

(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 104954331 A

(43) 申请公布日 2015. 09. 30

(21) 申请号 201410120762. 5

(22) 申请日 2014. 03. 27

(71) 申请人 杭州迪普科技有限公司

地址 310051 浙江省杭州市滨江区通和路
68 号中财大厦 6 层

(72) 发明人 黄崇代

(74) 专利代理机构 北京博思佳知识产权代理有
限公司 11415

代理人 林祥

(51) Int. Cl.

H04L 29/06(2006. 01)

H04L 29/08(2006. 01)

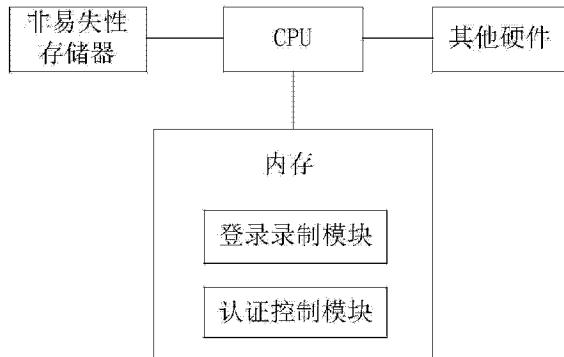
权利要求书1页 说明书4页 附图1页

(54) 发明名称

一种登录认证配置装置及方法

(57) 摘要

本发明提供一种登录认证配置装置及方法，所述装置包括：登录录制模块，用于录制用户在 web 页面登录成功时的第一认证信息，所述第一认证信息包括第一请求数据、第一响应数据及该会话对应的第一会话标识；认证控制模块，用于在 web 扫描工具登录认证时判断所述第一会话标识是否有效，若有效，则使用所述第一认证信息进行登录认证配置；否则，通过所述第一认证信息获取第二认证信息，并利用所述第二认证信息进行登录认证配置。本发明通过录制认证信息并在会话标识失效的时候可以利用录制的认证信息获取新的认证信息，因此实现 web 扫描工具的登录认证配置，从而对 web 应用进行有效的安全防护。



1. 一种登录认证配置装置，其特征在于，所述装置包括：

登录录制模块，用于录制用户在 web 页面登录成功时的第一认证信息，所述第一认证信息包括第一请求数据、第一响应数据及该会话对应的第一会话标识；

认证控制模块，用于在 web 扫描工具登录认证时判断所述第一会话标识是否有效，若有效，则使用所述第一认证信息进行登录认证配置；否则，通过所述第一认证信息获取第二认证信息，并利用所述第二认证信息进行登录认证配置。

2. 如权利要求 1 所述的装置，其特征在于，所述登录录制模块录制用户在 web 页面登录成功时的第一认证信息的录制过程具体为：

所述登录录制模块通过代理服务程序监控用户登录认证的配置过程，并录制第一请求报文、第一响应报文及该会话对应的第一会话标识。

3. 如权利要求 1 所述的装置，其特征在于，所述认证控制模块通过所述第一认证信息获取第二认证信息具体为：

认证控制模块向 web 页面重发所述第一请求数据，获取到所述 web 页面反馈的第二响应数据后，将所述第二响应数据与所述第一响应数据对比，若相同则使用所述第二认证信息进行登录认证配置。

4. 如权利要求 3 所述的装置，其特征在于，所述认证控制模块还用于，若所述第二响应数据与所述第一响应数据不同，则通知用户重新进行登录认证配置。

5. 如权利要求 1 所述的装置，其特征在于，所述第一会话标识具体为 Cookie 标识。

6. 一种登录认证配置方法，其特征在于，所述方法包括：

录制用户在 web 页面登录成功时的第一认证信息，所述第一认证信息包括第一请求数据、第一响应数据及该会话对应的第一会话标识；

在 web 扫描工具登录认证时判断所述第一会话标识是否有效，若有效，则使用所述第一认证信息进行登录认证配置；否则，通过所述第一认证信息获取第二认证信息，并利用所述第二认证信息进行登录认证配置。

7. 如权利要求 6 所述的方法，其特征在于，所述录制用户在 web 页面登录成功时的第一认证信息的录制过程具体为：

通过代理服务程序监控用户登录认证的配置过程，并录制第一请求报文、第一响应报文及该会话对应的第一会话标识。

8. 如权利要求 6 所述的方法，其特征在于，所述通过第一认证信息获取第二认证信息具体为：

向 web 页面重发所述第一请求数据，获取到所述 web 页面反馈的第二响应数据后，将所述第二响应数据与所述第一响应数据对比，若相同则使用所述第二认证信息进行登录认证配置。

9. 如权利要求 8 所述的方法，其特征在于，所述方法还包括：若所述第二响应数据与所述第一响应数据不同，则通知用户重新进行登录认证配置。

10. 如权利要求 6 所述的方法，其特征在于，所述第一会话标识具体为 Cookie 标识。

一种登录认证配置装置及方法

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种登录认证配置装置及方法。

背景技术

[0002] 随着互联网技术飞速发展，网络应用日益复杂和多元化，网络应用已经从原来的军事、科技和商业渗透到当今社会的各个领域。由于大多数的 web 应用不仅仅是静态的网页浏览，更涉及到服务端的动态处理。若网站的开发人员安全意识不足，对程序参数输入等检查不严格，将会导致 web 应用安全问题层出不穷。为了发现 web 应用的漏洞，靠手动排查是不太现实的，因此，web 扫描技术在保障网络安全方面将会起到越发重要的作用。

[0003] 通常 web 扫描工具在漏洞探测前，会利用爬虫技术对目标网站的链接进行抓取，然后根据这些链接的特征进行一系列的漏洞探测。但是，如今在许多政府机构、教学科研单位和企业中，会有各种各样的内部信息管理平台系统。这些系统一般都会要求用户进行身份认证，只有通过认证的才能获得相应的服务。这种情况下，自动化的 web 扫描工具就很难对网站进行安全评估。因此，如何需要登录认证的管理平台上实现 web 扫描的登录认证配置成为亟待解决的问题。

发明内容

[0004] 有鉴于此，本发明提供一种登录认证配置装置及方法来在 web 页面上完成 web 扫描工具的登录认证配置，从而对 web 应用进行有效安全防护。

[0005] 为了实现上述目的，本发明具体方案如下：

[0006] 一种登录认证配置装置，所述装置包括：

[0007] 登录录制模块，用于录制用户在 web 页面登录成功时的第一认证信息，所述第一认证信息包括第一请求数据、第一响应数据及该会话对应的第一会话标识；

[0008] 认证控制模块，用于在 web 扫描工具登录认证时判断所述第一会话标识是否有效，若有效，则使用所述第一认证信息进行登录认证配置；否则，通过所述第一认证信息获取第二认证信息，并利用所述第二认证信息进行登录认证配置。

[0009] 进一步的，所述登录录制模块录制用户在 web 页面登录成功时的第一认证信息的录制过程具体为：

[0010] 所述登录录制模块通过代理服务程序监控用户登录认证的配置过程，并录制第一请求报文、第一响应报文及该会话对应的第一会话标识。

[0011] 进一步的，所述认证控制模块通过所述第一认证信息获取第二认证信息具体为：

[0012] 认证控制模块向 web 页面重发所述第一请求数据，获取到所述 web 页面反馈的第二响应数据后，将所述第二响应数据与所述第一响应数据对比，若相同则使用所述第二认证信息进行登录认证配置。

[0013] 进一步的，所述认证控制模块还用于，若所述第二响应数据与所述第一响应数据不同，则通知用户重新进行登录认证配置。

- [0014] 进一步的,所述第一会话标识具体为Cookie标识。
- [0015] 基于同样的构思,本发明还提供一种登录认证配置方法,所述方法包括:
- [0016] 录制用户在web页面登录成功时的第一认证信息,所述第一认证信息包括第一请求数据、第一响应数据及该会话对应的第一会话标识;
- [0017] 在web扫描工具登录认证时判断所述第一会话标识是否有效,若有效,则使用所述第一认证信息进行登录认证配置;否则,通过所述第一认证信息获取第二认证信息,并利用所述第二认证信息进行登录认证配置
- [0018] 进一步的,所述录制用户在web页面登录成功时的第一认证信息的录制过程具体为:
- [0019] 通过代理服务程序监控用户登录认证的配置过程,并录制第一请求报文、第一响应报文及该会话对应的第一会话标识。
- [0020] 进一步的,所述通过第一认证信息获取第二认证信息具体为:
- [0021] 向web页面重发所述第一请求数据,获取到所述web页面反馈的第二响应数据后,将所述第二响应数据与所述第一响应数据对比,若相同则使用所述第二认证信息进行登录认证配置
- [0022] 进一步的,所述方法还包括:若所述第二响应数据与所述第一响应数据不同,则通知用户重新进行登录认证配置。
- [0023] 进一步的,所述第一会话标识具体为Cookie标识。
- [0024] 相对于现有技术,本发明通过录制认证信息并在会话标识失效的时候可以利用录制的认证信息获取新的认证信息,因此实现web扫描工具的登录认证配置,从而对web应用进行有效的安全防护。

附图说明

- [0025] 图1是本发明提供的一种登录认证配置装置的结构示意图;
- [0026] 图2是本发明实施例中一种登录认证配置方法的处理流程图。

具体实施方式

- [0027] 在现有技术方案中,针对web扫描工具登录过程的认证配置主要有自动表单填充和登录录制两种。
- [0028] 其中一种方案为自动表单填充,就是在web扫描前手动配置目标网站的登陆系统中的用户名与密码,而后在web扫描的过程中,将这两个参数填充到请求表单的相应键值中,从而实现登录认证。但自动表单填充所要求的条件比较苛刻,既要要求目标网站的登录过程不能有验证码,又要满足其用户名与密码没有经过加密处理。一旦这两个条件中的任何一个没有得到满足,则web扫描工具在登录页面进行登录认证时,就会导致所构造的http请求包不能成功认证。
- [0029] 另外一种方案为登录录制,就是在web扫描进行前对目标网站进行一次认证登录,扫描工具会在登录时录制登录过程,从而记录下本次登录认证的会话标识和http请求响应对以及站点管理系统内部的链接。相比之下,登录录制没有自动表单填充方案中所要求的那些苛刻条件,只需用户模拟一次正常的认证登录过程。由于登录过程中的储存在用

户本地终端上的数据(Cookie)标识可以保持登录信息到用户下次与服务器的会话,换句话说,下次访问同一网站时,用户不必输入用户名和密码就已经登录了。但 Cookie 标识在生成时就会被指定一个生存周期,在这个周期内 Cookie 标识有效,超出周期 Cookie 标识就会被清除。有些页面将 Cookie 标识的生存周期设置为“0”或负值,这样在关闭浏览器时,就马上清除 Cookie 标识,不会记录用户信息,更加安全。几乎所有的 web 扫描工具在进行登录录制时,仅能记录本次登录会话的 cookie 标识,当下次再进行扫描的时候,很有可能由于该会话标识已经失效,从而导致认证不成功。

[0030] 为了解决上述问题,本发明一种登录认证配置装置,如图 1 所示。其中,

[0031] 所述装置基本运行环境包括 CPU, 非易失性存储器、内存以及其他硬件, 从逻辑层面上来看, 所述装置包括:

[0032] 登录录制模块录制用户在 web 页面登录成功时的第一认证信息, 所述第一认证信息包括第一请求数据、第一响应数据及该会话对应的第一会话标识; 由于所述第一会话标识可以保持登录信息到用户下次与服务器的会话, 那么 web 扫描工具访问同一网站时, 不必输入用户名和密码就已经登录了。

[0033] 认证控制模块在 web 扫描工具登录认证时判断所述第一会话标识是否有效, 若有效, 则使用所述第一认证信息进行登录认证配置; 否则, 说明第一认证信息中的第一会话标识已经失效, 那么就可以通过以保存的所述第一认证信息模拟用户登录的方式去获取第二认证信息, 并利用所述第二认证信息进行登录认证配置。

[0034] 由此可见, 本发明通过录制认证信息并在会话标识失效的时候可以利用录制的认证信息获取新的认证信息, 因此实现 web 扫描工具的登录认证配置, 从而对 web 应用进行有效的安全防护。

[0035] 需要说明的是, 本发明中的登录录制模块处理过程不同于现有技术中的登录录制, 所述登录录制模块的实现录制的方式具体为: 所述登录录制模块通过 HTTP 反向代理服务程序监控用户登录认证配置过程中的数据交互, 并记录该过程中包含有所述第一请求报文、第一响应报文及该会话对应的第一会话标识的第一认证信息, 并将该信息分发至认证控制模块。值得注意的是, 通常的代理服务, 只用于代理内部网络对 Internet 的连接请求, 用户端会指定代理服务器, 并将本来要直接发送到 Web 服务器上的 http 请求发送到代理服务器中。由于外部网络上的主机并不会配置并使用这个代理服务器, 普通代理服务器也被设计成在 Internet 上搜寻多个不确定的服务器, 而不是针对 Internet 上多个用户端的请求访问某一个固定的服务器, 因此普通的代理服务器不支持外部对内部网络的访问请求。而本发明中的 HTTP 反向代理服务程序能够代理外部网络上的主机访问内部网络, 外部网络就可以简单把它当作一个标准的 Web 服务器而不需要特定的配置。不同之处在于, 这个服务器没有保存任何网页的真实数据, 所有的静态网页或者 CGI 脚本, 都保存在内部的 Web 服务器上。因此对反向代理服务程序的攻击并不会使得网页信息遭到破坏, 这样就增强了 Web 服务器的安全性。

[0036] 在优选的实施例中, 获取第二认证信息具体方案为: 所述认证控制模块向 web 页面重发所述第一请求数据, 当 web 页面的后台服务器收到该第一请求数据时, 会反馈第二响应数据; 所述装置会录制包含第二响应数据的第二认证信息, 并且所述第二认证信息中还携带着有效的第二会话标识; 当所述认证控制模块获取到所述第二响应数据后, 为了证

明请求成功，则将所述第二响应数据与登录成功时录制的所述第一响应数据对比，若相同则说明请求成功，于是可以使用所述第二认证信息进行登录认证配置。这样一来，即使会话标识失效，本发明也可以模拟用户登录认证的过程重新获取新的会话标识，进而实现登录认证配置。

[0037] 但是，若所述第二响应数据与所述第一响应数据的比较结果不同，则说明此次模拟用户登录的行为很可能不成功，因此就要通知用户重新进行手动的登录认证配置。

[0038] 在优选的实施例中，所述第一会话标识为 Cookie 标识。

[0039] 下面结合说明书附图 2，对本发明的实施方式进行详细介绍。

[0040] 假设一 web 扫描工具要对用户登录的淘宝网页进行安全扫描，由于淘宝网站需要用户的登录认证，因此 web 扫描工具就要结合本发明的登录认证配置方法进行登录认证，其具体步骤如下：

[0041] 101、在用户进行登录认证是开始录制，从而获取用户登录成功的第一认证信息，其中包括第一请求数据，以及网站服务器回复的第一响应数据和该会话的第一 Cookie 标识；

[0042] 102、当 web 扫描工具登录认证前，判断所述第一 Cookie 标识是否有效，若有效，则转步骤 103，否则转步骤 104；

[0043] 103、当第一 Cookie 标识有效时，就可以使用录制的第一认证信息进行登录认证配置；

[0044] 104、当第一 Cookie 标识失效了，就需要重新获取认证信息，因此要将所述第一认证信息中的第一请求数据重新发送到网站服务器，并接收网站服务器回复的第二响应数据；

[0045] 105、判断所述第二响应数据与第一响应数据是否相同，若相同则转步骤 106，否则转步骤 107；

[0046] 106、若所述第二响应数据与第一响应数据相同，说明请求成功，因此获取包含第二响应数据的第二认证信息并重新进行认证配置；

[0047] 107、若所述第二响应数据与第一响应数据不同，说明请求不成功，因此要通知用户重新进行手动配置认证信息，才能登录该网页。

[0048] 相对于现有技术，本发明通过录制认证信息并在会话标识失效的时候可以利用录制的认证信息获取新的认证信息，因此实现 web 扫描工具的登录认证配置，从而对 web 应用进行有效的安全防护。

[0049] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

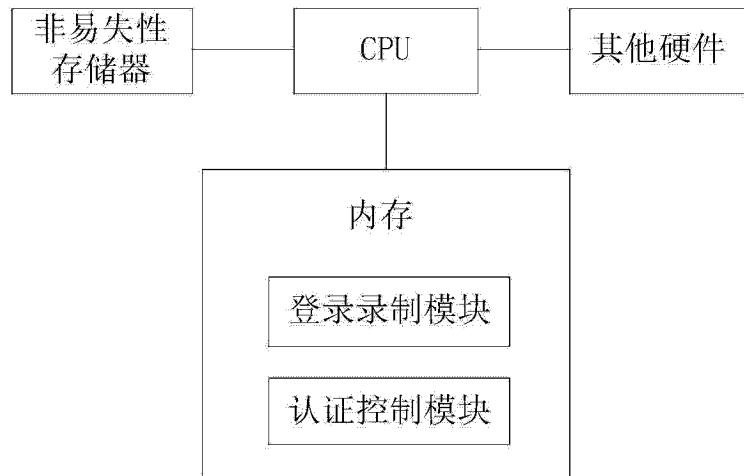


图 1

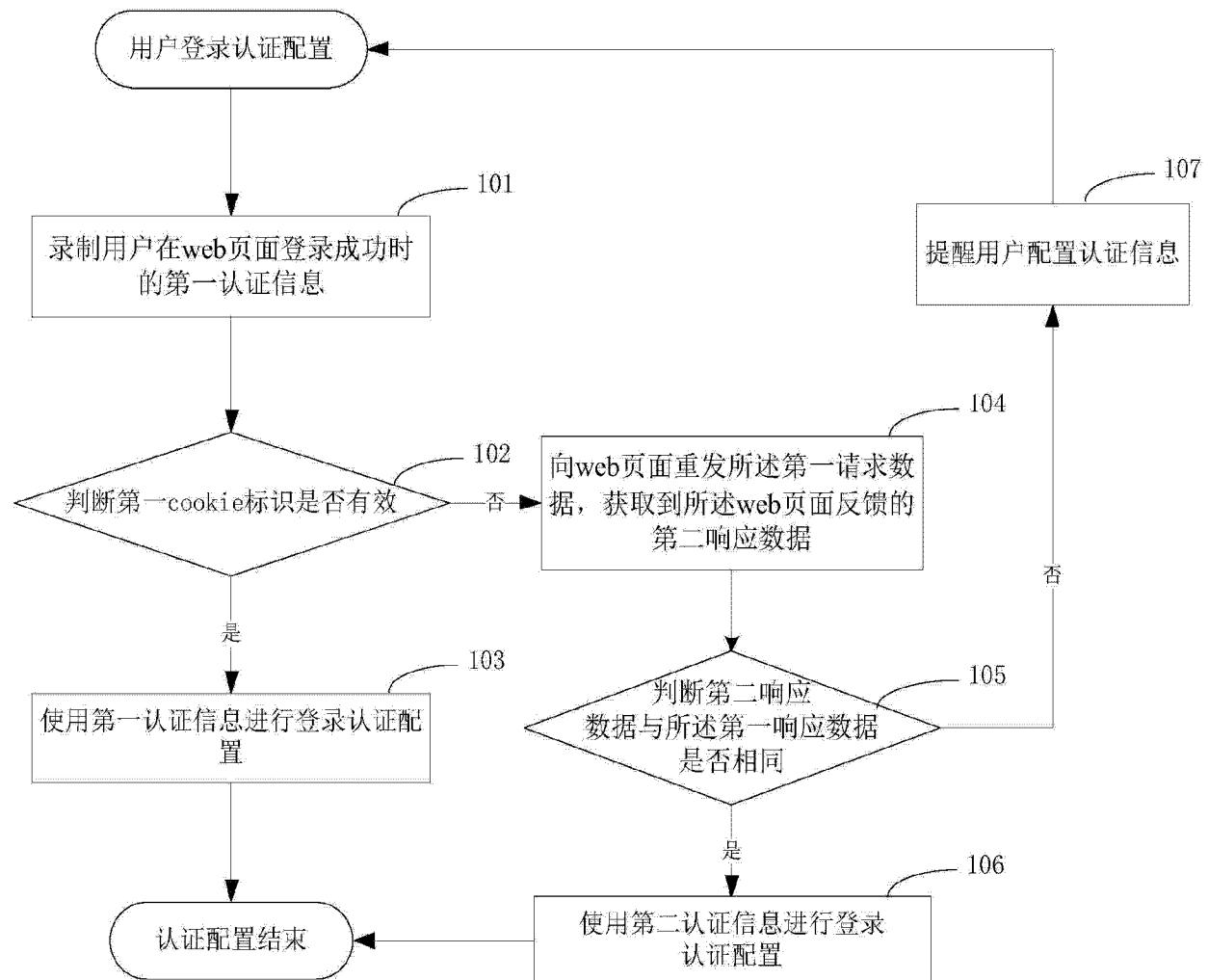


图 2