JAAM: Web Browser Security Framework

Deepak Singh Tomar deepaktomar@manit.ac.in
Jishan Shaikh jishashaikh9893*
Ankit Chouhan ankitchoudhan.dws97*
Ankit Chaudhary ankitchaudhary9838*
Mansoor Sediqi sedeqym*

***Abstract*—This paper presents a novel framework for web browser security. It will help organizations assess, evaluate, formulate, and implement a strategy for their web browser security concerns. It is quite adaptive to large scale organizations, also flexible to small and medium scale organizations. Major features of the framework includes easy customization, neutrality towards life-cycle models, open-source, and standardization of security practices. Core framework is based on four major components: Design sub-components, Tools and Applications, Code and Utilities, and Miscellaneous sub-components. Major design sub-components are Web Browser Security Assurance and Maturity Model (WBSAMM), Security Architecture, Testing guides, Verification standards, and Vulnerability query language (VQL). WBSAMM is based on modern security practices, business functions, and multiple maturity levels. Quantitative dependency of other parameters is also analyzed. Code utilities includes sanitizer sub-component for web browser languages such as HTML, JavaScript, XML, Python. Coding standards are also proposed under Code and Utilities component.**

A malicious URL detection tool is also developed as a part of tools and application component using data mining of 420K+ URLs giving an accuracy rate of 99.3%. Miscellaneous component includes review and analysis of various security aspects e.g. Browser forensics, Test suites (Static, Dynamic, and Runtime), Risk assessment methods, Threat modeling, Social and Reverse Engineering, Proxy and VPN, Attack tensors, Flash and JavaScript, Global Vulnerability Repository. Comparison of modern web browsers (Google Chromium, Mozilla Firefox, Tor) is presented on basis of abstract features, standards, and protocols.

***Index Terms*—Web Browsers, Security, Framework, JAAM**

I. Introduction

Open Web Application Security Project (OWASP) has presented Software Assurance Maturity Model (SAMM) for general software based on 3 maturity levels. WBSAMM is improved version of SAMM specially designed for web browsers.

II. Related Work and Research gap

Open Web Application Security Project (OWASP) has presented Software Assurance Maturity Model (SAMM) for general software based on 3 maturity levels. Software Engineering Institute has proposed Software Capability and Maturity Model based on 5 maturity levels. JAAM is web browser specialization of OWASP's SAMM in some aspects. Related work on Browser security presented as white paper by [1] and [2]. Gaps in providing secure browser and research in data breaches is presented in [3]. A rich encyclopedia of XSS attacks is [4]. Various methods of gaining/revoking control, bypassing same origin policy, and attacking through various vectors are presented in [5]. [5] is therefore considered as standard reference for web browser hackers.

III. JAAM: Web Browser Security Framework

A. Design components

B. Tools and Applications components

C. Code and Utilities components

D. Miscellaneous components

IV. Conclusions and Future Work

The component nature of framework allows inclusion of new sub-components to framework in either of four major components.

Acknowledgment

Authors are thankful to their supervisor Dr. Deepak Singh Tomar, Reviewers and Project co-ordinators Dr. Sanyam Shukla and Dr. Rajesh Wadhwani, Head of the department, CSE MANIT Bhopal Dr. Meenu Chawla, Director of MANIT Bhopal Dr. Narendra Raghuwanshi. Authors also appreciates all persons/organizations who contributed directly/indirectly to this project. This project is not funded by any agency.

References

[1] M. Vervier, M. Orrù, B. J. Wever, E. Sesterhenn, "Browser Security White Paper," X41 D-SEC GmbH, Dennewartstr. 25-27 D-52068 Aachen Amtsgericht Aachen: HRB19989, September 2017.

[2] I. M. Heiderich, A. Inführ, F. Fabler, N. Krein, M. Kinugawa, T. C. Hong, D. Weiber, P. Pustulka, "Cure53 Browser Security White Paper," Bielefelder Str. 14, D 10709, Berlin, cure53.de, November 2017.

[3] S. Donaldson, A. Florescu, K. Roemer, M. Zugec. Secure Browsing, Citrix XenApp, Citrix XenServer, Direct Inspect APIs, Bitdefender HVI. Joint white paper, 2016.

[4] J. Grossman, R. Hansen, P. D. Petkov, A. Rager, S. Fogie, "XSS Attacks: Cross Site Scripting Exploits and Defense," Syngress publishing, USA, 2007, ISBN-13: 978-1-59749-154-9.

[5] W. Alcorn, C. Frichot, M. Orrù, "The Browser Hacker's Handbook", Wiley publishing, USA, ISBN: 978-1-118-66209-0 ISBN: 978-1-118-66210-6 (ebk), 2014.

NOTE: This paper is an output of minor project entitled same in Security Lab, MANIT Bhopal by authors under supervision of Dr. Deepak Singh Tomar. *** indicates @gmail.com**