中国科学院研究生院学报 2011, 28(5) 668-675 DOI: ISSN: CN:



论文

# 一种基于行为的XSS客户端防范方法

**王夏莉, 张玉清**

中国科学院研究生院国家计算机网络入侵防范中心, 北京 100049

**摘要:**

跨站脚本(XSS)漏洞是Web安全的最大威胁之一.目前XSS防范方法主要为在服务端对用户输入进行过滤.这种方法漏报率较高,且不能及时保护互联网用户.通过对XSS攻击行为,尤其是XSS蠕虫的传播行为进行深入分析,设计并实现了一套新的基于行为的客户端XSS防范方案StopXSS.通过实验及与现有常用客户端XSS防范方案比较,证明其具有对XSS攻击,甚至对0-Day XSS蠕虫的防范能力.

**关键词:** Web安全 JavaScript 跨站脚本 XSS蠕虫

## A behavior-based client defense scheme against XSS

WANG Xia-Li, ZHANG Yu-Qing

National Computer Network Intrusion Protection Center, Graduate University, Chinese Academy of Sciences, Beijing 100049, China

Abstract:

Recent popularity of Web 2.0 application has given rise to a large number of Web vulnerabilities, and XSS vulnerability is among the top security threats. In recent years, the occurrence of XSS worms worsened the situation of Web security. Existing XSS defense methods mainly depend on filtering users' inputs on the server side, which cannot protect in time the main victims of XSS attacks, the Internet users. In this paper we focus on the analysis of XSS behavior, especially the propagation behavior of XSS worms, and propose a new client-side XSS defense method, StopXSS. The testing experiments show that our method can defend against XSS attacks effectively and can be used to detect even 0-Day XSS worms.

Keywords: Web security JavaScript cross site scripting (XSS) XSS worm

**收稿日期** 2010-09-07 **修回日期** 2010-11-07 **网络版发布日期**

DOI:

**基金项目**:

国家自然科学基金(60773135, 90718007, 60970140)资助

**通讯作者**:

**作者简介**:

**作者**Email: wangxl@nipc.org.cn

**参考文献:**

[1] Wichers D. The top 10 most critical web application security risks . The Open Web Application Security Project (OWASP), 2010.

[2] Kirda E, Vigna G, Jovanovic N. Noxes: a client-side solution for mitigating cross-site scripting attacks //The 21st Annual ACM Symposium on Applied Computing. New York, USA: ACM, 2006: 330-337.

[3] Kirda E, Kruegel C, Virgac G. Client-side cross-site scripting protection [J]. Computers and Security, 2009, 28(7): 592-604.

[4] Livshits B, Cui W. Spectator: detection and containment of JavaScript worms //USENIX 2008 Annual Technical Conference on Annual Technical Conference. Boston, USA: ACM, 2008: 335-348.

[5] Sun F, Xu L, Su Z. Client-side detection of XSS worms by monitoring payload propagation //Proceedings of the 14th European Conference on Research in Computer Security. Saint-Malo, France: ACM, 2009: 539-554.

[6] Fogie S, Hansen R, Rager A, et al. XSS attacks: cross site scripting exploits and defense [M]. New York: Syngress Media, 2007.

[7] Garcia J, Navarro G. A survey on cross-site scripting attacks: USA, abs/0905.4850 . (2009-05-29) http://arxiv.org/pdf/0905.4850v1.

[8] Faghani M, Saidi H. Social networks' XSS worms //International Conference on Computational Science and Engineering. Vancouver, Canada: IEEE Computer Society, 2009: 1137-1141.

[9] Dabirsiaghi A. Building and stopping next generation XSS worms //3rd International OWASP Symposium on Web Application Security. Ghent, Belguim, 2008.

[10] Network Working Group. HTTP methods: USA, internet RFC 2616 . (2004-09-01) http://www.w3.org/Protocols/rfc2616/rfc2616.html.

[11] Oda T, Oorschot P, Somayaji A. SOMA: mutual approval for included content in web pages [J]. ACM Computer and Communications Security, 2008:89-98.

[12] Vogt P. Cross site scripting (XSS) attack prevention with dynamic data tainting on the client side . Vienna: Technical University of Vienna, 2006.