(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104732144 B
(45)授权公告日 2017.06.23

(21)申请号 201510148842.6

(22)申请日 2015.04.01

(65)同一申请的已公布的文献号
申请公布号 CN 104732144 A

(43)申请公布日 2015.06.24

(73)专利权人 河海大学
地址 211100 江苏省南京市鼓楼区西康路1号

(72)发明人 傅晓 王志坚 桂飚 杨家奇 吴昊昊 王自钊

(74)专利代理机构 南京经纬专利商标代理有限公司 32200
代理人 许方

(51)Int.Cl.
G06F 21/56(2013.01)
G06F 21/57(2013.01)
G06F 17/30(2006.01)

(56)对比文件
CN 103413092 A,2013.11.27,
CN 101984409 A,2011.03.09,
CN 102546576 A,2012.07.04,
US 2014/0173731 A1,2014.06.19,
WO 2011/073982 A1,2011.06.23,
CN 101154185 A,2008.04.02,
CN 102156832 A,2011.08.17,
CN 102646135 A,2012.08.22,
CN 103218561 A,2013.07.24,

审查员 彭苏

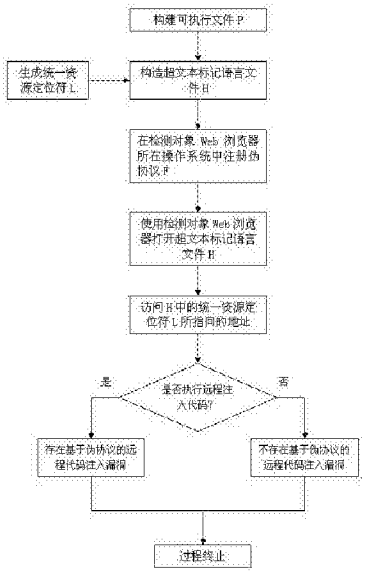
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种基于伪协议的远程代码注入漏洞检测方法

(57)摘要

本发明公开了一种基于伪协议的远程代码注入漏洞检测方法，首先构建可执行文件，设定其执行时获得的第一个命令参数为字符串；然后在待检测的对象Web浏览器所在的操作系统中注册伪协议F，其名称为字符串K、内核打开命令为所述可执行文件在操作系统中的路径；接着构造超文本标记语言文件H，其统一资源定位符为字符串K和远程注入代码组成；最后访问H中的统一资源定位符L所指向的地址，通过待检测的对象web服务器是否执行远程注入代码来判断是否存在基于伪协议的远程代码注入漏洞。本发明设计简单，使用方便，具有极高的穿透性，能够发现Web浏览器深度隐藏的远程代码注入漏洞。



CN 104732144 B

1.一种基于伪协议的远程代码注入漏洞检测方法，其特征在于，检测流程步骤为：

步骤1)，构建可执行文件，并设定其执行时获得的第一个命令参数为字符串、编码格式为E；所述可执行文件接收到参数后，根据编码格式E调用相应的解码算法将参数解码后作为命令参数执行；

步骤2)，构建命令行字符串CM为远程注入代码；

步骤3)，根据编码格式E调用相应的编码算法对命令行字符串CM进行编码；

步骤4)，在待检测的对象Web浏览器所在的操作系统中注册伪协议F，其中，伪协议F的名称为字符串K、内核打开命令为所述可执行文件在操作系统中的路径；

步骤5)，将字符串K尾部添加协议标识符“://”之后，得到字符串KP；

步骤6)，将经过编码后的命令行字符串CM附加到字符串KP尾部，得到字符串L；

步骤7)，构造超文本标记语言文件H，将字符串L作为其统一资源定位符；

步骤8)，采用待检测的对象Web浏览器打开超文本标记语言文件H，并访问统一资源定位符L所指向的地址；

步骤8.1)，若浏览器执行命令行字符串CM，判断待检测的对象 Web浏览器存在基于伪协议的远程代码注入漏洞；

步骤8.2)，若浏览器没有执行命令行字符串CM，判断待检测的对象Web浏览器不存在基于伪协议的远程代码注入漏洞。

2.根据权利要求1所述的基于伪协议的远程代码注入漏洞检测方法，其特征在于，所述Web浏览器采用机架式服务器。

3.根据权利要求2所述的基于伪协议的远程代码注入漏洞检测方法，其特征在于，所述Web浏览器的型号为联想万全R520 G7。

4.根据权利要求1所述的基于伪协议的远程代码注入漏洞检测方法，其特征在于，所述Web浏览器采用塔式服务器。

5.根据权利要求4所述的基于伪协议的远程代码注入漏洞检测方法，其特征在于，所述Web浏览器的型号为联想万全T260 G3。

一种基于伪协议的远程代码注入漏洞检测方法

技术领域

[0001] 本发明涉及信息安全中的漏洞检测技术，尤其涉及一种基于伪协议的远程代码注入漏洞检测方法。

背景技术

[0002] 随着互联网时代的来临，世界全面信息化时代也随之到来。借助以计算机、互联网等先进技术，人们越来越习惯于在各种各样的网站上获得信息和接受服务，Web系统由于其高兼容性和用户友好性，已成为当下互联网信息系统中最主流的系统类型。于此同时，Web系统的安全性也正面临严峻的挑战。

[0003] Web系统通常由Web浏览器和Web服务器两部分组成，浏览器和服务器之间使用超文本传输协议(Hyper Text Transfer Protocol，HTTP)进行信息交互。由于HTTP协议的开放性，攻击者可以模拟Web服务器的响应，通过构造特定的HTTP数据远程向客户端的Web浏览器注入恶意代码并执行，从而危害客户端计算机系统的安全性，以实现信息窃取、系统劫持等目的。这类攻击通常被称为远程代码注入攻击(Remote Code Injection)，可被攻击者利用进行此类攻击的漏洞被称为远程代码注入漏洞(Remote Code Injection Exploit)。

[0004] 目前大多数网络防火墙、入侵检测系统等安全工具，针对某些远程代码注入漏洞，如跨站脚本(Cross-Site Script，XSS)等，提供有效的检测与预防手段。但是，对于利用伪协议(URL Protocol)实施的远程代码注入，目前尚未引起安全行业内相关厂商的足够重视。

发明内容

[0005] 本发明所要解决的技术问题是针对背景技术中所涉及的问题，提供一种基于Web伪协议的远程代码注入漏洞检测方法，用以检测Web浏览器是否有潜在的远程代码注入漏洞，进而增强Web系统的安全性。

[0006] 本发明为解决上述技术问题采用以下技术方案：

[0007] 一种基于伪协议的远程代码注入漏洞检测方法，检测流程步骤为：

[0008] 步骤1)，构建可执行文件，并设定其执行时获得的第一个命令参数为字符串、编码格式为E；所述可执行文件接收到参数后，根据编码格式E调用相应的解码算法将参数解码后作为命令参数执行；

[0009] 步骤2)，构建命令行字符串CM为远程注入代码；

[0010] 步骤3)，根据编码格式E调用相应的编码算法对命令行字符串CM进行编码；

[0011] 步骤4)，在待检测的对象Web浏览器所在的操作系统中注册伪协议F，其中，伪协议F的名称为字符串K、内核打开命令为所述可执行文件在操作系统中的路径；

[0012] 步骤5)，将字符串K尾部添加协议标识符“://”之后，得到字符串KP；

[0013] 步骤6)，将经过编码后的命令行字符串CM附加到字符串KP尾部，得到字符串L；

[0014] 步骤7)，构造超文本标记语言文件H，将字符串L作为其统一资源定位符；

[0015] 步骤8)，采用待检测的对象Web浏览器打开超文本标记语言文件H，并访问统一资源定位符L所指向的地址；

[0016] 步骤8.1)，若浏览器执行命令行字符串CM，判断待检测的对象 Web浏览器存在基于伪协议的远程代码注入漏洞；

[0017] 步骤8.2)，若浏览器没有执行命令行字符串CM，判断待检测的对象Web浏览器不存在基于伪协议的远程代码注入漏洞。

[0018] 作为本发明一种基于伪协议的远程代码注入漏洞检测方法进一步的优化方案，所述Web服务器采用机架式服务器。

[0019] 作为本发明一种基于伪协议的远程代码注入漏洞检测方法进一步的优化方案，所述Web服务器的型号为联想万全R520 G7。

[0020] 作为本发明一种基于伪协议的远程代码注入漏洞检测方法进一步的优化方案，所述Web服务器采用塔式服务器。

[0021] 作为本发明一种基于伪协议的远程代码注入漏洞检测方法进一步的优化方案，所述Web服务器的型号为联想万全T260 G3。

[0022] 本发明采用以上技术方案与现有技术相比，具有以下技术效果：

[0023] 本发明设计简单，使用方便，通过编写特定的伪协议地址，可绕过Web浏览器端的漏洞检测措施实施远程代码注入，具有极高的穿透性，能够发现Web浏览器深度隐藏的远程代码注入漏洞。

附图说明

[0024] 图1是本发明的方法流程图。

具体实施方式

[0025] 下面结合附图对本发明的技术方案做进一步的详细说明：

[0026] 如图1所示，本发明公开了一种基于伪协议的远程代码注入漏洞检测方法，步骤如下：

[0027] 步骤101：构建可执行文件P，集成开发环境为Microsoft Visual Studio .Net 2008，使用语言为C#。可执行文件P算法流程如步骤102到步骤103所示：

[0028] 步骤102：设定P执行时获得的第一个命令参数的类型为字符串。设定编码格式E为“base64”，类型为字符串。P接收到参数时，调用base64解码算法将参数解码后作为命令参数执行。

[0029] 步骤103：在检测对象Web浏览器所在操作系统中注册伪协议F，此处选取浏览器为Microsoft Internet Explorer 8，操作系统为Windows 7，伪协议F的名称为字符串K，K的值为“ed2k”，因此在操作系统注册表中HKEY_CLASSES_ROOT节点下添加名称为ed2k的新节点；伪协议F的内核打开命令为步骤101中编写的可执行文件P在文件系统中的路径，因此在操作系统注册表中节点HKEY_CLASSES_ROOT\ed2k节点下创建新节点\Shell\Open\command，并设该节点的值为可执行文件P在文件系统中的路径。

[0030] 步骤104：构造超文本标记语言文件H，H的内容如下所示：

[0031] <html>

[0032] <body>

[0033] ed2k://Y21k

[0034] </body>

[0035] </html>

[0036] 其中，统一资源定位符“ed2k://Y21k”由步骤105到步骤107生成：

[0037] 步骤 105：设命令行字符串CM，其值为“cmd”，其含义是执行windows命令行程序，该字符串即为远程注入代码。由于步骤102中的编码格式E值为“base64”，因此调用base64编码算法将CM编码为“Y21k”，即即将传递给可执行文件P的参数；

[0038] 步骤 106：将步骤104中得到的字符串K尾部添加协议标识符“://”之后，得到字符串KP，KP的值为“ed2k://”；

[0039] 步骤 107：将步骤105中得到的编码后的命令行字符串CM附加到步骤107中得到的字符串KP尾部，得到字符串“ed2k://Y21k”，即所述统一资源定位符。

[0040] 步骤 108：使用检测对象Web浏览器，即步骤103中所述的Microsoft Internet Explorer 8，打开步骤104中构造的超文本标记语言文件H，并在浏览器图形界面中点击所显示的链接，Web浏览器将会自动执行步骤105中的命令行字符串CM，打开windows命令行程序窗口。因此，说明该Web浏览器存在基于Web浏览器帮助对象的远程代码注入漏洞。

[0041] 所述Web服务器可以采用机架式服务器，优先采用联想万全R520 G7。

[0042] 所述Web服务器也可以采用塔式服务器，优先采用联想万全T260 G3。

[0043] 本技术领域技术人员可以理解的是，除非另外定义，这里使用的所有术语(包括技术术语和科学术语)具有与本发明所属领域中的普通技术人员的一般理解相同的意义。还应该理解的是，诸如通用字典中定义的那些术语应该被理解为具有与现有技术的上下文中的意义一致的意义，并且除非像这里一样定义，不会用理想化或过于正式的含义来解释。

[0044] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限制本发明，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，均应包含在本发明的保护范围之内。

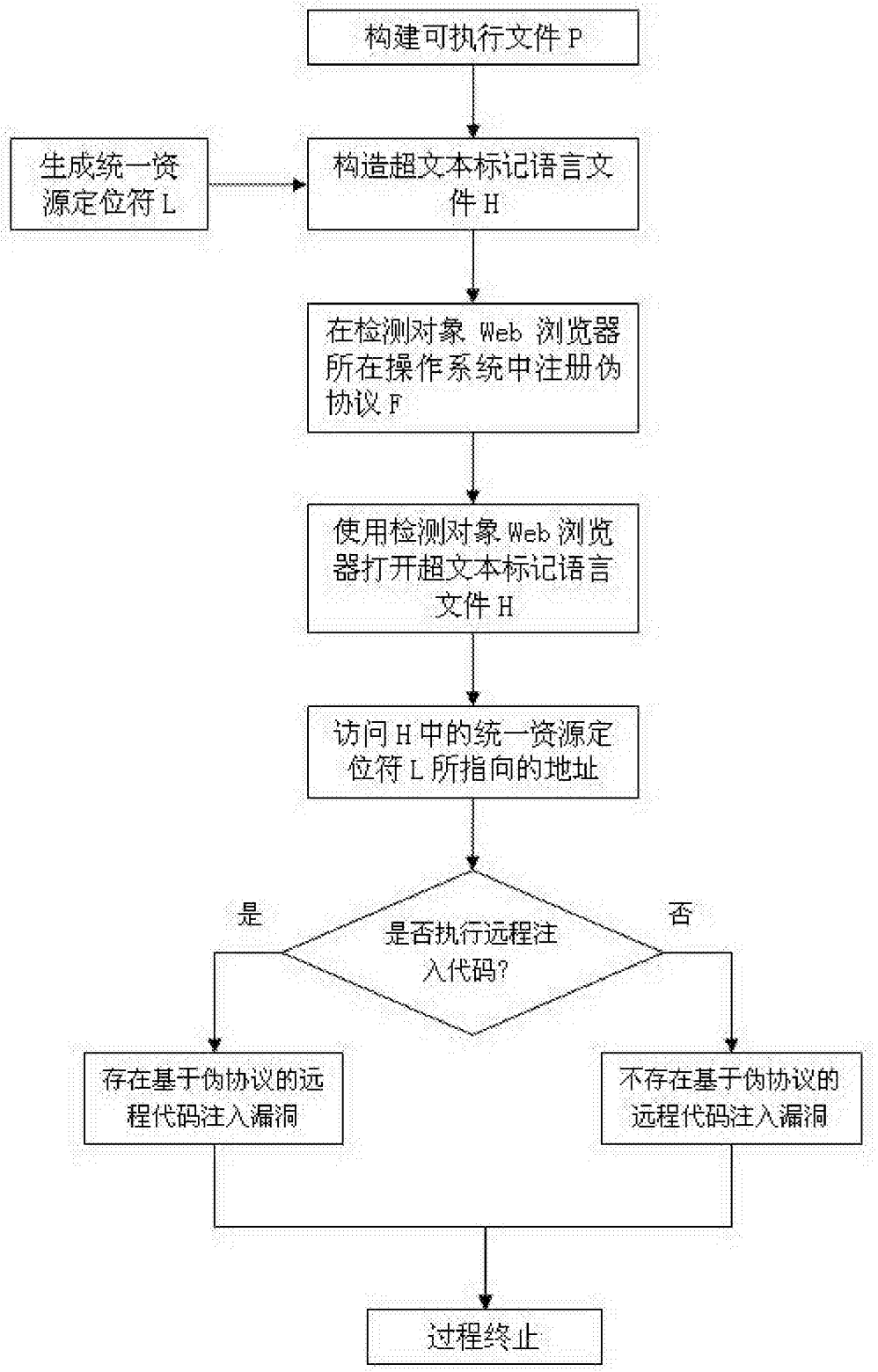

构建可执行文件 P
生成统一资源定位符 L
构造超文本标记语言文件 H
在检测对象 Web 浏览器所在操作系统中注册伪协议 F
使用检测对象 Web 浏览器打开超文本标记语言文件 H
访问 H 中的统一资源定位符 L 所指向的地址
是否执行远程注入代码?
是
否
存在基于伪协议的远程代码注入漏洞
不存在基于伪协议的远程代码注入漏洞
过程终止

图1