Conceptual foundation for an automated pentester based on a single board computer

Fundamento conceptual para un pentester automatizado con una base en el computador de placa única

Fundamento conceitual para executar pentester automatizado com base em um computador de placa única

Geraldín Vergara Fajardo[1]
Diana Marcela Montaño[2]
Siler Amador Donado[3]
Katerine Márceles Villalba[4]

Received: January 5th, 2018
Accepted: March 28th, 2019
Available: May 21th, 2019

How to cite this article:
G. Vergara-Fajardo, D. M. Montaño, S. Amador-Donado, K. Márceles-Villalba, "Conceptual foundation for an automated pentester based on a single board computer", *Revista Ingeniería Solidaria*, vol. 15, n.° 2, 2019.
DOI: https://doi.org/10.16925/2357-6014.2019.02.08

Research article. https://doi.org/10.16925/2357-6014.2019.02.08

[1] Facultad de Ingeniería. Institución Universitaria Colegio Mayor del Cauca. Popayán, Colombia
ORCID: https://orcid.org/0000-0001-5333-2154

[2] Facultad de Ingeniería. Institución Universitaria Colegio Mayor del Cauca. Popayán, Colombia
ORCID: https://orcid.org/0000-0002-0817-5978

[3] Facultad de Ingeniería. Universidad del Cauca. Popayán, Colombia
ORCID: https://orcid.org/0000-0002-4571-8273
Email: samador@unicauca.edu.co

[4] Facultad de Ingeniería. Institución Universitaria Colegio Mayor del Cauca. Popayán, Colombia
ORCID: https://orcid.org/0000-0002-4571-0714
Email: kmarceles@unimayor.edu.co

Abstract

Introduction: This article is the product of the research entitled "Automated Concept Tests on Web Applications Based on OWASP", carried out during 2017 and 2018 in the city of Popayan, capital of the Department of Cauca.

Problem: Establish and identify a theoretical support for the research topic that will help to solve the problem question of the research work. Is it necessary to develop scripts that automate the concept testing process for the detection of vulnerabilities corresponding to the Top 10 of OWASP 2017.

Objective: Propose a conceptual and background component, through the study of primary and secondary sources along with inclusion and exclusion factors, which helps determine the relevance to the proposed problem which in turn will assist in the construction of a solution.

Methodology: The methodology used was documentary, so several sources of databases were consulted, in order to determine the conceptual, theoretical and relevant background information that will support this research work.

Results: As a result, a very significant analysis was obtained, given that it was possible to obtain relevant conceptual bases that contributed to the solution of the problem.

Conclusion: Despite the existence of tools designed to perform web pentesting, none solve the problems posed in this article, however, the articles did contribute towards the solution of the objective.

Originality: Automation of the pentesting process, under the OWASP methodology, in an SBC, using free software, to reduce costs to entrepreneurs when testing the security of web applications.

Limitations: Access to databases in the institution, time and money used to perform tests on other SBC devices.

Keywords: OWASP, Pentesting, Security, SBC (Single Board Computer), Scripts.

Resumen

Introducción: Este artículo es producto del trabajo de investigación "Pruebas de Concepto Automatizado sobre Aplicaciones Web Basados en OWASP", realizado durante el 2017 y 2018 en la ciudad de Popayán, capital del departamento del Cauca.

Problema: Establecer e identificar un soporte teórico del tema de investigación que ayudará a resolver la pregunta problema del trabajo investigativo, ¿Es necesario desarrollar scripts que automaticen el proceso de pruebas de concepto para la detección de vulnerabilidades correspondientes al Top 10 de OWASP 2017?

Objetivo: Proponer un componente conceptual y de antecedentes, a través del estudio de fuentes primarias, secundarias, factores de inclusión y exclusión, que permitan determinar la relevancia a la problemática propuesta, para llegar a la construcción de una solución.

Metodología: La metodología empleada fue documental, por lo que se consultaron varias fuentes de bases de datos, para poder determinar las bases conceptuales, teóricas y de antecedentes pertinentes que soportarán este trabajo de investigación.

Resultados: Como resultado se obtuvo un análisis significativo, se logró obtener bases conceptuales pertinentes que permitieron aportar a la solución del problema.

Conclusión: A pesar de la existencia de herramientas para realizar pentesting web, ninguna resuelve totalmente la problemática planteada en este artículo, no obstante, los artículos encontrados ayudaron en la solución del objetivo.

Originalidad: Automatización del proceso de pentesting, bajo la metodología OWASP, en un SBC, utilizando software libre, para disminuir costos a empresarios al momento de probar la seguridad de aplicaciones web.

Limitaciones: El acceso a las bases de datos en la institución, el tiempo y dinero empleado para realizar pruebas en otros dispositivos SBC.

Palabras clave: OWASP, Pentesting, Security, SBC (Single Board Computer), Scripts.

Resumo

Introdução: este artigo é produto do trabalho de pesquisa "Testes de Conceito Automatizado sobre Aplicações Web baseados em OWASP", realizado durante 2017 e 2018 em Popayán, capital do estado do Cauca, Colômbia.

Problema: estabelecer e identificar um suporte teórico do tema de pesquisa que ajudará a resolver a pergunta problema da pesquisa: é necessário desenvolver scripts que automatizem o processo de testes de conceito para a detecção de vulnerabilidades correspondentes ao Top 10 de OWASP 2017?

Objetivo: propor um componente conceitual e de antecedentes, por meio do estudo de fontes primárias, secundárias, fatores de inclusão e exclusão que permitam determinar a relevância da problemática proposta, para chegar à construção de uma solução.

Metodologia: a metodologia utilizada foi documental, portanto foram consultadas diversas fontes de bases de dados para determinar as bases conceituais, teóricas e de antecedentes pertinentes que apoiarão este trabalho de pesquisa.

Resultados: obteve-se uma análise significativa; conseguiu-se obter bases conceituais pertinentes que permitiram contribuir para solucionar o problema.

Conclusão: apesar da existência de ferramentas para realizar *pentesting web*, nenhuma resolve totalmente a problemática proposta neste artigo; contudo, os artigos encontrados ajudaram na solução do objetivo.

Originalidade: automatização do processo de *pentesting*, sob a metodologia OWASP, num SBC, utilizando *software* livre, para diminuir custos a empresários no momento de testar a segurança de aplicações web.

Limitações: o acesso a bases de dados na instituição, o tempo e a verba empregados para realizar testes em outros dispositivos SBC.

Palavras-chave: OWASP, *pentesting*, segurança, Computador de Placa Única (SBC —Single Board Computer), scripts.

1. Introduction

Currently one of the biggest problems of websites worldwide has been the security of information, therefore, when there are different tools for the analysis of concept tests —which find vulnerabilities in Web sites, there are methodologies in the area of computer security where you can make not only the analysis but also a study of both technical risks and about business, due to website vulnerabilities. All of these aim to find potential solutions and improvements at sites to minimize the risks posed and to avoid the possible threats and attacks by external agents.

Today there are applications dedicated to the detection of vulnerabilities on websites, which are included in a Linux distribution Back Track, called Kali Linux [1][1], used to perform security audits and penetration tests. More than 300 tools are available for it; some of these are: Nmap, Zenmap, Nping, Sparta, sqlmap, Wireshark,

1 Available: http://www.kali.org

Nikto, Burpsuite, Owasp-zap, among others, but in some cases not all the necessary information is provided and therefore this doubles the work involved when trying to find vulnerabilities manually. This has generated the need to automate this process to minimize the risk of this problem, using the methodology OWASP 2017 [2], tackling the top 10 most important risks on websites and producing a guide where it explains how to check if there are vulnerabilities in web applications. The project also provides its own innovative touch by using low-cost computers to reduce the project budget.

All this begs the question: Is it necessary to develop scripts that automate the process of concept tests for the detection of vulnerabilities related to the OWASP Top 10 of 2017 .

Given the above, in order to answer the question, a literature review based on the methodology of Pino authors Piattini & Travassos [3] was used**,** to evaluate the available research that can support the answer to the question posed.

2. Assessment of literature relevant to the ESTS concept in web applications by OWASP

All reference material should be based on data sources that are up-to-date, reliable, and that support progress related to research, so it was important to conduct a literature review that would acquire as much updated information about SBC devices or pentesting tools, or vulnerabilities related primarily to the OWASP Top 10. The process used to carry out the literature review that served as support for the solution of the question problem is described below.

2.1 Database and search terms

Databases today are within reach of many, and thus should use clear search topics in order to obtain better results. In this case it is required that the foundations are focused to a bibliographic database that allows searching the web for information in articles in major scientific journals, all related to computer security.

Below are listed some of the following databases:

- ScienceDirect
- Scopus
- IEEE
- EBSCO

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

According to the required characteristics and evaluating the amount of information which can be accessed, ScienceDirect it is multidisciplinary group belonging to Elsevier[2] available to many, including students.

For the collection of information keywords should be identified that will provide better search results. Then the words obtained should be relevant to the answer given to the question posed in the introduction of the article, where it says, "Do you need to develop scripts that automate the process of concept tests for the detection of corresponding vulnerabilities OWASP Top 10 2017?"

"Low cost computer", "single board computer", "vulnerability", "testing guide", "penetration testing", "pentesting web application", "security", "risk", "web applications", "computer attacks", " testing tools "," vulnerability detection tools, " vulnerability scanning tools "," pentesting vulnerability "," web vulnerability detection "," OWASP. "

Once the keywords are defined, which define the search strings, the way in which they can be related by combinations of logical connectors should be considered; like AND and OR, for the next 3 chains.

The first string is related to the identification of a low-cost SBC in order to find the greatest amount of information that serves to highlight the most suitable for the development of a proof of concept. In the second chain the aim is to find the most tools that involve both scanning and detection of vulnerabilities so as to define which of the known vulnerabilities (according to OWASP) can be identified. And the third string should be dedicated to looking for information about the OWASP TOP 10 on security risks in web applications that organizations face.

Table 1. Search Strings

	Search strings
1	("Single board computer") AND ("low cost computer")
2	("Testing tools" OR "vulnerability detection tools" OR "vulnerability scanning tools" OR "web vulnerability detection" OR "penetration testing" OR "pentesting web application")
3	("OWASP") AND ("testing guide" OR "security risk" OR "web application security" OR "computer attacks" OR "vulnerability" OR "pentesting vulnerability")

Source: own work

2 Elsevier offers digital solutions based on the web. It is a global leader in providing information and analysis for all professions and industry suppliers.

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

3. Selection process

The selection process is divided into six stages as shown in Figure 1:

1. Search databases. Bibliographical sources that are deemed necessary are listed; search strings with keywords and their synonyms are constructed; then the chains are tailored to each search engine's bibliographical sources.
2. Eliminate redundant results. The search results of studies may be redundant, for that reason repeated studies are removed and then each is stored in a bibliographic reference manager.
3. Selection of primary studies. From the items found, the inclusion and exclusion criteria —title, abstract / summary, introductory and concluding remarks if necessary—, which are mentioned in the "Selection Criteria" section to extract primary articles, were applied. Then each primary study is stored.
4. Final selection. Once each primary study is stored, a complete reading of each study is made.
5. Eliminate concerns. If doubts and concerns arise whilst reading the articles, an expert is consulted on the subject to try and resolve the differences.
6. Quality assessment. Based on the quality criteria to be named in the Criteria section of the quality assessment, primary studies are evaluated and classified in order to ensure proper assessment of the primary studies.

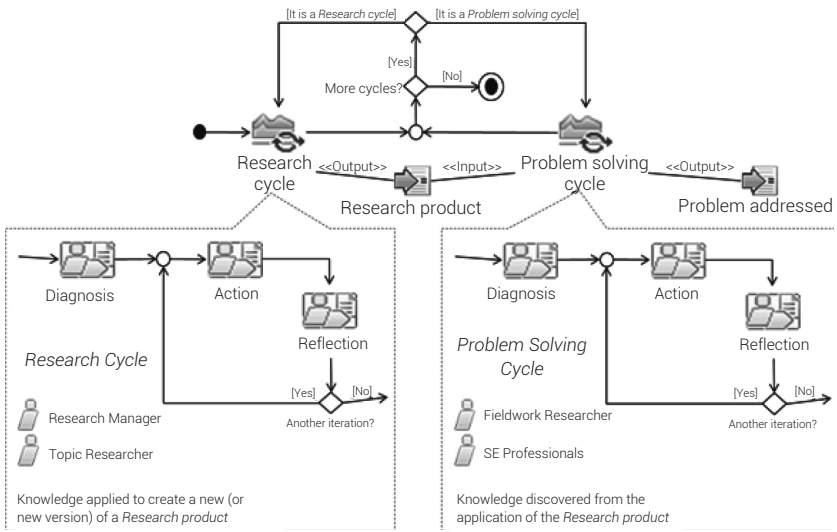

Figure 1. Diagram of the research procees.

Source: Pino, Piattini & Travassos. Management and development of research projects distributed software engineering through action research. Faculty of Engineering magazine.

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

3.1 Selection Criteria

One of the essential activities during the planning phase of this investigation, is the definition of the inclusion criteria and exclusion criteria according to research conducted by [4] in their degree work. The purpose of these criteria is to help researchers, at the time of selecting the appropriate items, and is used to reduce the amount of work that will be analyzed.

For the selection of relevant articles, the inclusion criterion was based on an analysis of title, abstract and keywords of the articles obtained in the search to identify if they are related to the SBC, if they are inexpensive, can provide more information and preparation for developing a proof of concept of web applications, and involve related vulnerabilities submitted to web pages, such as scanning and detection thereof, according to those defined by OWASP [5].

To determine which items were important enough to be considered as primary education, the exclusion criterion were chosen to highlight items of the following nature: display information about the characteristics and applicability of SBC but are not related to computer science or does not provide its functionality, or if the article provides information on proof of concept but not enough information to correctly assess the vulnerabilities which websites may face, or if the study does not show updated data about the most common risks according to the OWASP TOP 10.

3.2 Quality Evaluation Criteria

According to [4], the objective of quality evaluation criteria is to ensure that an appropriate evaluation of each study that was considered primary. Established evaluation criteria are:

- QEC 1. The study presents some useful contribution to at least one of the following: methodology, technique, tool, focus, model, method, strategy or framework?
- QEC 2. The study presents a research method based on the analysis and description of an empirical study, experimental study, proof of concept, theoretical or case study?
- QEC 3. The study mentions and applies the type of contribution raised?
- QEC 4. The study makes an analysis of the results?

For each of the evaluation criteria of quality, the following assessment was applied: S (Y) = 1, P (partially) = 0.5, N (no) = 0. Thus, the overall result for the evaluation of

each study (QEC1 + QEC2 + QEC4 + QEC3) may be as follows: 0, 0.5 and 1 (incomplete) 1.5 and 2 (regular), 2.5 (good), 3 (very good) and 3.5 and 4 (excellent).

To evaluate each primary study, rules to each evaluation criteria were established in order to supplement the qualitative part of the assessment:

- QEC 1. S, the study proposes the use of a new methodology, framework, model, tool or technique; P, the contribution is present but not clearly described; N, contribution cannot be identified or is not set.
- QEC 2. S, the study explicitly mentions that some research method is applied; P, the study presents relevant information but does not specify the method of investigation; N, research method cannot be identified or is not described.
- QEC 3. S, the study presents, in detail, the type of contribution that has been carried out; P, the type of contribution carried out is briefly represented; N, the study did not clearly describe the type of contribution carried out.
- QEC 4. S, the study presents a detailed analysis explaining the results obtained; P, the results are explained briefly; N, the results cannot be identified or are not described.

4. Quality assessment study

According to the results 98 studies were obtained. Upon review, with redundant studies being removed, this number can be considered closer to 84 studies. 34 of these studies remain upon filtering out studies that are considered to contain irrelevant information by reading the title, abstract and keywords applied. Finally, by applying the exclusion criteria, a total of 24 primary studies (Table 2) are obtained.

Table 2. Results of bibliographical sources

Databases	Studies			
	Obtained	**Not repeated**	**Relevant**	**Primary**
ScienceDirect	37	32	14	9
Scopus	31	28	10	7
IEEE Xplore Digital Library	16	14	6	5
EBSCO	14	10	4	3
Total	98	84	34	24

Source: own work

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

Table 3 shows the total result of primary studies after applying the quality assessment. Each study is listed by the ID column, the names of the primary studies are presented in the Name column with their respective year of publication in the year column. The QEC (Quality Evaluation Criteria) Columns correspond to the score of the evaluation criteria. The Quantitative and Qualitative columns show the final result of each criterion.

Table 3. Each primary study results regarding the quality evaluation criteria

ID	Study name	Year of publication	QEC				Quality	
			1	2	3	4	Quantitative	Qualitative
1	A guide to penetration testing [6].	2014	P	S	P	P	2.5	B
2	A Method for Web Application Vulnerabilities Detection by Using Boyer-Moore String Matching Algorithm [7].	2015	S	S	S	P	3.5	E
3	A Review of Information Security Cryptography Technique using [8].	2017	S	S	S	P	3.5	E
4	A Review on Symmetric Key Cryptography Algorithms [28].	2017	S	S	P	N	2.5	B
5	An algorithm to find relationships Between web vulnerabilities [9].	2018	S	N	S	P	2.5	B
6	Applicability of commodity, low cost, single board computers for Internet of Things devices [10].	2016	P	S	P	P	2.5	B
7	Black-box detection of XQuery injection and parameter tampering vulnerabilities in web applications [11].	2018	S	S	S	P	3.5	E
8	Blackbox on Web Applications Penetration Testing [12].	2014	S	P	S	P	3	MB
9	Edge Cryptography and the CoDevelopment of Computer Networks and Cybersecurity [13].	2016	S	P	S	P	3	MB
10	Empirical Analysis of Web Attacks [14].	2016	P	S	S	P	3	MB
11	Generation of SQL-injection Free Secure Algorithm to Detect and Prevent Sql-Injection Attacks [15].	2012	P	S	P	S	3	MB

(continúa)

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

(viene)

ID	Study name	Year of publication	QEC				Quality	
			1	2	3	4	Quantitative	Qualitative
12	ICS honeypot System (CamouflageNet) Based on Attacker's Human Factors [16].	2015	S	N	S	P	2.5	B
13	Improving penetration testing through static and dynamic analysis [17]	2011	S	P	P	P	2.5	B
14	Kali Linux - Assuring Security by Penetration Testing [18].	2014	P	S	N	P	2	R
15	Knowledge-based security testing of web applications by logic programming [19].	2017	S	P	S	S	3.5	E
16	Large-Scale Analysis & Detection of Cross-Site Request Authentication [20].	2017	S	S	S	P	3.5	E
17	On perspective of security and privacy-preserving solutions in the Internet of things [21].	2016	P	S	P	S	3	MB
18	Overview and open issues on penetration test [22].	2017	P	S	N	P	2	R
19	Raspberry Pi 3: The revolutionary $ 35 mini-PC cures ITS biggest headaches [23].	2016	N	S	N	S	2	R
20	Reverse Engineering and Vulnerability Analysis in Cyber Security [24].	2017	P	S	S	P	3	MB
21	Security Testing Methodology for Detection of XSS Vulnerabilities in Web Services and WS-Security [25].	2014	S	P	S	P	3	MB
22	Towards resilient cyber security for embedded devices on the Internet [26].	2016	S	P	S	P	3	MB
23	Vulnerability Assessment & Penetration Testing as Cyber Defense Technology [27].	2015	S	P	S	S	3.5	E
24	WebGuardia - An integrated penetration testing system to detect web application vulnerabilities [29].	2016	S	P	S	S	3.5	E

Source: own work

5. Analysis of results

Claim that for the definition of some aspects in the process of a literature review[4], keywords, concepts and context of the research should be taken into account, so as

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

to provide a more detailed understanding of each selected study where each activity provides identification of the following: (I) Target scenarios: web applications, SBC low-cost devices, software and applications and vulnerable applications; (II) Type of research: empirical study, experimental study, proof of concept, industrial, theoretical experience and case study; (III) Type of contribution: methodology, technique, tool, focus, model, method, strategy, framework and review of literature. This classification can be seen in Figures 2, 3 and 4.

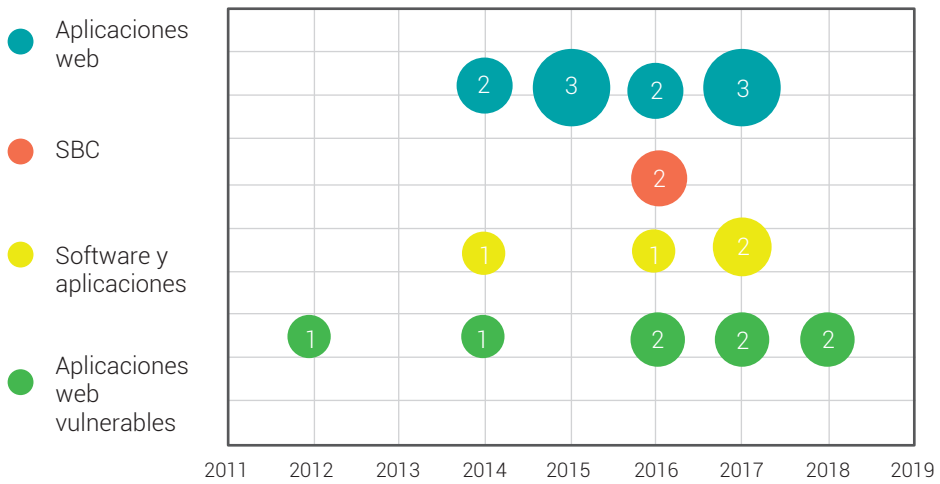

Figure 2. Bubbles diagram Studies and Stage by Year
Source: own work

This section presents a quantitative assessment regarding the contexts in which the research project may be carried out. Figure 2 shows a bubble chart with the distribution of scenarios regarding the year of publication, where the bubble size indicates the number of related issues mentioned earlier in each intersection of the studios axes.

The studies are grouped by year, so it is possible to visualize how the proof of concept was developed in recent years. Thus, as shown in Figure 3, the proof of concept has been applied most frequently in the context of web applications in recent years. Therefore, the scenarios show that web applications are one of the main topics of current research. But you can see how other scenarios are still relevant in equal measure.

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

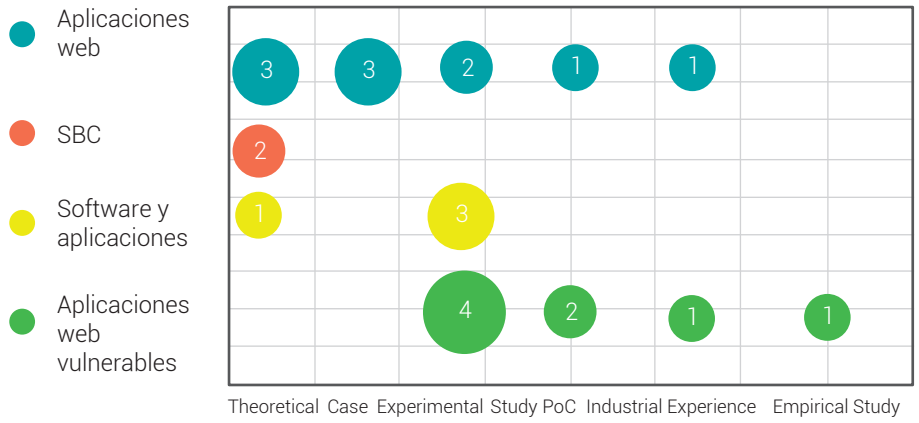

Figure 3. Bubble chart type vs Scenarios Research
Source: own work

Figure 3 shows the relationship between the target scenario and the type of research. Most selected primary studies were analyzed and characterized as experimental studies. This result suggests that research is usually apply to a specific area, looking to get the best result through a cause-effect and are not general strategies that can be applied to any context.

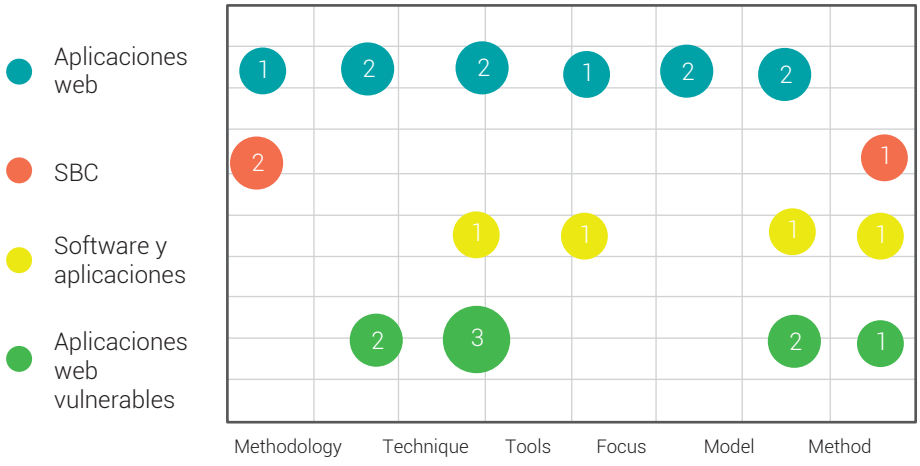

Figure 4. Bubble chart Scenarios vs Contribution type
Source: own work

Meanwhile Figure 4 shows the relationship between the stage and the type of contribution. It can be seen that most studies use or develop some kind of tool to carry out their research in a given context. This result seems consistent with the way the work is normally carried out in the field of pentesting, namely, works that tend to develop or apply a tool to evaluate or test concepts on web applications.

6. Discussion and conclusions

The results of the studies identified in this work support the findings obtained in other reviews of studies, where one of the main contributions was the analysis of web vulnerabilities; which determined some domains to be implemented for the detection of said vulnerabilities for this research work. It also contributed towards the interaction between the Raspberry Pi and the Kali Linux operating system for the execution of penetration tests and vulnerability tests, providing a very profitable joint management of both, and gave an insight into the capabilities of using Raspberry pi. With regards to the handling of network traffic and intrusion traffic, the performance of the CPU and memory usage was also measured to determine certain hardware limitations that could affect the use of certain tools in this project. Finally, the comparison of methodologies aimed at information security was observed to establish the best methodology for performing penetration analysis for web applications, in which the OWASP methodology was established, which is specifically aimed at web applications**.**

In conclusion it can be established that the main threats that could be identified during the evaluation and review of the literature, using the selection process as proposed by [4] are:

- Publication bias: refering to the possibility that some items are not selected because the search process did not produce the desired results or because the research was conducted on topics that do not feature in conferences, lectures, magazines and articles.
- Selection bias of primary studies: one cannot guarantee that all the selected primary studies were ideal during the search process and subsequent evaluation. In this regard, quality criteria and a points scoring system was introduced to mitigate this threat.
- Unfamiliarity with other fields: three search strings were defined based on the knowledge and experience of the authors, but it cannot be completely avoided that some terms are synonyms that have not yet been identified. To minimize this threat, each chain, adapted to bibliographic databases, were refined until the best results are found.
- Selection bias of relevant studies: the selection of relevant articles may have discarded some studies because the analysis was based on the title, abstract and keywords of the articles obtained in the search, obviating the material or method from the article.

e-ISSN 2357-6014 / Vol. 15, n°. 2 / mayo 2019 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

Acknowledgement

thanks to Innovation Cauca, to the Universidad del Cauca, especially to its GTI research group and to the seedbed Beta Bit of the Faculty of Engineering of the Colegio Mayor of Cauca University Institution, for the support provided for the development of the project.

References

[1] K. Linux, *Kali Linux Official Documentation*, 2016. [Online]. Available: http://es.docs.kali.org/introduction-es/que-es-kali-linux.

[2] OWASP, *OWASP Top Ten Project*, 2017. [Online]. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[3] P. &. T. Pino, "Gestión y desarrollo de proyectos de investigación distribuidos en ingeniería del software por medio de investigación-acción," *Revista Facultad de Ingeniería Universidad de Antioquia*, Vol. 1, 2013.

[4] Muñoz S. & Perez A, *Pentester de Aplicaciones web alineado a la metodología Owasp basados en un Cluster de SBC*, Facultad de Ingenieria, UNICAUCA, 2018.

[5] OWASP, *OWASP Testing Project,* 2017. [Online]. Available: https://www.owasp.org/index.php/OWASP_Testing_Project.

[6] AndrewTang, "A guide to penetration testing", *Science Direct,* vol. 1, no. 2, pp. 8-11, 2014. [Online]. doi: https://doi.org/10.1016/S1353-4858(14)70079-0

[7] N. A. A. G. K. A. F. H. M. T. F. A. R. "Ain Zubaidah MohdSaleha, A Method for Web Application Vulnerabilities Detection by Using Boyer-Moore String Matching Algorithm", *Science Direct,* vol. vol. 72. pp. 112-121, 2015. [Online]. doi: https://doi.org/10.1016/j.procs.2015.12.111.

[8] P. E. H. K. Neha Sharma, "A Review of Information Security using Cryptography Technique", *International Journal of Advanced Research in Computer Science,* vol. 8. [Online]. Available: https://www.ijarcs.info/index.php/Ijarcs/article/download/3760/3246, 2017.

[9] L. J. G. V. Fernando Román Muñoz, "An algorithm to find relationships between web vulnerabilities", *The Journal of Supercomputing,* vol. 74, no. 3. [Online]. doi: https://doi.org/10.1007/s11227-016-1770-3, pp. 1061-1089 , 2018.

[10] S. J. Johnston, M. Apetroaie-Cristea, M. Scott & S. J. Cox, "Applicability of commodity, low cost, single board computers for Internet of Things devices", *IEEE XPLORE Digital Library.* [Online]. doi: https://doi.org/10.1109/WF-IoT.2016.7845414, 2016.

[11] G. D. S. T. A. K. P. R. P. Palsetia, "Black-box detection of XQuery injection and parameter tampering vulnerabilities in web applications", *International Journal of Information Security,* vol. 17, no.1. [Online]. doi: https://doi.org/10.1007/s10207-016-0359-4, pp. 105-120, 2018.

[12] G. R. D. S. Aruina Jaiswal, "Blackbox Penetration Testing on Web Applications", *International Journal of Computer Applications,* vol. 88, no. 3, 2014.

[13] Q. DuPont & B. Fidler, "Edge Cryptography and the Codevelopment of Computer Networks and Cybersecurity," *IEEE XPLORE Digital Library,* vol. 38. [Online]. doi: https://doi.org/ 10.1109/MAHC.2016.49, pp. 55 - 73, 2016.

[14] P. K. DaljitKaur, "Empirical Analysis of Web Attacks," *Science Direct,* vol. 78, no. [Online]. doi: https://doi.org/10.1016/j.procs.2016.02.057, pp. 298-306, 2016.

[15] S. S. Kanchana Natarajan, "Generation of Sql-injection Free Secure Algorithm to Detect and Prevent Sql-Injection Attacks," *Science Direct,* vol. 4, no. 4. [Online]. doi: https://doi.org/10.1016/j.protcy.2012.05.129, pp. 790-796, 2012.

[16] M. M. W. M. T. A. M. K. I. K. Y. H. Hidemasa Naruoka, "ICS Honeypot System (CamouflageNet) Based on Attacker's Human Factors," *Science Direct,* vol. 3. [Online]. doi: https://doi.org/10.1016/j.promfg.2015.07.175, pp. 1074 - 1081, 2015.

[17] S. R. C. A. O. William & G. J. Halfond, "Improving penetration testing through static and dynamic analysis," *Published online in Wiley Online Library (wileyonlinelibrary.com).* [Online]. doi: https://doi.org/10.1002/stvr.450 , 2011.

[18] S. A. T. H. Lee Allen, Kali Linux – Assuring Security by Penetration Testing, Packt Publishing, volumen 2014, Issue 8, https://doi.org/10.1016/S1353-4858(14)70077-7, 2014.

[19] M. F. R. B. Philipp Zech, "Knowledge-based security testing of web applications by logic programming" *International Journal on Software Tools for Technology Transfer,* vols. 1, no. 2. [Online]. doi: https://doi.org/10.1007/s10009-017-0472-3, pp. 1-26, 2017.

[20] R. C. L. C. N. D. A. A. U. M. Avinash Sudhodanan, "Large-Scale Analysis & Detection of Authentication Cross-Site Request," *IEEE XPLORE Digital library.* [Online]. doi: https://doi.org/10.1109/EuroSP.2017.45, 2017.

[21] J. H. R. F. J. H. Lukas Malina, "On perspective of security and privacy-preserving solutions in the internet of things," *Science Direct,* vol. 102. [Online]. doi: https://doi.org/10.1016/j.comnet.2016.03.011, pp. 83-95, 2016.

[22] A. F. Z. Daniel Dalalana Bertoglio, "Overview and open issues on penetration test," *Journal of the Brazilian Computer Society.* [Online]. doi: https://doi.org/10.1186/s13173-017-0051-1, 2017.

[23] B. Chacos, "Raspberry Pi 3: The revolutionary $35 mini-PC cures its biggest headaches," *PcWorld*, vol. 9, no. 9. 2016. [Online]. Available: https://www.pcworld.com/article/3057888/computers/raspberry-pi-3-review-the-revolutionary-35-mini-pc-cures-its-biggest-headaches.html. [Último acceso: 2 12 2017].

[24] A. Manu Kumar, "Reverse Engineering and Vulnerability Analysis in Cyber Security," *International Journal of Advanced Research in Computer Science,* vol. 8, no. 5. pp. 950- 953, 2017. [Online]. Availablbe: https://www.ijarcs.info/index.php/Ijarcs/article/viewFile/3502/3456

[25] P. S. E. M. M.I, "Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security," *Science Direct,* vol. 302, no. 25. [Online]. doi: https://doi.org/10.1016/j.entcs.2014.01.024, pp. 133-154, 2014.

[26] D. M. D. M. S. M. B. Alie El-Din Mady, "Towards resilient cyber security for embedded devices on Internet," *IEEE Computer Society - IEEE 3rd World Forum on Internet of Things (WF-IoT),* pp. 1-2, 2016. [Online]. Available: http://www.computer.org/csdl/proceedings/wf-iot/2016/4130/00/07845439-abs.html,

[27] B. Jai Narayan Goel, "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology," *Science Direct,* vol. 57. [Online]. doi: https://doi.org/10.1016/j.procs.2015.07.458, pp. 710-715, 2015.

[28] M. Ubaidullah & Q. Makki, "A Review on Symmetric Key Encryption Techniques in Cryptography," *International Journal of Computer Applications*, vol. 147, no. 10, , pp.43-48, 2016. [Online]. Available: https://www.ijarcs.info/index.php/Ijarcs/article/download/3777/3258

[29] N. J. Nisal Madhushan Vithanage, "WebGuardia - An integrated penetration testing system to detect web application vulnerabilities," *IEEE XPLORE Digital Library - 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. [Online]. doi: https://doi.org/10.1109/WiSPNET.2016.7566124, 2016.