

一种敏感信息处理方法、装置、服务器及安全判定系统

技术领域

本申请属于信息通信领域，尤其涉及计算机页面信息交互中一种敏感信息处理方法、装置、服务器及安全判定系统。

背景技术

随着信息科技的发展，通过互联网获取信息已经成为人们获取信息的一种重要方式。其中主要的方式中包括通过客户端浏览器发送 HTTP 页面请求至服务器，由服务器响应 HTTP 请求并将请求的页面信息返回至客户端，供客户端的用户浏览。

所述服务器返回的页面中常常包含与用户个人有关的敏感信息，例如用户的账号名称、通信地址、手机号码、身份证信息等。而非法用户可以通过查看页面源代码、网络抓取数据包等简单易行的方式获取页面中的敏感信息，导致用户信息泄露。例如可以通过网络工具提取页面信息中“mailto:”后面的信息或者“@”前后的信息达到提取页面中的 Email 信息的目的。

现有技术中，常用的对敏感信息处理的方法包括通过嵌入页面中 JavaScript 脚本对敏感信息进行加密、屏蔽，或者阻止非法用户对服务器返回的页面进行抓包等处理方法。例如可以将 Email 敏感信息转换成 ASCII 编码的字符串形式，然后用 JavaScript 脚本语言中的 document.write 方法写入到页面中，完成对电子邮箱敏感信息的处理。

但是，现有技术中，服务器返回的页面中的敏感信息常常是未经过 JavaScript 脚本处理的原始敏感信息，进一步的，即使页面的中的敏感信息通过 JavaScript 脚本处理，非法用户也可以在客户端通过删除 JavaScript 脚本或阻止相应的 JavaScript 脚本的运行等低难度手段获取页面中的敏感信息。因此，现有技术常用的对页面敏感信息的处理方法的导致页面中敏感信息的安全性较低。

发明内容

本申请目的在于提供一种敏感信息处理的方法、装置、服务器及安全判定系统，可以提高页面中敏感信息的安全性。

本申请提供的一种敏感信息处理的方法、装置、服务器及安全判定系统是这样实现的：
一种敏感信息处理的方法，所述方法包括：

获取页面中的待处理信息；

根据预先设置的敏感信息识别策略判断所述待处理信息是否为敏感信息；

在所述待处理信息为敏感信息时，按照预先设置的敏感信息处理策略进行处理，形成已处理敏感信息；

将所述已处理敏感信息替换所述页面中相应的待处理信息，形成敏感信息处理后的页面。

一种实现敏感信息处理的装置，所述装置包括：

信息获取单元，用于获取页面中的待处理信息；

敏感信息库，用于存储敏感信息；

敏感信息识别单元，用于基于所述敏感信息库中存储的敏感信息判断所述待处理信息是否为敏感信息；

处理策略单元，用于存储敏感信息处理策略；

信息处理单元，用于在所述敏感信息识别单元判断所述待处理信息为敏感信息时，基于所述处理策略单元存储的敏感信息处理策略对所述待处理信息进行处理，形成已处理敏感信息。

一种实现敏感信息处理的服务器，所述服务器包括：

MVC 目标系统，用于接收客户端发送的 HTTP 请求，并根据所述 HTTP 请求生成页面模版 ModelMap；还用于向所述生成的页面模版 ModelMap 中传入待处理信息，完成对所述 HTTP 请求相对应的页面的渲染；还用于将渲染后的页面发送至客户端；还用于接收敏感信息处理模块发送的已处理敏感信息，并将所述已处理敏感信息替换所述页面模版 ModelMap 中相对应的待处理信息；

拦截器，用于获取所述页面模版 ModelMap 中的待处理信息，并将所述待处理信息发送至敏感信息处理模块；还用于接收敏感信息处理模块发送的已处理敏感信息，并将所述已处理敏感信息发送至所述 MVC 目标系统；

敏感信息处理模块，用于接收并判断所述待处理信息是否为敏感信息；还用于按照预先设置的敏感信息处理策略对所述判断为敏感信息的待处理进行处理，形成已处理敏感信息；

所述敏感信息处理模块包括：

信息接收单元，用于接收待处理信息；

第一敏感信息库，用于存储敏感信息；

第一敏感信息识别单元，用于基于所述第一敏感信息库中存储的敏感信息判断所述待处理信息是否为敏感信息；

第一处理策略单元，用于存储敏感信息处理策略；

第一信息处理单元，用于在所述第一敏感信息识别单元判断所述待处理信息为敏感信息时，基于所述第一处理策略单元存储的敏感信息处理策略对所述待处理信息进行处理，形成已处理敏感信息；

第一回传单元，用于将所述已处理敏感信息发送至拦截器。

一种安全判定系统，所述系统包括：

第二敏感信息库，用于存储敏感信息；还用于接收第二待处理敏感信息单元发送的变量名，并判断所述存储的敏感信息中是否包括所述接收的变量名；还用于在所述判断结果为所述敏感信息库中不包括所述接收的变量名时，将所述变量名作为新增敏感信息进行存储；

第二敏感信息识别单元，用于获取页面中的待处理信息；还用于基于所述第二敏感信息库中存储的敏感信息判断所述待处理信息是否为敏感信息；

第二信息处理单元，用于存储敏感信息处理策略；还用于在所述第二敏感信息识别单元判断所述待处理信息为敏感信息时，基于所述存储的敏感信息处理策略对所述待处理信息进行处理，形成已处理敏感信息；

监控单元，用于存储预先设置的敏感信息监控策略；还用于根据所述存储的敏感信息监控策略判断所述页面服务器 MVC 框架结构中 ModelMap 的变量信息的值是否为待处理敏感信息；还用于在判断所述变量信息的值为待处理敏感信息时，将与所述变量信息的值相对应的变量名发送至所述第二敏感信息库；

新增敏感信息日志单元，用于生成新增敏感信息日志，所述新增敏感信息日志包括所述第二敏感信息库中新增敏感信息的数目；

待处理敏感信息日志单元，用于生成待处理敏感信息日志，所述待处理敏感信息日志包括监控单元判断的待处理敏感信息的数目；

第一安全判定单元，用于获取第一目标系统的所述新增敏感信息日志或所述待处理敏感信息日志或所述第二敏感信息库中的数据，并根据预定的判定规则判定所述第一目标系统的所属的安全级别。

本申请提供的一种敏感信息处理的方法、装置、服务器及安全判定系统，可以在页面服务器端获取待处理的信息，并按照预定的敏感信息识别策略判断所述待处理信息是否为敏感信息。在所述待处理信息为敏感信息时，可以按照预先设置的敏感信息处理策略对敏感信息进行处理，然后将已处理敏感信息返回至页面中，形成敏感信息处理后的页面。客户端接收的页面为在服务器端经过敏感信息处理的页面，即使客户端的非法用户采用抓取数据包或删除JavaScript脚本等也无法获取页面中真实的敏感信息，提高了页面中敏感信息的安全性。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图1是本申请所述服务器采用MVC框架页面结构的用户与服务器的交互流程示意图；

图2是本申请一种敏感信息处理的方法的一个实施例的方法流程图；

图3是本申请一种敏感信息处理的方法的另一种实施例的流程示意图；

图4是本申请一种实现敏感信息处理装置一种实施例的模块结构示意图；

图5是本申请一种实现敏感信息处理装置中敏感信息识别单元的模块结构示意图；

图6是本申请一种实现敏感信息处理装置中处理策略单元的模块结构示意图；

图7是本申请一种实现敏感信息处理的装置另一种实施例的模块结构示意图；

图8是本申请一种实现敏感信息处理的装置另一种实施例的模块结构示意图；

图9是本申请一种实现敏感信息处理的装置另一种实施例的模块结构示意图；

图10是本申请所述一种实现敏感信息处理的服务器的另一种实施例的模块结构示意图；

图11是本申请一种安全判定系统的一种实施例的模块结构示意图；

图12是本申请一种安全判定系统的另一种实施例的模块结构示意图。

具体实施方式

为了使本技术领域的人员更好地理解本申请中的技术方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护的范围。

MVC框架是一种Web服务器常用的使用MVC（Model View Controller 模型-视图-控制器）将软件业务逻辑、数据、界面显示进行分离的web应用程序的设计创建模式。其中，模型（Model）可以用于封装与应用程序的业务逻辑相关的数据以及对数据的处理方法，通常有对数据的直接访问的权限，例如对数据库的访问。视图（View）可以用于数据的显示，通常是应用程序中与用户界面相关的部分，例如用户可以浏览并与之交互的页面界面。通常情况下视图可以是依据所述模型数据创建的。控制器（Controller）起到不同层面间的组织作用，可以用于处理事件并作出响应。MVC框架模式的三个模块可以相互独立，改变其中一个可以

不影响其他两个，可以使同一个模型被不同的视图重复使用。例如，用户A希望可以通过浏览器收发电子邮件，同时还希望可以通过手机访问电子邮箱。在服务器端可以采用MVC框架设计模式，模型可以响应用户的请求并返回响应数据，视图可以格式化数据并可以呈现给用户页面的Internet界面和WAP界面。

图1为服务器采用MVC框架页面结构的用户与服务器的交互流程示意图。如图1所述，用户可以通过客户端的浏览器向服务器发送HTTP请求。采用MVC框架模式的Web服务器在获取用户通过浏览器发送的HTTP请求时，根据所述HTTP请求生成相应的页面模型，然后对所述生成的页面模型进行渲染。所述页面模型通常可以由页面设计开发人员预先设计或系统存储的页面模版（ModelMap），所述页面模版中可以包括变量信息。所述对页面模型渲染可以包括通过控制器（Controller）找到页面模版中的变量信息，并根据用户的HTTP请求将所述页面模块中的变量替换成相应的真实数据。服务器完成对页面模版（ModelMap）的渲染后，可以将渲染后的页面回传给用户，视图模块（View）可以控制所述渲染后的页面在用户客户端的显示界面。

本申请提供一种敏感信息处理的方法，可以在服务器向用户回传页面之前，对用户的敏感信息进行处理，使用户客户端接收到的页面中所包含的敏感信息为已在服务器端进行相应处理的敏感信息。图2是本申请所述一种敏感信息处理的方法的一个实施例的方法流程图。如图2所示，所述的一种敏感信息处理的方法可以包括：

S1：获取页面中的待处理信息；

所述待处理信息可以根据页面服务器的框架结构进行设定。本实施例中所述待处理信息可以包括页面服务器 MVC 框架结构中 ModelMap 的变量信息。所述页面服务器在收到用户端发送的 HTTP 请求时，可以创建一个空的 ModelMap 页面模版。该页面模版 ModelMap 在 MVC 框架结构中可以是作为一个存储结构，可以用于存储页面中需要返回给用户端的信息。前述中，所述页面模版 ModelMap 可以包括变量，所述变量的数据格式通常为包括变量名（键）与值的 map（key：value）键值对数据格式，其中变量的值“value”通常可以采用空值或默认的字符串表示初始值。在 Controller 阶段，可以通过 ModelMap.put（）操作向 ModelMap 中的变量存放数据。例如，ModelMap 中设置的一个变量为（name1：value），可以通过 ModelMap.put（“name1”，“张三”）这样的操作向所述 ModelMap 中的“name1”变量存放该变量的值“张三”。

在本实施例中，在向所述 ModelMap 中的变量存放数据后，可以获取 ModelMap 的数据，本实施例中可以指获取页面服务器 MVC 框架结构中 ModelMap 的变量信息，以所述 ModelMap 中的变量信息作为所述页面中的待处理信息。需要说明的，本申请中所述的一种

敏感信息处理的方法中，可以在页面服务器向页面中的变量存放数据的同时获取该变量信息，也可以在页面服务器存放完页面中所有的变量后获取页面中的变量信息。在本实施例在采用 MVC 框架结构的页面服务器中，可以在 MVC 框架向所述 ModelMap 中存放完所有的变量的数据后获取所述变量信息，并将所述变量信息作为待处理信息。

在本申请的另一个实施例中，图 3 是本申请所述一种敏感信息处理的方法的另一种实施例的流程示意图。如图 3 所示，所述一种敏感信息处理的方法中所述获取页面中的待处理信息可以包括通过拦截器的 postHandle 处理程序获取 MVC 框架中变量信息，所述获取的变量信息作为待处理信息。具体的可以包括：

在 MVC 框架的 Controller 阶段，页面服务器以(变量名：值)的形式向 ModelMap 中的变量存放变量信息。在存放完 ModelMap 中的所有变量后，MVC 框架可以将 ModelMap 数据发送至拦截器，由拦截器的 postHandle 处理程序接收所述 MVC 框架发送的 ModelMap 数据。所述 postHandle 处理程序可以遍历所述 ModelMap 中的变量信息，获取所述 ModelMap 中的变量，并以所述获取的变量信息作为待处理信息。

所述拦截器，通常可以包括用于在应用程序某个执行步骤或字段被访问之前对访问源进行拦截，可以在拦截之前或之后执行特定的处理步骤。在 MVC 框架结构中，所述拦截器可以包括三种处理方法：

preHandle () --在 Controller 被调用之前调用，可以用于初始化操作或对请求进行预处理；

postHandle () --在 Controller 被调用之后渲染视图之前调用，可以用于对模型数据或视图进行处理；

afterCompletion () --在视图呈现之后调用，可以用于进行资源清理。

通常所述拦截器各个处理方法可以由相应的处理单元实现，例如所述 preHandle 处理阶段可以由拦截器的实体装置 preHandler 实现，当然，所述 postHandle 处理阶段可以由拦截器的实体装置 postHandler 实现。

如图 3 所示，通常在 preHandle 阶段，所述 ModelMap 中还没有存放数据，因此可以在 postHandle 或 afterCompletion 阶段获取所述待处理信息，即本实施例中 MVC 框架结构 ModelMap 中的变量信息。本实施例中优选的方式为可以在 MVC 框架结构中 Controller 被调用之后、视图渲染之前通过拦截器获取所述页面中的待处理信息，介入对敏感信息的判别处理。具体的在本实施例，向所述 ModelMap 中存放变量数据之后，可以由拦截器的 postHandle 处理程序获取 ModelMap 中的变量信息。当然，也可以在所述 MVC 框架结构中渲染(Velocity)调用之后通过拦截器获取所述页面中的待处理信息，即在所述拦截器的 afterCompletion 阶段

获取所述待处理信息。

需要说明的是，本实施例中通过拦截器获取及后续的修改 **ModelMap** 中变量信息的方法适用于基于所述 **MVC** 框架其他框架结构中，例如 **webx** 框架结构等。针对不同的页面服务器框架可以有不同的拦截器，在本实施例在基于所述 **MVC** 的框架结构中，可以在页面渲染（**Velocity**）之前、**Controller** 被调用之后由相应的拦截器获取及处理所述待处理信息，也可以在所述页面渲染（**Velocity**）之后由相应的拦截器获取及处理所述待处理信息。优选的实施方式为在页面渲染（**Velocity**）之前、**Controller** 被调用之后由相应的拦截器获取及处理所述待处理信息。

获取页面服务器 **MVC** 框架结构中 **ModelMap** 中的变量信息，以所述变量信息作为页面中的待处理信息。

S2：根据预先设置的敏感信息识别策略判断所述待处理信息是否为敏感信息。

所述的敏感信息识别策略可以为预先设置的判断所述获取的待处理信息是否为敏感信息的判别规则或方法的集合。例如所述待处理信息为所述页面服务器 **MVC** 框架结构中 **ModelMap** 的变量信息时，所述敏感信息识别策略可以包括设置用于存储敏感信息的敏感信息库。所述根据预先设置的敏感信息识别策略判断所述待处理信息是否为敏感信息可以包括：

S201：获取页面服务器 **MVC** 框架结构 **ModelMap** 中变量信息的变量名；

S202：将所述获取的 **ModelMap** 中变量信息的变量名与敏感信息库中存储的敏感信息相比较，判断所述变量名是否在所述敏感信息库中；

S203：根据所述变量名是否在所述敏感信息库中的判断结果判断所述待处理信息是否为敏感信息。

在本实施例中，可以设置包括预先定义的敏感信息的敏感信息库。例如，可以将用户的用户名、电话号码、电子邮件、身份证号码信息预先定义为敏感信息，可以将其在所述 **ModelMap** 中的对应的变量名（key）“**User**”、“**Tel_Num**”、“**E-Mail**”、“**ID_Num**”预先存储在敏感信息库中。在获取所述 **ModelMap** 中变量信息的变量名后，可以将获取的变量名与所述敏感信息库中存储的敏感信息相比较。如果所述敏感信息库中包括与所述获取的变量名相同的敏感信息，则可以表示所述待处理信息为敏感信息，即可以表示本实施例中所述变量名所对应的 **ModelMap** 中的变量信息为敏感信息；如果所述比较的结果为所述敏感信息库中不包括与所述获取的变量名相同的敏感信息，则可以表示所述待处理信息不是敏感信息，即可以表示本实施例中所述变量名所对应的 **ModelMap** 中的变量信息不是敏感信息。

上述所述敏感信息库中存储的敏感信息可以根据需求进行增加或删除或修改。

当然，所述业务服务器框架结构为其他架构模式时，所述获取的待处理信息可以为其他与所述服务器框架结构相对应的数据格式，所述敏感信息识别策略也可以根据待处理信息和服务器框架进行相应的设置，例如可以直接判断所述待处理信息整个数据是否为敏感信息或者基于指定的数据判断所述待加密信息是否为敏感信息。

在本实施例基于 MVC 的框架结构中，所述根据预先设置的敏感信息识别策略判断所述待处理信息是否为敏感信息。

S3: 在判断所述待处理信息为敏感信息时，可以按照预先设置的敏感信息处理策略进行处理，形成已处理敏感信息。

在所述待处理信息判断的结果为敏感信息时，可以按照预先设置的敏感信息处理策略对所述待处理信息进行处理。所述敏感信息处理策略可以包括预先设置的对判断为敏感信息的所述待处理信息的处理规则或方法的集合。在本实施例中，所述待处理信息为 **ModelMap** 中的变量（变量名：值）的数据格式时，所述按照预先设置的敏感信息处理策略进行处理可以包括对所述变量信息中变量名所对应的值进行处理。具体的所述敏感信息处理策略可以包括下述中的至少一种：

不处理、预定部分展示、完全屏蔽、按权限屏蔽、变换后展示、误报。

所述不处理，可以包括对所述变量名所对应的值不进行屏蔽、变换、替代等处理，所述变量名所对应的值变。

所述预定部分展示，可以包括根据预定的展示规则展示所述变量名所对应的值的特定字段。例如所述待处理信息为（Tel_Num: 15912344321）时，所述预定的展示规则可以包括将变量名为“Tel: Num”所对应的值的第四位至第八位用字符“*”代替。上述待处理信息（Tel_Num: 15912344321）按照上述预定部分展示的处理策略处理后可以形成已处理敏感信息为（Tel_Num: 159*****321）。

所述完全屏蔽，可以包括根据预定的屏蔽规则屏蔽所述变量名所对应的值的所有字段。例如可以将变量名为“Tel: Num”所对应的值用一个或多个“*”字符代替，形成已处理敏感信息可以为（Tel_Num: *）或（Tel_Num: *****）。

所述按权限屏蔽，可以包括根据指定字段的权限对所述变量名所对应的值进行处理。例如，所述知道字段为获取的客户端用户的用户名，可以根据用户名所在不同域组的权限设置相应的处理方法。具体的可以例如下表 1 中所示，可以根据接收到的发送 HTTP 请求的客户端的用户的权限对敏感信息进行处理。具体例如接收的发送 HTTP 请求的用户名属于超级管理员域组时，可以设置对所有敏感信息不进行处理；所述发送 HTTP 请求的用户名属于管理员域组时，可以设置对指定敏感信息进行部分屏蔽；所述发送 HTTP 请求的用户名属于用户

域组时，可以设置对指定敏感信息进行全部屏蔽或部分屏蔽。

表 1 按权限屏蔽处理策略示意表

变量名	值	所属域组	处理策略	处理后值
Name1	张三	超级管理员	不处理	张三
Name2	李四	管理员	部分展示	李*
Name3	王五	用户	屏蔽	**
Tel_Num	15912344321	用户	部分展示	159*****321
E-Mail	user1@163.com	用户	部分展示	use**@163.com
ID_Num	320322198708081234	管理员	屏蔽	320****
Add_ID	浙江省杭州市	用户	部分展示	浙江省
Gender	女	用户	不处理	女

所述变换后展示，可以包括将所述变量名所对应的值按照预定变换规则进行变换，以所述变换后的值作为所述变量名的值。例如将 ModelMap 中的第四变量（Name4: evil）中的值“evil”按照预定规则变换为“live”后作为处理后的第四变量的值，即已处理敏感信息可以为（Name4: live）。

所述误报，可以表示为由于敏感信息的识别规则出现异常或所述判断出的敏感信息不符合根据其他条件设置的敏感信息判断标准时，对所述变量名所对应的值不进行处理操作，此时可以生成误报日志。所述误报日志中可以存储记录产生误报的次数以及每次误报的目标源（例如原始的变量名与值）、误报原因、日志产生时间等。在本实施例中可以存储所述生成的误报日志，可以用于后续的行为统计。

在具体的实施过程中，可以根据需求组合或嵌套设置所述敏感信息处理策略。例如所述按照预先设置的敏感信息处理策略进行处理可以包括：

根据所述变量信息中不同的变量名对所述不同变量名所对应的值设置敏感信息处理策略；

或者，

在所述变量信息的同一变量名中根据指定字段信息的权限对所述同一变量名所对应的值设置敏感信息处理策略。

具体的例子中，可以将用户的用户名、电话号码、电子邮件、身份证号码信息预先定义为敏感信息，其在所述 ModelMap 中的对应的变量名(key)“User”、“Tel_Num”、“E-Mail”、“ID_Num”。在设置所述敏感信息处理策略时，可以根据预先设置的敏感信息的安全级别将用户名的变量名“User”所对应的值按照预定部分展示处理策略设置只显示前两个字符，其余用“*”字符代替；将用户的电子邮箱的变量名“E-Mail”所对应的值按照预定部分展示

处理策略设置只显示字符“@”及“@”后面的字符。对于相对重要的用户的身份证号码，可以按照完全屏蔽处理策略将身份证号码的变量名“ID_Num”所对应的值全部用4位“*”字符代替。

当然，在另一种实施方式中，也可以对变量信息的同一变量中根据预先设置的指定字段信息的权限对所述同一变量名所属对应的值设置敏感信息处理策略。所述的指定字段可以包括获取的页面中的特定字段信息，例如发送HTTP请求的用户的用户名。具体的例如可以根据获取的发送HTTP请求的用户的权限对所述敏感信息进行处理。例如发送HTTP请求的用户为管理员权限时，可以将用户的电话号码的变量名“Tel_Num”所对应的值不处理，管理员在最终返回的页面中可以查看到完整的电话号码信息。如果所述发送HTTP请求的用户为普通会员，则可以将用户的电话号码的变量名“Tel_Num”所对应的值按照预定的展示规则只显示电话号码的前三位与后三位数字，其余用“*”字符代替。

在判断所述待处理信息为敏感信息时，可以按照预先设置的至少一种敏感信息处理策略进行处理，形成已处理敏感信息。

S4: 将所述已处理敏感信息替换所述页面中相应的待处理信息，形成敏感信息处理后的页面。

所述获取的页面中的待处理信息形成所述已处理敏感信息后，可以将所述已处理敏感信息发送至页面中与之相对应的待处理信息的相应位置，替换页面中的原有的待处理信息。例如在本实施例中，按照所述敏感信息处理策略对所述变量名所对应的值进行替换后，可以将值替换后的变量返回至MVC服务器框架结构的ModelMap，在MVC框架中用值替换后的变量对页面进行渲染。具体的例如在VM页面模版渲染时，可以将所述ModelMap中变量信息的变量名与所述已处理敏感信息变量名相同的变量信息中的值替换成所述已处理敏感信息中该变量名所对应的值。例如可以将已处理敏感信息（Name2: 李*）的值“李*”替换掉ModelMap中的变量（Name2: 李四）的值“李四”。当然，在判断所述待加密信息不是敏感信息或所述对敏感信息的处理策略为不处理或误报时，可以不需要对所述待加密信息进行处理，具体的，在本实施例可以不需要对ModelMap中的变量进行值的替换。

用已处理敏感信息对所述页面进行渲染形成敏感信息处理后的页面后，可以将所述敏感信息处理后的页面回传给客户端的浏览器。客户端收到经过敏感信息处理后的页面后，展示给用户的是已处理敏感信息的页面。例如，在显示当前登录的用户名的模块显示区域中本来要显示的用户名“李四”，在敏感信息处理后展示给客户端用户的用户名可以为“李*”。

本实施例提供的一种敏感信息处理的方法，可以在页面服务器端获取待处理的信息，并按照预定的敏感信息识别策略判断所述待处理信息是否为敏感信息。在所述待处理信息为敏

感信息时，可以按照预先设置的敏感信息处理策略对敏感信息进行处理，然后将已处理敏感信息返回至页面中，可以形成敏感信息处理后的页面。所述敏感信息处理后的页面中所包括的敏感信息为在服务器端经过相应处理的信息，即使客户端的非法用户采用抓取数据包或删除 JavaScript 脚本也无法获取页面中真实的敏感信息，提高了页面中敏感信息的安全性。

客户端用户发送的 HTTP 请求页面中可以包括多个待识别和处理的敏感信息，这些敏感信息可以出现在不同请求页面的不同位置，其在 MVC 框架结构 ModelMap 中也可以对应不同的变量，在后续的敏感信息处理中增加了敏感信息的识别难度。基于 MVC 框架的不同页面服务器或不同设计开发人员可以对相同的敏感信息，例如用户的电子邮箱、身份证号码等在 ModelMap 中设置不同的变量名。例如在一次页面请求的 ModelMap 中所述身份证号码变量信息对应的变量名为“ID_Num”，而在另一次页面请求中，所述 ModelMap 中身份证号码变量信息对应的变量名可以为“Num_001”。本申请提供一种动态的敏感信息处理方法的另一种实施例，在该实施例中可以根据预先设置的敏感信息监控策略动态的调整敏感信息识别策略。具体的，所述一种敏感信息处理的方法还可以包括：

S5: 根据预先设置的敏感信息监控策略判断所述页面服务器 MVC 框架结构中 ModelMap 的变量信息的值是否为待处理敏感信息；

S6: 在所述根据敏感信息监控策略判断所述变量信息的值为待处理敏感信息时，将与所述变量信息的值相对应的变量名发送至所述敏感信息库。

在本实施例中，可以根据预先设置的敏感信息监控策略判断所述 ModelMap 中变量信息的值是否为待处理的敏感信息。在具体的实施应用中，所述的敏感信息通常具有一定的数据结构格式，例如移动电话号码通常可以为 11 位的非零开头的数字组合，电子邮箱通过可以包括“@”字符。此时所述敏感信息监控策略可以通过正则匹配的方法匹配所述 ModelMap 中变量信息的值是否符合预先设置的 11 位的数字组合，或者判断所述 ModelMap 中变量信息的值是否含有“@”字符并且“@”前至少有一位非空字符等。如果通过所述敏感信息监控策略判断所述 ModelMap 中变量信息的值为待处理敏感信息，则可以将与所述变量信息的值相对应的变量名“Phone_Num”或“First_Contact”发送至所述敏感信息库中。所述敏感信息库可以接收所述与所述变量信息的值相对应的变量名“Phone_Num”或“First_Contact”，并比较所述敏感信息库中是否存储有与所述变量名相同的敏感信息。如果所述敏感信息库中没有与所述变量名相同的敏感信息，可以将所述敏感信息库中未包含但所对应的值为所述待处理敏感信息的变量名作为新增敏感信息存储在所述敏感信息库中。这样，如果当前所述敏感信息库中没有存储所述新增敏感信息“Phone_Num”或“First_Contact”时，通过所述敏感信息监控策略可以将所述变量名为“Phone_Num”或“First_Contact”的待处理敏感信息

作为新增敏感信息添加到敏感信息库中。在下次响应用户 HTTP 请求时，可以识别出变量名为“Phone_Num”或“First_Contact”的敏感信息，可以根据敏感信息处理策略对所述变量名为“Phone_Num”或“First_Contact”所对应的值进行处理。

对应上述 S5 中识别出的待处理敏感信息，还可以生成相应的待处理敏感信息日志。所述待处理敏感信息日志可以包括待处理敏感信息的个数、以及待处理敏感信息的值、值对应的变量名、是否已发送至敏感信息库以及每个待处理敏感信息的处理时间、待处理敏感信息日志生成时间等，可以用于后续系统安全判定时数据的处理。

对应上述所述敏感信息库存储的所述新增敏感信息，还可以生成相应的新增敏感信息日志。所述新增敏感信息日志可以包括新增敏感信息的个数、以及所述新增敏感信息的值、值所对应的变量名、是否已经存储在敏感信息库中以及存储时间、新增敏感信息日志生成时间等，可以用于后续系统安全判定时数据的处理。

通过本申请包括敏感信息监控策略的一种敏感信息处理的方法可以实现对敏感信息库的动态更新，可以更加准确的识别待处理信息中的敏感信息，完成对敏感信息的处理，提高页面敏感信息的安全性。

基于本申请思想，本申请提供一种实现敏感信息处理的装置。图 4 是本申请所述一种实现敏感信息处理装置一种实施例的模块结构示意图。如图 4 所示，所述装置可以包括：

信息获取单元 101，可以用于获取页面中的待处理信息；

敏感信息库 102，可以用于存储敏感信息；

敏感信息识别单元 103，可以用于基于所述敏感信息库 102 中存储的敏感信息判断所述待处理信息是否为敏感信息；

处理策略单元 104，可以用于存储敏感信息处理策略；

信息处理单元 105，可以用于在所述敏感信息识别单元 103 判断所述待处理信息为敏感信息时，基于所述处理策略单元 104 存储的敏感信息处理策略对所述待处理信息进行处理，形成已处理敏感信息。

在具体的一个实施例中，所述信息获取单元 101 获取的待处理信息可以包括：

页面服务器 MVC 框架结构中 ModelMap 的变量信息。

具体的处理过程中，所述处理策略单元 104 存储的敏感信息处理策略可以包括：

根据所述变量信息中不同的变量名对所述变量名所对应的值设置敏感信息处理策略；

或者，

在所述变量信息的同一变量名中根据指定字段信息的权限对所述同一变量名所对应的值设置敏感信息处理策略。

图 5 是本申请一种实现敏感信息处理装置中敏感信息识别单元 103 的一种实施例的模块结构示意图。如图 5 所示，所述敏感信息识别单元 103 可以包括：

键值获取单元 1031，可以用于获取页面服务器 MVC 框架结构 ModelMap 中变量信息的变量名；

比较单元 1032，可以用于比较所述获取的 ModelMap 中变量信息的变量名与所述敏感信息库 102 存储的敏感信息是否相同；

第一判断单元 1033，可以用于根据所述比较单元 1032 的比较结果判断所述待处理信息是否为敏感信息。

上述所述第一判断单元 1033 中，如果所述比较单元 1032 比较所述变量名与敏感信息库 102 存储的敏感信息的结果为相同，所述第一判断单元 1033 可以判断所述信息获取单元 101 获取的待处理信息为敏感信息；相应的，如果所述比较单元 1032 遍历所述敏感信息库 102 存储的敏感信息中没有查询到与所述变量名相同的敏感信息，比较结果为不相同，则所述第一判断单元 1033 可以判断所述信息获取单元 101 获取的待处理信息不是敏感信息。

图 6 为本申请所述一种实现敏感信息处理的装置中处理策略单元的一种实施例的模块结构示意图。如图 6 所示，所述处理策略单元 104 可以包括下述单元中的至少一种：

预定部分展示单元 1041，可以用于根据预定的展示规则展示所述变量名所对应的值的特定字段；

完全屏蔽单元 1042，可以用于根据预定的屏蔽规则屏蔽所述变量名所对应的值的所有字段；

权限屏蔽单元 1043，可以用于根据指定字段的权限对所述变量名所对应的值进行处理。具体的例如可以对权限高的用户设置对指定敏感信息不屏蔽或部分屏蔽，对权限相对较低的用户设置对指定敏感信息部分屏蔽或完全屏蔽。

变换展示单元 1044，可以用于将所述变量名所对应的值按照预定变换规则进行变换，以所述变换后的值作为所述变量名的值。

误报单元 1045，可以用于在所述敏感信息处理装置中所述的任意一个结构模块出现异常或所述敏感信息识别单元 103 所判断的敏感信息不符合第三方模块设置的敏感信息判断标准时，对所述变量名所对应的值不进行处理，并生成误报日志。所述第三方模块设置可以包括设置在所述敏感信息处理装置内或外部的其他判断所述待处理信息是否为敏感信息的模块。如果本申请所述实现敏感信息处理的装置识别敏感信息的方法与其他模块识别敏感信息的方法有冲突，可以设置对此处的敏感信息为误报，可以不进行敏感信息的数据处理。例如根据所述变量名所对应的值中包括字符“@”判断所对应的待处理信息为用户的电子邮件的敏

感信息，同时依据所述第三方模块可以判断该变量所对应的待处理信息为用户在文本框中输入的对卖家的评论，不是设置的敏感信息。此时所述敏感信息处理装置的误报单元 1045 可以对所述待处理信息不进行处理屏蔽、变换等处理，可以记录此次误报的日志。

本实施例中所述的一种实现敏感信息处理的装置，可以获取页面中的待处理信息，并根据预先设置的敏感信息识别策略判断所述待处理信息是否为敏感信息。如果是，可以根据预先设置的敏感信息处理策略对所述待处理信息进行处理，完成敏感信息的识别和处理。

在本申请另一种优选的实施例中，所述实现敏感信息处理的装置还可以包括用于维护敏感信息库中的敏感信息的单元。图 7 是本申请所述一种实现敏感信息处理的装置另一种实施例的模块结构示意图，如图 7 所述，所述装置可以包括：

监控策略单元 106，可以用于存储预先设置的敏感信息监控策略；

待处理敏感信息单元 107，可以用于根据预先设置的敏感信息监控策略判断所述页面服务器 MVC 框架结构中 ModelMap 的变量信息的值是否为待处理敏感信息；

发送单元 108，可以用于所述待处理敏感信息单元 107 判断所述变量信息的值为待处理敏感信息时，将与所述变量信息的值相对应的变量名发送至所述敏感信息库 102。

相应的，所述敏感信息库 102 可以接收与所述变量信息的值相对应的变量名，并比较所述敏感信息库 102 中是否存储有与所述变量名相同的敏感信息。如果所述敏感信息库 102 中没有与所述变量名相同的敏感信息，可以存储所述变量名。

图 8 是本申请所述一种实现敏感信息处理装置的另一种实施例，如图 8 所示，所述装置还可以包括：

替换单元 109，可以用将所述已处理敏感信息替换所述页面中相应的待处理信息。

在本实施例中，所述实现敏感信息处理的装置可以在所述装置中将所述已处理敏感信息替换所述页面中相应的待处理信息。在另一种实施方式中，可以将所述已处理敏感信息发送至服务器，由所述服务器将所述已处理敏感信息替换所述页面中相应的待处理信息，形成敏感信息处理后的页面。图 9 是本申请所述一种实现敏感信息处理装置的另一种实施例，如图 9 所示，所述装置还可以包括：

回传单元 110，可以用于将所述已处理敏感信息直接发送至服务器或通过拦截器发送至服务器的已处理敏感信息接收单元。

本申请还提供一种实现敏感信息处理的服务器，所述服务器可以包括上述实施例中任意一种所述实现敏感信息处理的装置。

本申请提供的一种实现敏感信息处理的服务器在不使用拦截器时可以包括：

第一 MVC 目标系统，可以用于接收客户端发送的 HTTP 请求，并根据所述 HTTP 请求

生成页面模版 **ModelMap**；还可以用于向所述生成的页面模版 **ModelMap** 中传入待处理信息，完成对所述 **HTTP** 请求页面的渲染；还可以用于将渲染后的页面发送至客户端；还可以用于接收敏感信息处理模块发送的已处理敏感信息，并将所述已处理敏感信息替换所述页面模版 **ModelMap** 中相对应的待处理信息；

第一敏感信息处理模块，可以用于获取所述页面模板 **ModelMap** 中的待处理信息，并根据预先设置的敏感信息识别策略判断所述待处理信息是否为敏感信息；还可以用于在所述待处理信息为敏感信息时，按照预先设置的敏感信息处理策略进行处理，形成已处理敏感信息；还可以用于将所述已处理敏感信息发送至所述 **MVC** 目标系统。

图 10 是本申请所述一种实现敏感信息处理的服务器的另一种实施例的模块结构示意图。所述服务器可以包括 **MVC** 框架结构。本申请中所述的一种实现敏感信息处理的服务器可以包括上述任意一项所述的实现敏感信息处理装置，优选实施方式中可以包括拦截器。具体的如图 10 所示，所述服务器可以包括：

MVC 目标系统 1，可以用于接收客户端发送的 **HTTP** 请求，并根据所述 **HTTP** 请求生成页面模版 **ModelMap**；还可以用于向所述生成的页面模版 **ModelMap** 中传入待处理信息，完成对所述 **HTTP** 请求页面的渲染；还可以用于将渲染后的页面发送至客户端；还可以用于接收敏感信息处理模块发送的已处理敏感信息，并将所述已处理敏感信息替换所述页面模版 **ModelMap** 中相对应的待处理信息；

拦截器 2，可以用于获取所述页面模版 **ModelMap** 中待处理信息，并将所述待处理信息发送至敏感信息处理模块 3；还可以用于接收敏感信息处理模块 3 发送的已处理敏感信息，并将所述已处理敏感信息发送至所述 **MVC** 目标系统 1；

敏感信息处理模块 3，可以用于接收并判断所述待处理信息是否为敏感信息；还用于按照预先设置的敏感信息处理策略对所述判断为敏感信息的待处理进行处理，形成已处理敏感信息。所述敏感信息处理模块可以包括：

信息接收单元，可以用于接收待处理信息；

第一敏感信息库，可以用于存储敏感信息；

第一敏感信息识别单元，可以用于基于所述第一敏感信息库中存储的敏感信息判断所述待处理信息是否为敏感信息；

第一处理策略单元，可以用于存储敏感信息处理策略；

第一信息处理单元，可以用于在所述第一敏感信息识别单元判断所述待处理信息为敏感信息时，基于所述第一处理策略单元存储的敏感信息处理策略对所述待处理信息进行处理，形成已处理敏感信息；

第一回传单元，可以用于将所述已处理敏感信息发送至拦截器。

上述所述 MVC 目标系统 1 具体的可以包括：

ModelMap 模块 11，可以用于接收客户端发送的 HTTP 请求，并根据所述 HTTP 请求生成页面模版 ModelMap；

Controller 模块 12，可以用于向所述生成的页面模版 ModelMap 中传入待处理信息；还可以用于接收拦截器发送的已处理敏感信息；

Velocity 模块 12，可以用于将所述 Controller 模块 12 接收的已处理敏感信息替换所述页面模版 ModelMap 中相对应的待处理信息；还可以用于完成对所述 HTTP 请求相应页面的渲染；

回传模块 14，可以用于将渲染后的页面发送至客户端。

所述拦截器通常可以包括 preHandler (21)、postHandler (22)、afterCompletion (23)。本申请所述的一种实现敏感信息处理的服务器中所述拦截器 2 获取页面模版 ModelMap 中的待处理信息可以包括：

通过所述拦截器的 postHandle 或 afterCompletion 处理程序获取所述页面模版 ModelMap 中的待处理信息。

在所述 MVC 目标系统中，所述待处理信息可以包括所述 ModelMap 的变量信息。

上述所述的一种实现敏感信息处理的服务器，所述第一处理策略单元包括下述单元中的至少一种：

第一预定部分展示单元，可以用于根据预定的展示规则展示所述变量名所对应的值的特定字段；

第一完全屏蔽单元，可以用于根据预定的屏蔽规则屏蔽所述变量名所对应的值的所有字段；

第一权限屏蔽单元，可以用于根据指定字段的权限对所述变量名所对应的值进行处理；

第一变换展示单元，可以用于对所述变量名所对应的值按照预定变换规则进行变换，以所述变换后的值作为所述变量名的值；

第一误报单元，可以用于在所述敏感信息处理装置中所述的任意一个结构模块出现异常或所述敏感信息识别单元所判断的敏感信息不符合第三方模块设置的敏感信息判断标准时，对所述变量名所对应的值不进行处理，并生成误报日志。

上述所述的一种实现敏感信息处理的服务器，所述第一敏感信息识别单元包括：

第一键值获取单元，可以用于获取所述 MVC 目标系统中 ModelMap 中变量信息的变量名；

第一比较单元，可以用于比较所述获取的 ModelMap 中变量信息的变量名与所述第一敏感信息库存储的敏感信息是否相同；

第二判断单元，可以用于根据所述第一比较单元的比较结果判断所述待处理信息是否为敏感信息。

上述所述的一种实现敏感信息处理的服务器，优选的实施例中，还可以包括：

第一监控策略单元，可以用于存储预先设置的敏感信息监控策略；

第一待处理敏感信息单元，可以用于根据预先设置的敏感信息监控策略判断所述 MVC 目标系统中 ModelMap 的变量信息的值是否为待处理敏感信息；

第一发送单元，可以用于所述第一待处理敏感信息单元判断所述变量信息的值为待处理敏感信息时，将与所述变量信息的值相对应的变量名发送至所述第一敏感信息库。

本申请提供的一种实现敏感信息处理的服务器中，所述 MVC 目标系统 1 在接收用户的 HTTP 请求可以由 ModelMap 模块生成页面模版 ModelMap，然后所述 MVC 目标系统中的 Controller 模块 12 向所述生成的 ModelMap 中的变量传入信息后，可以由拦截器 2 的 postHandler 中的 postHandle 处理程序获取 ModelMap 中的变量信息。进一步的所述拦截器可以将获取的变量信息发送至敏感信息处理模块 3，可以由敏感信息处理模块 3 判断所述变量信息是否为敏感信息，并对敏感信息按照预定的敏感信息处理策略进行处理，形成已处理敏感信息。所述 MVC 目标系统可以接收所述敏感信息处理模块 3 发送的已处理敏感信息，并可以将所述已处理敏感信息替换所述页面模版 ModelMap 中相应的待处理信息，完成页面的渲染。然后所述服务器可以通过回传模块 14 将敏感信息处理后的页面回传至用户的客户端。

本申请中所述的 MVC 框架包括基于 MVC（Model View Controller 模型-视图-控制器）设计创建 web 应用程序模式各种 spring mvc 框架，例如 sofa2、sofa3 或 webx 等 mvc 框架结构。

本申请提供的一种实现敏感处理的服务器，可以在服务器端实现对敏感信息的识别，并对判断为敏感信息的信息在服务器端根据预先设置的敏感信息处理策略进行处理，使服务器发送给用户客户端浏览器的页面中所包括的敏感信息为已处理敏感信息。非法用户无法通过数据截取、本地网页修改等方式获取真实的敏感信息，提供了页面敏感信息的安全性。

根据本申请所述的一种敏感信息处理方法、装置及服务器对所述敏感信息的识别、处理思想，本申请还提供一种安全判定系统，可以用于判断页面服务器是否安全以及判定所述页面服务器安全性能，还可以用于多个服务器系统之间安全性的比较，及时对安全性较低的服务器进行维护，提高服务器的安全性。图 11 是本申请所述一种安全判定系统的模块结构示意图，如图 11 所示，所述的一种安全判定系统可以包括：

第二敏感信息库 201，可以用于存储敏感信息；还可以用于接收第二待处理敏感信息单元 205 发送的变量名，并判断所述存储的敏感信息中是否包括所述接收的变量名；还可以用于在所述判断结果为所述敏感信息库中不包括所述接收的变量名时，将所述变量名作为新增敏感信息进行存储；

第二敏感信息识别单元 202，可以用于获取页面中的待处理信息；还可以用于基于所述第二敏感信息库 201 中存储的敏感信息判断所述待处理信息是否为敏感信息；

第二信息处理单元 203，可以用于存储敏感信息处理策略；还可以用于在所述第二敏感信息识别单元 202 判断所述待处理信息为敏感信息时，基于所述存储的敏感信息处理策略对所述待处理信息进行处理，形成已处理敏感信息；

监控单元 204，可以用于存储预先设置的敏感信息监控策略；还可以用于根据所述存储的敏感信息监控策略判断所述页面服务器 MVC 框架结构中 ModelMap 的变量信息的值是否为待处理敏感信息；还用于在判断所述变量信息的值为待处理敏感信息时，将与所述变量信息的值相对应的变量名发送至所述第二敏感信息库 201；

新增敏感信息日志单元 205，可以用于生成新增敏感信息日志，所述新增敏感信息日志可以包括所述第二敏感信息库 201 所述新增敏感信息的数目；

待处理敏感信息日志单元 206，可以用于生成待处理敏感信息日志，所述待处理敏感信息日志可以包括监控单元 204 判断的待处理敏感信息的数目；

第一安全判定单元 207，可以用于获取第一目标系统的所述新增敏感信息日志或所述待处理敏感信息日志或所述第二敏感信息库中的数据，并根据预定的判定规则判定所述第一目标系统的所属的安全级别。

所述第一安全判定单元 207 可以包括下述单元中的至少一种：

第一数目判定单元，可以用于根据第一时间窗内所述新增敏感信息的数目/第二敏感信息库中存储的敏感信息数目判定所述第一目标系统的安全级别；

第一比值判定单元，可以根据第二时间窗内所述新增敏感信息的数目与所述待处理敏感信息的数目的比值判定所述第一目标系统的安全级别。

具体的例如，可以根据第一时间窗内所述新增敏感信息的数目判定所述第一目标系统的安全级别时，可以预先划分不同安全级别所对应的新增敏感信息的数目，例如第四安全级别所包括的新增敏感信息可以为 100 条以下，第三安全级别可以为 100~1000 条，第二安全解闭可以为 1001~5000 条，第一安全级别为 5000 条以上。在另一种实施方式中，可以根据第二时间窗内所述新增敏感信息的数目与所述待处理敏感信息的数目的比值判定所述第一目标系统的安全级别。所述比值越大，表示新发现的待处理敏感信息中被处理的待敏感信息越

多或越及时，可以用于表示系统的安全性越高；相应的，所述比值越小，可以表示未被处理的待处理敏感信息越多，可以表示系统的安全性越低。当然，可以根据所述比值划分相应的安全等级，具体的可以参考上述其他实施例，再次不做赘述。

图 12 为本申请所述一种安全判定系统的另一种优选的实施例的模块结构示意图，如图 12 所示，所述安全判定系统还可以包括多系统判定单元 208，还可以用于根据预定的判定规则比较所述第一目标系统与第二目标系统的安全级别；相应的，所述第一安全判定单元 207 可以获取第二目标系统的所述新增敏感信息日志或所述待处理敏感信息日志或所述第二敏感信息库中的数据。

所述多系统判定单元 208 可以包括下述单元中的至少一种：

第二数目判定单元，可以用于根据所述第一时间窗内所述第一目标系统与第二目标系统的新增敏感信息的数目/第二敏感信息库中存储的敏感信息数目比较所述第一目标系统与第二目标系统的安全级别；

第二比值判定单元，可以根据第二时间窗内所述第一目标系统与第二目标系统新增敏感信息的数目与所述待处理敏感信息的数目的比值比较所述第一目标系统与第二目标系统的安全级别。

具体的，例如统计一周内所述第一目标系统新增的敏感信息的数目大于所述第二目标系统新增敏感信息的数目，可以表示所述第二目标系统的安全性高于所述第一目标系统。当然，所述在统计周期内所述第一目标系统新增敏感信息的数目与所述待处理敏感信息的数目的比值大于所述第二目标系统新增敏感信息的数目与所述待处理敏感信息的数目的比值，则可以表示所述第一目标对敏感信息处理及时，安全性更高。需要说明的是，上述两种方式是从不同的维度来判定系统的安全级别，例如同一个系统可以包括更多的新增敏感信息但所述比值更大，可以表示该系统初始安全性较低，但由于及时维护，安全成长性较高。

本申请提供的一种安全判定系统，摒弃了现有技术中通过目标系统存在的系统漏洞、需要更新的补丁数目等方式来判断系统是否安全以及安全性的高低。本申请的提供的从敏感信息的角度来判定系统安全性的系统，从可以目标系统中可以识别出的敏感信息数据以及对识别出的敏感信息的处理是否及时来判定目标系统的安全性能，可以从评定系统安全性的本质上对目标系统做出更加准确的安全性判定。例如，如果所述目标系统可以识别并处理总共 10 万个敏感信息中的全部敏感信息，或者新发现 100 的个待处理敏感信息中的 99 个通过操作加入到所述第二敏感信息库中，即使在现有技术中因目标系统有 M 个补丁未打或存在 N 个漏洞而导致判定目标系统的安全性低，但从对敏感信息的识别及处理的本质层面来判定所述目标系统，实质上所述目标系统的安全性是高的。利用本申请所述的一种安全判定系统可以

更加准确的判定目标系统的安全性。利用本申请可以从不同纬度比较不同目标系统的安全性，对安全性较低的目标系统，可以及时对其敏感信息进行处理或采取其他措施对目标系统进行维护，可以提高系统的安全性。

尽管本申请内容中提到包括HTTP在内的协议之类的描述，但是，本申请并不局限于必须是完全符合规范的HTTP在内的协议的情况。某些协议的基础上略加修改后的传输机制也可以实行上述本申请各实施例的方案，例如HTTPS或者HTTP的2.0版本传输协议。当然，即使不采用上述HTTP协议，而是采用私有协议，只要符合本申请上述各实施例的页面信息交互和信息判断反馈方式，仍然可以实现相同的申请，在此不再赘述。

上述实施例阐明的装置或模块，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。为了描述的方便，描述以上装置时以功能分为各种模块分别描述。当然，在实施本申请时可以把各模块的功能在同一个或多个软件和/或硬件中实现，也可以将实现同一功能的模块由多个子模块或子单元的组合实现。

本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内部包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构、类等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本申请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，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，移动终端，服务器，或者网络设备等）执行本申请各个实施例或者实施例的某些部分所述的方法。

本说明书中的各个实施例采用递进的方式描述，各个实施例之间相同或相似的部分互相

参见即可，每个实施例重点说明的都是与其他实施例的不同之处。本申请可用于众多通用或专用的计算机系统环境或配置中。例如：个人计算机、服务器计算机、手持设备或便携式设备、平板型设备、多处理器系统、基于微处理器的系统、置顶盒、可编程的电子设备、网络PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境等等。

虽然通过实施例描绘了本申请，本领域普通技术人员知道，本申请有许多变形和变化而不脱离本申请的精神，希望所附的权利要求包括这些变形和变化而不脱离本申请的精神。

权 利 要 求 书

1、一种敏感信息处理的方法，其特征在于，所述方法包括：

获取页面中的待处理信息；

根据预先设置的敏感信息识别策略判断所述待处理信息是否为敏感信息；

在所述待处理信息为敏感信息时，按照预先设置的敏感信息处理策略进行处理，形成已处理敏感信息；

将所述已处理敏感信息替换所述页面中相应的待处理信息，形成敏感信息处理后的页面。

2、如权利要求 1 所述的一种敏感信息处理的方法，其特征在于，所述获取页面中的待处理信息包括：

在 MVC 框架结构中 Controller 被调用之后、视图渲染之前通过拦截器获取所述页面中的待处理信息；

或者，

在 MVC 框架结构中 Velocity 调用之后通过拦截器获取所述页面中的待处理信息。

3、如权利要求 1 所述的一种敏感信息处理的方法，其特征在于，所述待处理信息包括：页面服务器 MVC 框架结构中 ModelMap 的变量信息。

4、如权利要求 3 所述的一种敏感信息处理的方法，其特征在于，所述根据预先设置的敏感信息识别策略判断所述待处理信息是否为敏感信息包括：

获取页面服务器 MVC 框架结构 ModelMap 中变量信息的变量名；

将所述获取的 ModelMap 中变量信息的变量名与敏感信息库中存储的敏感信息相比较，判断所述变量名是否在所述敏感信息库中；

根据所述变量名是否在所述敏感信息库中的判断结果判断所述待处理信息是否为敏感信息。

5、如权利要求 4 所述的一种敏感信息处理的方法，其特征在于，所述方法还包括：

根据预先设置的敏感信息监控策略判断所述页面服务器 MVC 框架结构中 ModelMap 的变量信息的值是否为待处理敏感信息；

在所述根据敏感信息监控策略判断所述变量信息的值为待处理敏感信息时，将与所述变量信息的值相对应的变量名发送至所述敏感信息库。

6、如权利要求 3 所述的一种敏感信息处理的方法，其特征在于，所述按照预先设置的敏感信息处理策略进行处理包括：

根据所述变量信息中不同的变量名对所述不同变量名所对应的值设置敏感信息处理策略；

或者，

在所述变量信息的同一变量名中根据指定字段信息的权限对所述同一变量名所对应的值设置敏感信息处理策略。

7、如权利要求 6 所述的一种敏感信息处理的方法，其特征在于，所述敏感信息处理策略包括下述中的至少一种：

不处理、预定部分展示、完全屏蔽、按权限屏蔽、变换后展示、误报。

8、一种实现敏感信息处理的装置，其特征在于，所述装置包括：

信息获取单元，用于获取页面中的待处理信息；

敏感信息库，用于存储敏感信息；

敏感信息识别单元，用于基于所述敏感信息库中存储的敏感信息判断所述待处理信息是否为敏感信息；

处理策略单元，用于存储敏感信息处理策略；

信息处理单元，用于在所述敏感信息识别单元判断所述待处理信息为敏感信息时，基于所述处理策略单元存储的敏感信息处理策略对所述待处理信息进行处理，形成已处理敏感信息。

9、如权利要求 8 所述的一种实现敏感信息处理的装置，其特征在于，所述信息获取单元获取的待处理信息可以包括：

页面服务器 MVC 框架结构中 ModelMap 的变量信息。

10、如权利要求 9 所述的一种实现敏感信息处理的装置，其特征在于，所述处理策略单元存储的敏感信息处理策略包括：

根据所述变量信息中不同的变量名对所述不同变量名所对应的值设置敏感信息处理策略；

或者，

在所述变量信息的同一变量名中根据指定字段信息的权限对所述同一变量名所对应的值设置敏感信息处理策略。

11、如权利要求 9 所述的一种实现敏感信息处理的装置，其特征在于，所述处理策略单元包括下述单元中的至少一种：

预定部分展示单元，用于根据预定的展示规则展示所述变量名所对应的值的特定字段；

完全屏蔽单元，用于根据预定的屏蔽规则屏蔽所述变量名所对应的值的所有字段；

权限屏蔽单元，用于根据指定字段的权限对所述变量名所对应的值进行处理；

变换展示单元，用于将所述变量名所对应的值按照预定变换规则进行变换，以所述变换后的值作为所述变量名的值；

误报单元，用于在所述敏感信息处理装置中所述的任意一个结构模块出现异常或所述敏感信息识别单元所判断的敏感信息不符合第三方模块设置的敏感信息判断标准时，对所述变量名所对应的值不进行处理，并生成误报日志。

12、如权利要求 9 所述的一种实现敏感信息处理的装置，其特征在于，所述敏感信息识别单元包括：

键值获取单元，用于获取页面服务器 MVC 框架结构 ModelMap 中变量信息的变量名；

比较单元，用于比较所述获取的 ModelMap 中变量信息的变量名与所述敏感信息库存储的敏感信息是否相同；

第一判断单元，用于根据所述比较单元的比较结果判断所述待处理信息是否为敏感信息。

13、如权利要求 9 所述的一种实现敏感信息处理的装置，其特征在于，还包括：

监控策略单元，用于存储预先设置的敏感信息监控策略；

待处理敏感信息单元，用于根据预先设置的敏感信息监控策略判断所述页面服务器 MVC 框架结构中 ModelMap 的变量信息的值是否为待处理敏感信息；

发送单元，用于所述待处理敏感信息单元判断所述变量信息的值为待处理敏感信息时，将与所述变量信息的值相对应的变量名发送至所述敏感信息库。

14、如权利要求 9 所述的一种实现敏感信息处理的装置，其特征在于，还包括：

回传单元，用于将所述已处理敏感信息直接发送至服务器或通过拦截器发送至服务器的已处理敏感信息接收单元。

15、如权利要求 9 所述的一种实现敏感信息处理的装置，其特征在于，还包括：

替换单元，用于将所述已处理敏感信息替换所述页面中相应的待处理信息。

16、一种实现敏感信息处理的服务器，其特征在于，所述服务器包括：

MVC 目标系统，用于接收客户端发送的 HTTP 请求，并根据所述 HTTP 请求生成页面模版 ModelMap；还用于向所述生成的页面模版 ModelMap 中传入待处理信息，完成对所述 HTTP 请求相对应的页面的渲染；还用于将渲染后的页面发送至客户端；还用于接收敏感信息处理模块发送的已处理敏感信息，并将所述已处理敏感信息替换所述页面模版 ModelMap 中相对应的待处理信息；

拦截器，用于获取所述页面模版 ModelMap 中的待处理信息，并将所述待处理信息发送

至敏感信息处理模块；还用于接收敏感信息处理模块发送的已处理敏感信息，并将所述已处理敏感信息发送至所述 MVC 目标系统；

敏感信息处理模块，用于接收并判断所述待处理信息是否为敏感信息；还用于按照预先设置的敏感信息处理策略对所述判断为敏感信息的待处理进行处理，形成已处理敏感信息；

所述敏感信息处理模块包括：

信息接收单元，用于接收待处理信息；

第一敏感信息库，用于存储敏感信息；

第一敏感信息识别单元，用于基于所述第一敏感信息库中存储的敏感信息判断所述待处理信息是否为敏感信息；

第一处理策略单元，用于存储敏感信息处理策略；

第一信息处理单元，用于在所述第一敏感信息识别单元判断所述待处理信息为敏感信息时，基于所述第一处理策略单元存储的敏感信息处理策略对所述待处理信息进行处理，形成已处理敏感信息；

第一回传单元，用于将所述已处理敏感信息发送至拦截器。

17、如权利要求 16 所述的一种实现敏感信息处理的服务器，其特征在于，所述拦截器获取所述页面模版 ModelMap 中的待处理信息包括：

通过所述拦截器的 postHandle 或 afterCompletion 的处理程序获取所述页面模版 ModelMap 中的待处理信息。

18、如权利要求 16 所述的一种实现敏感信息处理的服务器，其特征在于，所述第一处理策略单元包括下述单元中的至少一种：

第一预定部分展示单元，用于根据预定的展示规则展示所述变量名所对应的值的特定字段；

第一完全屏蔽单元，用于根据预定的屏蔽规则屏蔽所述变量名所对应的值的所有字段；

第一权限屏蔽单元，用于根据指定字段的权限对所述变量名所对应的值进行处理；

第一变换展示单元，用于对所述变量名所对应的值按照预定变换规则进行变换，以所述变换后的值作为所述变量名的值；

第一误报单元，用于在所述敏感信息处理装置中所述的任意一个结构模块出现异常或所述敏感信息识别单元所判断的敏感信息不符合第三方模块设置的敏感信息判断标准时，对所述变量名所对应的值不进行处理，并生成误报日志。

19、如权利要求 16 所述的一种实现敏感信息处理的服务器，其特征在于，所述第一敏感信息识别单元包括：

第一键值获取单元，用于获取所述 MVC 目标系统中 ModelMap 中变量信息的变量名；

第一比较单元，用于比较所述获取的 ModelMap 中变量信息的变量名与所述第一敏感信息库存储的敏感信息是否相同；

第二判断单元，用于根据所述第一比较单元的比较结果判断所述待处理信息是否为敏感信息。

20、如权利要求 16 所述的一种实现敏感信息处理的服务器，其特征在于，还包括：

第一监控策略单元，用于存储预先设置的敏感信息监控策略；

第一待处理敏感信息单元，用于根据预先设置的敏感信息监控策略判断所述 MVC 目标系统中 ModelMap 的变量信息的值是否为待处理敏感信息；

第一发送单元，用于所述第一待处理敏感信息单元判断所述变量信息的值为待处理敏感信息时，将与所述变量信息的值相对应的变量名发送至所述第一敏感信息库。

21、一种安全判定系统，其特征在于，所述系统包括：

第二敏感信息库，用于存储敏感信息；还用于接收第二待处理敏感信息单元发送的变量名，并判断所述存储的敏感信息中是否包括所述接收的变量名；还用于在所述判断结果为所述敏感信息库中不包括所述接收的变量名时，将所述变量名作为新增敏感信息进行存储；

第二敏感信息识别单元，用于获取页面中的待处理信息；还用于基于所述第二敏感信息库中存储的敏感信息判断所述待处理信息是否为敏感信息；

第二信息处理单元，用于存储敏感信息处理策略；还用于在所述第二敏感信息识别单元判断所述待处理信息为敏感信息时，基于所述存储的敏感信息处理策略对所述待处理信息进行处理，形成已处理敏感信息；

监控单元，用于存储预先设置的敏感信息监控策略；还用于根据所述存储的敏感信息监控策略判断所述页面服务器 MVC 框架结构中 ModelMap 的变量信息的值是否为待处理敏感信息；还用于在判断所述变量信息的值为待处理敏感信息时，将与所述变量信息的值相对应的变量名发送至所述第二敏感信息库；

新增敏感信息日志单元，用于生成新增敏感信息日志，所述新增敏感信息日志包括所述第二敏感信息库中新增敏感信息的数目；

待处理敏感信息日志单元，用于生成待处理敏感信息日志，所述待处理敏感信息日志包括监控单元判断的待处理敏感信息的数目；

第一安全判定单元，用于获取第一目标系统的所述新增敏感信息日志或所述待处理敏感信息日志或所述第二敏感信息库中的数据，并根据预定的判定规则判定所述第一目标系统的所属的安全级别。

22、如权利要求 21 所述的一种安全判定系统，其特征在于，所述第一安全判断单元包括下述单元中的至少一种：

第一数目判定单元，用于根据第一时间窗内所述新增敏感信息的数目/第二敏感信息库中存储的敏感信息数目判定所述第一目标系统的安全级别；

第一比值判定单元，根据第二时间窗内所述新增敏感信息的数目与所述待处理敏感信息的数目的比值判定所述第一目标系统的安全级别。

23、如权利要求 21 或 22 所述的一种安全判定系统，其特征在于，还包括第二多系统判定单元，用于根据预定的判定规则比较所述第一目标系统与第二目标系统的安全级别；相应的，所述第一安全判定单元获取第二目标系统的所述新增敏感信息日志或所述待处理敏感信息日志或所述第二敏感信息库中的数据。

24、如权利要求 23 所述的一种安全判定系统，其特征在于，所述多系统判定单元包括下述单元中的至少一种：

第二数目判定单元，用于根据所述第一时间窗内所述第一目标系统与第二目标系统的新增敏感信息的数目/第二敏感信息库中存储的敏感信息数目比较所述第一目标系统与第二目标系统的安全级别；

第二比值判定单元，根据第二时间窗内所述第一目标系统与第二目标系统新增敏感信息的数目与所述待处理敏感信息的数目的比值比较所述第一目标系统与第二目标系统的安全级别。