方面的原理的各种方式中的若干种，并且本描述旨在涵盖所有此类方面及其等效方面。

附图说明

5 以下将结合附图来描述所公开的方面，提供附图是为了说明而非限定所公开的方面，附图中相似的标号标示相似要素，并且在其中：

图 1 为本发明实施例的一种实施方式的示意图。

具体实施方式

10 为详细说明技术方案的技术内容、构造特征、所实现目的及效果，以下结合具体实施例并配合附图 1 详予说明。在以下描述中，出于解释目的阐述了众多的具体细节以提供对一个或更多个方面的透彻理解。但是显而易见的是，没有这些具体细节也可实践此类方面。

可以理解的是 xss 攻击产生的场景复杂，且黑客的 xss 攻击代码在不断进步，本发明实施例力求提供在一些场景中的 xss 攻击的解决方案，而并非
15 解决所有可能的 xss 攻击。

参照图 1，本发明实施例提供一种预防 xss 攻击的方法，包括步骤：

配置 xssfilter，使其在过滤函数中对网页向目标服务器发送的请求的参数进行过滤，所述进行过滤指判断请求的参数中是否包含设定的关键字，若请求的参数中出现设定的关键字，则将其替换为对应的设定字符。

20 如果 Web 应用程序接受用户通过 HTTP 请求（如 GET 或 POST）提交的输入信息，然后使用输出 HTML 代码在某些地方显示这些信息，便可能存在 xss 漏洞，通过下述实施例说明本发明解决上述 xss 攻击的方法：

1、Web 请求如下所示：

GET http://www.example.com/page.asp?pageid=10&title=Section%20Title

2、在发出请求后，服务器返回的 HTML 内容包括：

```
<h1>Section Title</h1>
```

3、现在，如果遇到 xss 攻击，例如攻击者通过摆脱<h1>标记来注入代码：

```
5 http://www.example.com/page.asp?pageid=1&title=Section%20Title</h1>  
<script>alert('xss%20attack')</script>
```

这个请求的 HTML 输出将为：

```
<h1>Section Title</h1>< script >alert('xss attack')< /script ></h1>
```

参照图 1，例如对于 ie 浏览器，可以通过下述方法实现本发明实施例的方法：在 web.xml 中配置打开 xssfilter，通过实现一个自定义的
10 HttpServletRequestWrapper，然后在 Filter 里面调用它，替换掉 getParameter 函数即可将网页向目标服务器发送的请求的参数进行过滤。本领域技术人员在了解了针对一个浏览器的上述 xssfilter 设置方法，其也可以根据其已掌握的其他浏览器的知识，为其他浏览器设置实现上述方法的代码。

15 本发明实施例中进行过滤指判断请求的参数中是否包含设定的关键字，若请求的参数中出现设定的关键字，则其替换为对应的设定字符，即请求中的参数中

即上述例子中在 getParameter 函数中将 title 对应的参数值
Section%20Title</h1><script>alert('xss%20attack')</script>的所有的半角尖
20 括号字符转成全角的尖括号字符，则这个请求的 HTML 输出将为：

```
<h1>Section Title</h1>< script >alert('xss attack')< /script ></h1>
```

，其中下划线内的至少尖括号为全角字符，在另一些替换方式中也可以是将、反斜杠、单引号替换为全角字符。

因此破坏了 html 标签原有的语义，浏览器不会执行
25 <script>alert('xss%20attack')</script>，而是显示一段普通的文本：Section Title</h1>< script >alert('xss attack')< /script >，即经过半角转全角后，脚本

已被破坏，不能在浏览器中执行，所以 xss 攻击失效。

上述方法设置简单，相比分别在不同的 jsp 函数中对用于请求的每个参数都进行不同的验证（例如现有技术中常用的在 jsp 函数中对用户登入的用户名和密码的参数进行是否是全数值的校验、或全字母的校验），本发明实
5 施例提供的方法不需要逐一设置验证规则，而可以对网页发送的请求的参数进行过滤，其有效的防御 xss 攻击的同时，也降低了工程师的代码量，有效的缩短了开发时间和缩短了开发成本。

相比于通过过滤 script 等关键字字符串，本发明实施例通过过滤字符，黑客无法在过滤字符中注入空格等方式规避，从而有效的避免现有技术中黑
10 客通过在字符串中加入空格等方式规避对 xss 攻击的过滤的问题。

优选的所述“设定的关键字”是指 ASCII 编码中的指除数字、大写字母、小写字母、美元符号外的所有字符所对应的全角字符。

还包含设置关键字白名单，在对请求的参数进行过滤时，对关键字白名单中的字符不进行替换处理。即设定的关键字指 ASCII 编码中的指除数字、大写字母、小写字母、美元符号，以及关键字白名单所包含的字符的
15 之外的所有字符。从而便于在系统开发和维护过程中，根据具体的 xss 攻击的情景或检测项目的需求，快速的改进过滤效果。

在另一些实施例中所述设定的关键字至少包括以下一个或多个字符：
半角左尖括号、半角右尖括号；半角左尖括号、半角右尖括号分别对应的
20 设定字符为全角左尖括号、全角右尖括号。可以理解的是若在 Section
Title</h1>< script >alert('xss attack')</script>中，将半角<替换为全角<，也足以影响其在浏览器中的解析，从而使其在浏览器中不能执行。在另一些实施例中，所述设定的关键字包括以下一个或多个字符：半角双竖线和半角等号，半角双竖线和半角等号分别对应的设定字符为全脚双竖线和全角
25 等号。

以下实施例用于说明本方法:

用户发起一个请求如下:

`http://127.0.0.1:7001/ams-web/UserServlet?deleteUser&userid=1001`

这个请求本意是实现删除 `userid` 为 1001 的这个用户。

- 5 假设服务端实现业务逻辑的 sql 语句是这样的: `sql="delete t_user where id=" +userid`, `userid` 为用户提交的请求参数。

黑客只要在请求中针对 `userid` 这个请求参数, 进行修改如下

`http://127.0.0.1:7001/ams-web/UserServlet?deleteUser&userid=1001|||1=1`

则服务端执行的 sql 语句变成

- 10 “`delete t_user where id=1001|||1=1`”

该语句会删除所有用户表中信息。

引入上述安全过滤机制后, 上面请求参数中的 `userid=1001|||1=1`, 过滤器中会将 `1001|||1=1` 中的特殊字符, 这样在服务端拼接的 sql 语句变成:

“`delete t_usre where id=1001 | | 1 = 1`”

- 15 这条语句包含了全脚字符, 不是一个合法的 sql 语句, 是不能被执行的。
从而避免了 xss 攻击对服务器数据库的非法修改。

在另一些实施例中, 所述设定的关键字包括以下一个或多个字符: 半角 `'"\/#&`; 半角 `'"\/#&`分别对应的设定字符为全角 `'"\/#&`。

- 需要说明的是, 在本发明实施例中, 诸如术语“包括”、“包含”或者
20 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、物品或者终端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、物品或者终端设备所固有的要素。在没有更多限制的情况下, 由语句“包括……”或“包含……”限定的要素, 并不排除在包括所述要素的过程、方法、物品或者终端设备
25 中还存在另外的要素。此外, 在本发明实施例中, “大于”、“小于”、“超过”等理解为不包括本数; “以上”、“以下”、“以内”等理解为包括本数。

上述各实施例是参照根据实施例所述的方法、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计算机设备的处理器以产生一个机器，使得通过计算机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。

这些计算机程序指令也可存储在能引导计算机设备以特定方式工作的计算机设备可读存储器中，使得存储在该计算机设备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。

这些计算机程序指令也可装载到计算机设备上，使得在计算机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。

尽管已经对上述各实施例进行了描述，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改，所以以上所述仅为本发明的实施例，并非因此限制本发明的专利保护范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围之内。

工业实用性

本发明实施例的方法设置简单，相比分别在不同的jsp函数中对用于请求的每个参数都进行不同的验证(例如现有技术中常用的在jsp函数中对用户登入的用户名和密码的参数进行是否是全数值的校验、或全字母的校

验), 本发明实施例提供的方法不需要逐一设置验证规则, 而可以对网页发送的请求的参数进行过滤, 其有效的防御 xss 攻击的同时, 也降低了工程师的代码量, 有效的缩短了开发时间和缩短了开发成本。

相比于通过过滤 script 等关键字符串, 本发明实施例通过过滤字符, 黑客无法在过滤字符中注入空格等方式规避, 从而有效的避免现有技术中黑客通过在字符串中加入空格等方式规避对 xss 攻击的过滤的问题。

权利要求书

1、一种预防 xss 攻击的方法，包括步骤：

配置 xssfilter，使其在过滤函数中对网页向目标服务器发送的请求的参数进行过滤，所述进行过滤指判断请求的参数中是否包含设定的关键字，若请求的参数中出现设定的关键字，则将其替换为对应的设定字符。

2、根据权利要求 1 所述的预防 xss 攻击的方法，其中，所述设定的关键字指 ASCII 编码中的指除数字、大写字母、小写字母、美元符号外的所有字符，设定的关键字所对应的字符为其对应的全角字符。

3、根据权利要求 1 所述的预防 xss 攻击的方法，其中，所述的配置 xssfilter 包括步骤：

在 web 应用的配置文件 web.xml 中进行配置使 xssfilter 生效；

通过 xssHttpRequestWrapper 获取请求的参数；

并对请求的参数进行过滤。

4、根据权利要求 1 所述的预防 xss 攻击的方法，其中，所述方法还包含设置关键字白名单，在对请求的参数进行过滤时，对关键字白名单中的字符不进行替换处理。

5、根据权利要求 1 所述的预防 xss 攻击的方法，其中，所述设定的关键字至少包括以下一个或多个字符：半角左尖括号、半角右尖括号；半角左尖括号、半角右尖括号分别对应的设定字符为全角左尖括号、全角右尖括号。

6、根据权利要求 1 所述的预防 xss 攻击的方法，其中，所述设定的关键字至少包括以下一个或多个字符：半角双竖线和半角等号，半角左尖括号、半角右尖括号分别对应的设定字符为全角双竖线和全角等号。

7、根据权利要求 1 所述的预防 xss 攻击的方法，其中，所述设定的关键字至少包括以下一个或多个字符：半角字符'"\/#&；半角'"\/#&

分别对应的设定字符为全角'"\"/ # &。

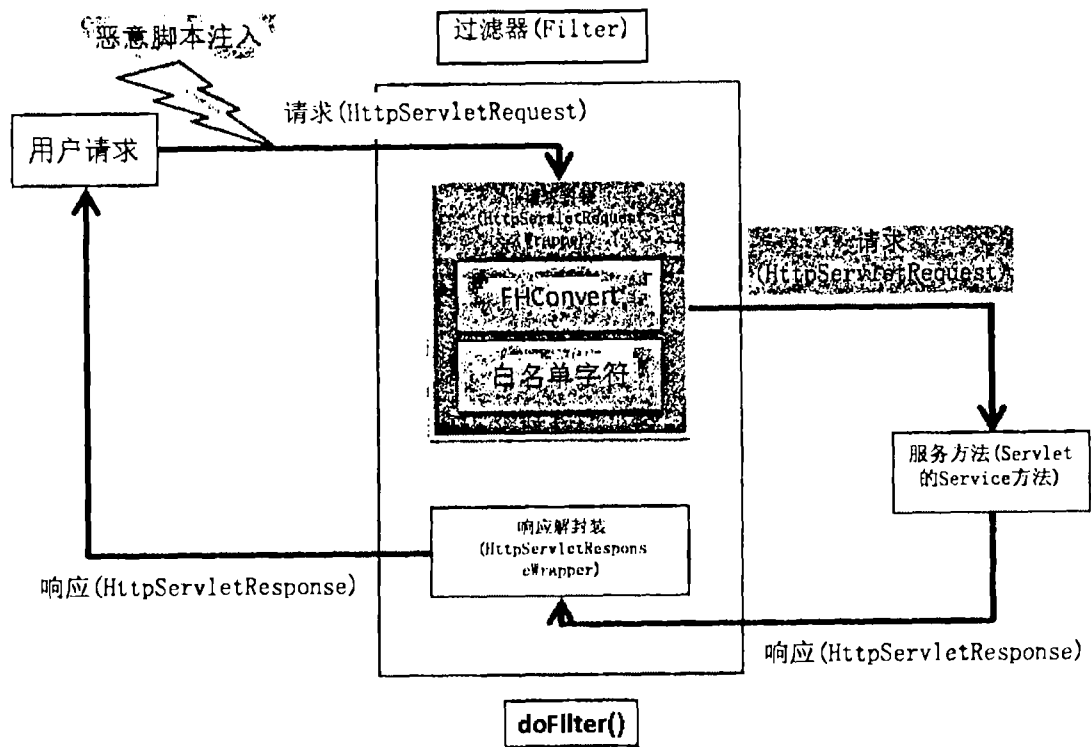


图 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/107349

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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 29/-; G06F 21/-

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)

CPRSABS, DWPI: 过滤, 参数, 关键字, 字符, xss, filter, parameter, key word, character

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104182685 A (BEIJING JINGDONG SHANGKE INFORMATION TECHNOLOGY CO., LTD.; BEIJING JINGDONG CENTURY TRADING CO., LTD.) 03 December 2014 (03.12.2014), claims 1-10	1-7
A	CN 104601540 A (HUAWEI TECHNOLOGIES CO., LTD.) 06 May 2015 (06.05.2015), entire document	1-7
PX	CN 106357668 A (FUJIAN YIRONG INFORMATION TECHNOLOGY CO., LTD.; STATE GRID CORP CHINA; STATE GRID INFORMATION & TELECOMMUNICATION CO., LTD.; STATE GRID INFO-TELECOM GREAT POWER SCIENCE AND TECHNOLOGY CO., LTD.) 25 January 2017 (25.01.2017), claims 1-7	1-7

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 10 July 2017	Date of mailing of the international search report 20 July 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer MING, Mei Telephone No. (86-10) 62411851

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/107349

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104182685 A	03 December 2014	None	
CN 104601540 A	06 May 2015	None	
CN 106357668 A	25 January 2017	None	

国际检索报告

国际申请号

PCT/CN2016/107349

A. 主题的分类 H04L 29/06 (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) H04L29/-; G06F21/- 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)) CPRSABS, DWPI: 过滤, 参数, 关键字, 字符, xss, filter, parameter, key word, character		
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
X	CN 104182685 A (北京京东尚科信息技术有限公司 北京京东世纪贸易有限公司) 2014 年 12 月 3 日 (2014 - 12 - 03) 权利要求 1-10	1-7
A	CN 104601540 A (华为技术有限公司) 015) 5. 6. (015) - 56) 全文	1-7
PX	CN 106357668 A (福建亿榕信息技术有限公司 国家电网公司 国网信息通信产业集团有限公司 国网信通亿力科技有限责任公司) 2017 年 1 月 25 日 (2017 - 01 - 25) 权利要求 1-7	1-7
☐ 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 2017 年 7 月 10 日		国际检索报告邮寄日期 2017 年 7 月 20 日
ISA/CN 的名称和邮寄地址 中华人民共和国国家知识产权局 (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 明媚 电话号码 (86-10) 62411851

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/107349

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	104182685	A	2014年 12月 3日	无	
CN	104601540	A	2015年 5月 6日	无	
CN	106357668	A	2017年 1月 25日	无	