PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

MOHAMED BOUDIAF UNIVERSITY - M'SILA
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE

COMPUTER SCIENCE DEPARTMENT

Thesis submitted in partial fulfillment of the requirements for the Degree of MASTER

Domain: Mathematics and Computer Science
Branch : Computer Science
Specialty : Networks

By: BOULANOUAR SOUHIL LARBI

TOPIC

Optimized XSS Vulnerability Scanner Approach

Publicly defended : / /2016 before a Jury composed of :

Ms SAOUDI LALIA	**University of M'sila**	**Supervisor**
A.MOUSSAOUI	**University of M'sila**	**Examiner**
Y.ARIOUET	**University of M'sila**	**Examiner**

Academic Year : 2015 /2016

Contents

General introduction

1 Context of the study

Web applications are becoming more popular and widely being used in all aspects of work and social activities.

Now web applications are the dominant method for implementing and providing access to on-line services and becoming truly pervasive in all kinds of business models and organizations.

Today, most systems such as Social Networks, health care, banking, or even emergency response are relying on these applications.

However, the exponential development of web technologies comes at a price, because the number of Web application security issues increases rapidly as well and Web applications are becoming more prone to worrisome vulnerabilities.

Cross-site scripting (XSS) attack considered as one of the top 10 web application vulnerabilities of 2013 by the Open Web Application Security Project (OWASP) [13]. According Cenzic Application Vulnerability Trends Report (2013) Cross Site Scripting represents 26% of the total population respectively [42] and considers as top most first attack.

Cross Site Scripting attack carried out using HTML, JavaScript, VBScript, ActiveX, Flash, and other client-side languages. A weak input validation on the web application leads Cross Site Scripting attacks to gather data from account hijacking, changing of user settings, cookie theft.

2 Statement of the Problem

The Detection of XSS is a topic of active research in the industry and academia. To achieve those purposes, automatic scanners have been implemented.

XSS Vulnerability scanner is a tool that detects the XSS vulnerabilities in web applications, generally, there are two types of vulnerability scanners:

White Box scanner: provides the penetration testers with the knowledge of implementation details (e.g. the internal structure of the program).From this information; test cases are created according to the coverage criteria [27].

Tools taking white-box approaches suffer from the following shortcomings:

- Sometimes source code is not available.

- Different programming languages are used for building Web applications.

Black-box scanner: Black-box means that the implementation details are not examined by the tester. According to inputs, outputs are verified with expected (predefined) behavior. Since code details are unknown, black-box testers should identify as many inputs as possible [28], to help him to detect as many vulnerabilities as possible, for this reason the XSS attack vector of input may have a large number.

By using a large-number of attack vector , XSS vulnerability detection may cost too much time, and the result may have a high false positive.

3 Objectives

In order to solve the above problem of black box scanner with large number of attack vector, we propose an approach to implement an efficient XSS scanner which aims to optimize its XSS attack vector in order to reduce the scan time and maximize the detected vulnerabilities point. Our work makes the following contributions:

- A method for generating and optimizing XSS vector attack: we propose a grammar to dynamic generation of all possible XSS scripts but we select the most promising ones.
- A method for detecting stored XSS; we search for each not searchable form (entry point for stored XSS injection) its related searchable form (entry point for stored XSS detection) , this link help us to go directly to the page in which the stored XSS code will be executed.

4 Report Outline

This report divided in four chapters:

The first chapter provides the basic concepts of Web Applications and Web Security , we present the top 10 OWASP web vulnerabilities, we focus on the Cross-Site Scripting(XSS)

The second chapter provides a general overview of Web Security Testing and different approaches of web scanners implementation, then we present the most popular web scanners.

The third chapter presents the conceptual design of our scanner with its different modules and methods for generating and optimizing XSS vector attack ,and for detecting stored XSS.

In the fourth chapter we will present the implemented XSS scanner, and discuss the results obtained from running the scanner, to demonstrate the effectiveness of the method proposed in this work.

Finally, we conclude this project by a general conclusion and perspectives.

General conclusion

Current-day scanner of XSS vulnerability are used to detect most of the vulnerabilities (Reflected or Stored XSS). However, none of them are complete or accurate enough to guarantee an absolute level of security on web application.

In this project, we developed our scanner of XSS vulnerability, which have three basic phases :

- Crawling phase : for collect and save the information from the Web application.
- Injection phase : for simulating XSS attacks based on the injection codes generated by the Code Generator and the user data entry points collected in the Crawling Phase
- Detection phase: for detecting failures resulting from the Injection phase (detection of vulnerabilities)

Time and number of vulnerabilities detected are the most factors to evaluate the Success of scanners, for this reason ,We proposed a method to optimize the detection of stored XSS vulnerabilities, and other method for generating and optimizing XSS vector attack.

In the experimentation phase we choose three of the most popular scanners used to conduct a comparative study with our approach. The OWASP ZAP scanner , Acunetix Web Vulnerability (IBM), and Vega Vulnerability Scanner .
we choose three websites for testing: Damn Vulnerable Web App (DVWA), testphp.vulnweb.com ,and template site.

The results prove the effectiveness of our scanner in identification of vulnerabilities and reduce the time of scan.

Perspective: detection of DOM vulnerabilities

Bibliography

[1] *Nations, Daniel.* "Web Applications". *About.com. Retrieved 20 January 2014.*

[2] OWASP. A Guide to Building Secure Web Applications. The Open Web Application Security Project, 2005.

[3] Fielding, Roy T.; Gettys, James; Mogul, Jeffrey C.; Nielsen, Henrik Frystyk; Masinter, Larry; Leach, Paul J.; Berners-Lee, Tim (June 1999). Hypertext Transfer Protocol -- HTTP/1.1. IETF. RFC 2616.

[4] Berners-Lee, Tim; Fielding, Roy T.; Nielsen, Henrik Frystyk. "Method Definitions".Hypertext Transfer Protocol -- HTTP/1.0. IETF. pp. 30-32. sec. 8. RFC 1945.

[5] Fielding, Roy T.; Gettys, James; Mogul, Jeffrey C.; Nielsen, Henrik Frystyk; Masinter, Larry; Leach, Paul J.; Berners-Lee, Tim (June 1999). *Hypertext Transfer Protocol -- HTTP/1.1.* IETF. RFC 2616 "Method Definitions". pp. 51-57. sec. 9.

[6] Fielding, Roy T.; Gettys, James; Mogul, Jeffrey C.; Nielsen, Henrik Frystyk; Masinter, Larry; Leach, Paul J.; Berners-Lee, Tim (June 1999). *Hypertext Transfer Protocol -- HTTP/1.1.* IETF. RFC 2616."POST". p. 54. sec. 9.5.

[7]. "http tutorial",[Online]. Available: http://www.tutorialspoint.com/http/http_pdf_version.htm Visited : 07/04/2016.

[8] Programming notes , HTTP (HyperText Transfer Protocol), https://www.ntu.edu.sg/home/ehchua/programming/webprogramming/HTTP_Basics.html ., Visited : 07/04/2016 .

[9] XSS Attacks: Cross Site Scripting Exploits and Defense 1st Edition by Seth Fogie (Author), Jeremiah Grossman (Author), Robert Hansen (Author), Anton Rager (Author), Petko D. Petkov (Author) .

[10] Marcel Dekker. Security of the Internet, 1997.

[11] Chris Joscelyne. Information Management, 2005.

[12] Claudia Eckert. IT-Sicherheit. Oldenbourg–Verlag, second edition, 2003.

[13] https://www.owasp.org/index.php/Top_10_2013-Top_10. , Visited : 15/04/2016 .

[14] https://www.owasp.org/index.php/Cross-site_Scripting_(XSS) , Visited : 12/04/2016 .

[15] http://www.acunetix.com/blog/articles/preventing-xss-attacks , Visited : 14/04/2016 .

[16] https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_ Cheat_Sheet ,Visited : 14/04/2016 .

[17] Gunter Ollmann. HTML Code Injection and Cross-Site Scripting. http: //www.technicalinfo.net/papers/CSS.html, Visited : 10/042016 .

[18] CERT Coordination Center. Understanding Malicious Content Mitigation for Web Developers. http://www.cert.org/tech tips/malicious code ,Visited : 10/042016 .

[19] Web application vulnerability scanner US 8365290 B2 ,Frederick Young ,18 11 2010.

[20] https://msdn.microsoft.com/en-us/library/cc751383.aspx ,Visited 20/04/2016.

[21] Edsger W. Dijkstra. Structured Programming. Software Engineering Techniques,1990.

[22] Glenford J. Myers. The Art of Software Testing. Wiley, 1979.

[23] Glenford J. Myers. Software Reliability. Wiley, 1976.

[24] Bill Hetzel. The Complete Guide to Software Testing. QED Information Sciences,second edition, 1988.

[25] AD Brucker, T Deuster - US Patent 8,881,293, 2014.

[26] https://cmsreport.com/articles/web-application-security-testing-sast-dast-or-iast--13728 ,Visited : 21/04/2016

[27] Bill Hetzel.. QED Information Sciences, second edition, 1988.

[28] Black Box Security Testing Tools C.C. Michael, Ken van Wyk, and Will Radosevich July 31, 2013 .

[29] https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools 2016 , Visited: 23/04/2016

[30] http://wapiti.sourceforge.net/ , Visited: 23/04/2016

[31] http://w3af.org/howtos/understanding-the-basics , Visited: 23/04/2016

[32] https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project ,Visited: 23/04/2016 .

[33] http://www.acunetix.com/company/ ,Visited : 23/04/2016.

[34] https://subgraph.com/vega/ Visited : 23/04/2016 .

[35] https://jsoup.org 2016 , Visited : 06/05/2016.

[36] https://usa.kaspersky.com/internet-security-center/definitions/malicious-code#. VynIWYQrLIU ,Visited : 07/05/2016.

[37] https://netbeans.org/about/ ,Visited : 10/05/2016

[38] https://jsoup.org/ ,Visited : 10/05/2016

[39] http://htmlunit.sourceforge.net/ ,Visited : 10/05/2016

[40] http://www.mysql.com/about/ ,Visited : 10/05/2016

[41] http://www.dvwa.co.uk/ ,Visited : 27/04/2016.

[42] H. Chen and M. V. Gundy, "Using randomization to enforce information flow tracking

and thwart cross site scripting attacks," In Proceedings of the 16th Annual Network and Distributed System Security Symposium (NDSS), (2009).

[43] Y. W Huang, F. Yu, C. Hang, C. H. Tsai, D. Lee and S. Y. Kuo, "Verifying Web Application using Bounded Model Checking," In Proceedings of the International Conference on Dependable Systems and Networks, (2004).

[44]: G. Wassermann, and Z. Su, "Static detection of cross-site scripting vulnerabilities," Proceedings of the 30th international conference onSoftware engineering (ICSE '08), New York, USA, pp. 171-780, 2008.

[45]: N. Jovanovic, C. Kruegel, and E. Kirda, "Precise alias analysis for static detection of web application vulnerabilities," Proceedings of the 2006 workshop on Programming languages and analysis for security (PLAS '06), New York, USA, pp. 27-36, 2006.

[46]: Y. Wang, Z. Guo, "Program slicing stored XSS bugs in web application," Proceedings of the Fifth IEEE International Conference on Theoretical Aspects of Software Engineering, pp. 191-194, 2011.

[47] G. Wassermann, Z. Su. Static Detection of Cross-Site Scripting Vulnerabilities. ICSE'08, May 10–18, 2008, Leipzig, Germany.

[48] T. Jim, N. Swamy and M. Hicks, "BEEP: Browser-Enforced Embedded Policies," In Proceedings of the 16th International World Wide Web Conference, ACM, (2007), pp. 601-610.

[49] P. Bisht and V. N. Venkatakrishnan, "XSS-GUARD: Precise dynamic prevention of Cross-Site Scripting Attacks," In Proceeding of 5th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, LNCS, vol. 5137, (2008), pp. 23-43.

[50] Z. Su and G. Wassermann, "The essence of command Injection Attacks in Web Applications," In Proceeding of the 33rd Annual Symposium on Principles of Programming Languages, USA: ACM, (2006) January, pp. 372-382.

[51] D. Balzarotti, M. Cova, V. V. Felmetsger and G. Vigna, "Multi-Module Vulnerability Analysis of Webbased Applications," In proceeding of 14th ACM Conference on Computer and Communications Security,Alexandria, Virginia, USA, (2007) October.

[52] T. Pietraszek and C. V. Berghe, "Defending against Injection Attacks through Context-Sensitive String Evaluation", In Proceeding of the 8th International Symposium on Recent Advance in Intrusion Detection (RAID), (2005) September.

[53] Z. Su and G. Wassermann, "The essence of command Injection Attacks in Web Applications," In Proceeding of the 33rd Annual Symposium on Principles of Programming Languages, USA: ACM, (2006).

[54] D. Scott, and R. Sharp, —Abstracting Application-Level Web Security, In Proceeding 11thinternational World Wide Web Conference, Honolulu, Hawaii: 2002, pp. 396-407

[55] Xiaobing Guo, Shuyuan Jin, and Yaxing Zhang Institute of Computing Technology, Chinese Academy of Sciences Beijing, China XSS Vulnerability Detection Using Optimized Attack Vector Repertory 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery .

[56] Fabien Duchene ,Sanjay Rawat_IIIT Hyderabad, India, Jean-Luc Richier, Roland Groz LIG Lab Grenoble F-38402, France KameleonFuzz:Evolutionary Fuzzing for Black-Box XSS Detection March 2014

[57] Fabien Duchene ,Sanjay Rawat_IIIT Hyderabad, India, Jean-Luc Richier, Roland Groz LIG Lab Grenoble F-38402, France KameleonFuzz:Evolutionary Fuzzing for Black-Box XSS Detection March 2014

[58] Fabien Duchene, Roland Groz, Sanjay Rawat, Jean-Luc Richier. XSS Vulnerability Detection Using Model Inference Assisted Evolutionary Fuzzing. SECTEST 2012 - 3rd International Workshop on Security Testing (a_liated with ICST), Apr 2012, Montreal, Canada. IEEE Computer Society, pp.815-817, 2012, <10.1109/ICST.2012.181>. <hal-00857294>

[59] D. Balzarotti, M. Cova, V. V. Felmetsger and G. Vigna, "Multi-Module Vulnerability Analysis of Webbased Applications," In proceeding of 14th ACM Conference on Computer and Communications Security, Alexandria, Virginia, USA, (2007) October.

[60] Y. Xie and A. Aiken, "Static detection of security vulnerabilities in scripting languages," Stanford University Stanford, CA 94305.

[61]: N. Jovanovic, C. Kruegel and E. Kirda, "Pixy: A static analysis tool for detecting web application vulnerabilities (short paper)," In 2006 IEEE Symposium on Security and Privacy, Oakland, CA, (2006) May .

الملخص

أصبحت تطبيقات الويب أكثر شعبية مع تقدم التكنولوجيا ، ومع ذلك، أمن الواب أصبح واحد من القضايا الأمنية الأكثر شيوعا.

تركز هذا المذكرة على ثغرة XSS الموجودة عادة في معظم تطبيقات الويب و يمكن أن تخلق مشاكل أمنية خطيرة.

في عملنا ، نقترح نهج للكشف عن الثغرات باستعمال الصندوق الأسود و جدول الهجوم الأمثل ،هذه الطريقة تولد جدول الهجوم تلقائيا ، و تحسنه باستخدام نموذج التبديل ،لتكشف عن ثغرات XSS الموجودة في تطبيقات الويب ديناميكيا .

❖ **الكلمات المفتاحية :** كشف ثغرات XSS ، تحسين جدول الهجوم ,ماسح الصندوق الاسود ، ، ماسح ثغرة XSS.

Summary

The Web applications are becoming more popular with the advancement of technology. However, the web security is becoming one of the most common security issues.

This report focuses on the XSS vulnerabilities which commonly present in most Web applications and can create serious security problems.

In our work, we propose a black box detection approach using optimal attack vector. This method generates an attack vector automatically, optimizes the attack vector repertory using a mutation operator model, and detects XSS vulnerabilities in web applications dynamically.

❖ **Keywords**: XSS vulnerability detection, attack vector optimization, black box scanner, XSS vulnerability scanner.

Résumé

L'avancement de la technologie web prépare la voie à la popularité des applications Web, Cependant, la sécurité de Web est devenu l'un des problèmes de sécurité les plus courants.

Ce mémoire porte sur les vulnérabilités XSS qui sont généralement présentent dans la plupart des applications Web et peuvent créer des problèmes de sécurité graves.

Dans notre travail, nous proposons une approche de détection de boîte noire utilisant le vecteur d'attaque optimale. Cette méthode génère automatiquement un vecteur d'attaque, puis l'optimise à l'aide d'un modèle basé sur la mutation, puis détecte dynamiquement les vulnérabilités XSS dans les applications web.

❖ **Mots-clés :** détection de vulnérabilité XSS, optimisation du vecteur d'attaque, scanner boîte noire, scanner de vulnérabilité XSS.