*Intelligent Automation & Soft Computing*
DOI:10.32604/iasc.2021.017260
***Article***

Tech Science Press

# Analysis of Security Testing Techniques

**Omer Bin Tauqeer[1], Sadeeq Jan[1,*], Alaa Omar Khadidos[2], Adil Omar Khadidos[3], Fazal Qudus Khan[3] and Sana Khattak[1]**

[1]National Center for Cyber Security, Department of Computer Science & IT, University of Engineering & Technology, Peshawar, 25120, Pakistan
[2]Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[3]Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
*Corresponding Author: Sadeeq Jan. Email: sadeeqjan@uetpeshawar.edu.pk
Received: 25 January 2021; Accepted: 03 April 2021

**Abstract:** In the past decades, a significant increase has been observed in cyber-attacks on the web-based systems used for financial purposes. Such individual systems often contain security weaknesses, called vulnerabilities that can be exploited for malicious purposes. The exploitation of such vulnerabilities can result in disclosure and manipulation of sensitive data as well as have destructive effects. To protect such systems, security testing is required on a periodic basis. Various detection and assessment techniques have been suggested by developers and researchers to address these security issues. In this paper, we survey the contributions of academia in the field of security testing for software applications and communication systems. A comprehensive review and in-depth analysis of the existing literature testing approaches has been performed to analyze their effectiveness and applicability under various scenarios. Further, we discuss various techniques used for conducting various security assessments. We follow the widely used method by Kitchenham and Charters for conducting a comprehensive systematic literature review process. Also, we propose a taxonomy for security testing techniques consisting of three main categories (Identification, Testing, and Reporting) and 17 subcategories consisting of specific security testing techniques (e.g., Black-box testing, risk assessment). Further, we assign a distinctive category from our taxonomy to each published paper in the security testing area, based on the material presented/discussed in the paper.

**Keywords:** Software testing; cyber-attacks; security testing; black-box testing; white-box testing

## 1 Introduction

A fundamental part of the Software Development Life Cycle (SDLC) is software testing comprising of two attributes, functional and non-functional. Functional testing is performed to verify the main functions/requirements of the System Under Test (SUT). Non-functional testing verifies the non-functional aspects

of the SUT, such as performance, usability, and security. Although security is a non-functional requirement, it is still considered one of the most important provision requiring an allocation of significant effort during the software development process as to ensure unhinged protection of the SUT. Software systems often contain weaknesses that make them vulnerable to various types of attacks. These weak points, also known as vulnerabilities, must therefore be identified, and appropriate security measures should be adopted to protect them from malicious incursions. One of the widely used techniques for the detection of such vulnerabilities is security testing.

Computer systems and applications are being affected by many vulnerabilities discovered from time to time. Such vulnerabilities may be exploited by attackers to disclose, modify, or delete confidential/private data [1]. They use various methods for exploiting vulnerabilities, for example, spoofing, man-in-the-middle attacks [2]. Several researchers have worked on developing new security testing techniques and improving the existing ones for the detection and prevention of vulnerabilities. Such research works are usually summarized in the form of Systematic Literature Reviews (SLRs). An SLR follows a pre-defined guideline to review the literature published in a specific field of study. In the field of security testing, very few SLRs have been carried out over the years that focus on specific vulnerabilities, applications, and hardware. Further, these SLRs discuss the literature focused on a specific platform only. One of the previously published relevant SLRs is the study by Latif et al. [3] that provides a review of various challenges, risks in cloud computing, and current countermeasures available to overcome them. Similarly, two other studies have been conducted by Dougan et al. [4] and Rafique et al. [5] in security testing. The authors provide a taxonomy based on the industrial and academic security testing process to categorize the academic literature. These studies are discussed in more detail in Section 3: Related Work.

In this study, we followed the standard methodology of Kitchenham et al. [6] for conducting the SLR. In addition, our contributions include: (i) we surveyed the most recent literature related to security testing techniques, (ii) we performed an in-depth analysis of each technique proposed in the literature for its effectiveness and applicability in various scenario, (iii) we proposed a taxonomy for security testing techniques and classified all our studied materials in appropriate categories.

The remaining paper is organized as follows: Section 2 provides the Review Plan for carrying out our study based on the guidelines of Kitchenham and Charters. In Section 3, we discuss the previous SLRs carried out in the field of security testing concerning our study. In Section 4, we present our proposed taxonomy for security testing techniques. Section 5 presents the research questions that we aim to answer in this study. The results have been discussed in Section 6 in detail. Finally, the conclusion is provided in Section 7.

## 2 Review Plan

This section presents the main components used in performing a Systematic Literature Review based on the guidelines of Kitchenham et al. [6]. It provides an overall summary of the information related to the collection and analysis of the relevant literature for our study.

### *2.1 Academic Search Engines*

For this study, we collected the published papers, from various academic journals and conferences, related to Computer Science specifically focused on cybersecurity. A total of 292 papers were selected from the online portals via Google Scholar as listed in Tab. 1.

### *2.2 Search Strings*

Tab. 2 lists the Strings and Keywords used for searching of papers during the study.

**Table 1:** List of academic databases and number of initial papers selected

| S. No | NAME | URL | No. of Papers |
|---|---|---|---|
| 1. | IEEE Xplore Digital library | ieeexplore.ieee.org | 85 |
| 2. | ScienceDirect | www.sciencedirect.com | 33 |
| 3. | SpringerLink | link.springer.com | 31 |
| 4. | ACM Digital Library | dl.acm.org | 21 |
| 5. | ResearchGate | www.researchgate.net | 20 |
| 6. | Semantic Scholar | pdfs.semanticscholar.org | 15 |
| 7. | CiteSeerX | citeseerx.ist.psu.edu | 9 |
| 8. | USENIX | www.usenix.org | 9 |
| 9. | Academia | www.academia.edu | 6 |
| 10. | arXiv.org e-Print Archive | arxiv.org | 5 |
| 11. | Emerald Insight | www.emerald.com | 4 |
| 12. | Chinese National Knowledge Infrastructure | en.cnki.com.cn | 3 |
| 13. | Scientific.Net | www.scientific.net | 3 |
| 14. | Other sources | Multiple Sources | 48 |

**Table 2:** List of search keywords

| S. No. | STRING / KEYWORDS | S. No. | STRING / KEYWORDS |
|---|---|---|---|
| 1. | Vulnerability scanning | 9. | Posture assessment |
| 2. | Vulnerability discovery | 10. | Security testing |
| 3. | Web vulnerability scanning | 11. | Penetration testing |
| 4. | Web vulnerability testing | 12. | Black box testing |
| 5. | Security scanning and testing | 13. | White box |
| 6. | Security scanning model approach | 14. | Fuzzy testing |
| 7. | Risk assessment and testing | 15. | Model based testing |
| 8. | Cyber risk assessment | | |

### *2.3 Inclusion & Exclusion Criteria*

#### *2.3.1 Inclusion Criteria*

Following is the inclusion criteria for the selection of papers for this study:

- Papers are published in the period 2010–2019.
- Papers provide information related to security testing.
- Papers propose methodologies and techniques used for security testing.

#### *2.3.2 Exclusion Criteria*

The rejection criteria for papers is given below:

- Papers that do not contain any information related to security testing are excluded.
- Papers published before 2010 are excluded.

### *2.4 Quality Checking Criteria*

For quality assessment, the following points are considered regarding each paper:

- Numbers of citations of the specified paper/study.
- Quality/Impact Factor of the journal/conference where the paper has been published/presented.

## 3 Related Work

Rafique et al. [5] carried out an SLR to analyze academic literature related to the detection of security vulnerabilities and their effects on web applications. The authors' criteria for selection is based on integrating the security methods in software development lifecycle, mostly in the requirements, design and implementation phases, with papers published in the period of 2002–2015. They follow the guidelines of Kitchenham et al. [6] for conducting an SLR. Their findings show the lack of standardized techniques for security testing.

De Franco Rosa et al. [7] presented a review on the use of ontologies in security assessment. The authors discuss their findings about the papers on security assessment, the number of citations, and important concepts of each paper. The domain of this study is limited to system security and software testing with a focus on top-level ontologies, tasks, and application ontologies. In contrast to security assessment, our study is focused on security testing. Another review paper, focused on the combination of risk analysis and security testing techniques for software security, is provided by Erdogan et al. [8]. The results show a lack of tool support as well as formal definition and empirical evidence. Similarly, Doğan et al. [4] performed a systematic literature review on web application testing techniques. The authors claim that web application testing is important because of its massive use as well as different programming languages of these applications. This study includes the papers published in the period of 2000–2013. Another review of literature on software testing techniques has been provided by Jamil et al. [9]. The authors discuss the depth and type of testing required at various phases of the software development and software release life cycle among the existing test methodologies.

Jaisawal et al. [10] discuss the issues and challenges of testing web-based systems. The authors summarize the previously published literature related to security testing including important results, e.g., various vulnerabilities affecting web applications, challenges faced by security testers, use of risk analysis in security testing, and use of agile techniques in security testing. Garousi et al. [11] conducted a survey of previous reviews published in the field of software testing. The study is focused on identifying the challenges in software testing that have been investigated in the past. The authors claim that the survey papers received more citations than the systematic mapping/literature review papers. Similarly, Bertoglio et al. [12] performed a study on the papers published regarding penetration testing. They performed a systematic mapping of various studies published related to penetration testing. The study is structured using the PICO (Population, Intervention, Comparison, Outcome) technique.

In contrast to all of the above studies, our work encompasses the security testing techniques used in the detection of vulnerabilities and their classification based on existing standards. In addition, our proposed new taxonomy and analysis of a large number of latest papers (in the period of 2010–2019) are the unique features of our study.

## 4 Proposed Taxonomy

Based on the analysis of the existing literature and industrial standards, we propose a generalized taxonomy to bridge the existing gap between the academic studies and industrial literature [13–16]. We have also used this taxonomy to classify the large number of papers that we studied in this work. Fig. 1 depicts the proposed taxonomy where various security testing techniques have been categorized in three levels (1-3) based on the types of activities in each technique. Following is a short description of each security testing technique:

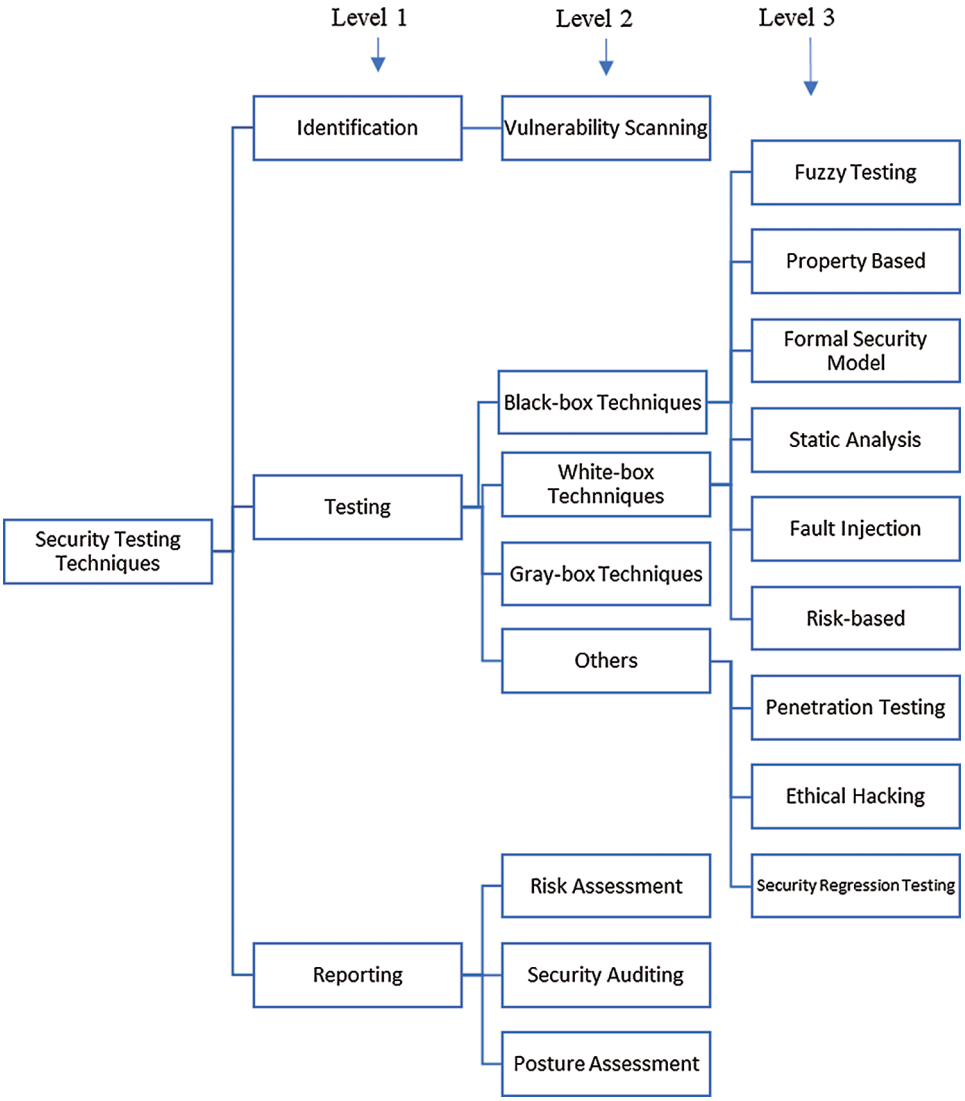


**Figure 1:** Taxonomy of security testing techniques at three levels (1, 2, 3)

### *4.1 Identification*

The identification category includes the techniques that utilize enumeration and reconnaissance of an application or a system, and identify the system's vulnerabilities/threats. These techniques utilize publicly available information on vulnerabilities from different CVE, Exploit-DB, etc. All such techniques are mostly referred to as vulnerability scanning or vulnerability discovery.

### *4.2 Testing*

We classify the testing techniques into various subcategories based upon their interaction with the system, time of processing, and knowledge requirements. Most of the existing techniques are classified into three main categories: Black-box, White-box, and Gray-box.

#### *4.2.1 Black-box Techniques*

Black-box testing includes the techniques where information on the internal working of the application is not known. Such techniques examine the fundamental aspects of the system, having little relevance to the internal structure. They can further be divided into the following two subcategories:

- Fuzzy Testing: A testing technique that utilizes the execution of randomly generated data to infect or damage a system.
- Property-Based Testing: A type of model-based approach focusing on the conversion of security properties into specifications. It extracts the code relative to the specific property using program slicing.

#### *4.2.2 White-box Techniques*

White-box testing techniques are used in the detailed investigation of the software. In such a technique, the tester is provided with all knowledge of the system under test including the source code.

- Model-based: This technique generates system models to check their adherence to the security requirements and properties.
- Static Analysis: Static Analysis, also termed manual code review, is a technique for finding vulnerabilities in the source code.
- Fault Injection: The fault injection technique tests the interaction points in a system. It further tests the limits of how far a system can be forced to execute malicious commands.
- Risk-based: These testing techniques are a subgroup of the model-based approach and utilize the previously solved test cases to mitigate any potential risks to the system.

#### *4.2.3 Gray-box Techniques*

Gray-box testing techniques are used for testing the application/system with limited knowledge of the internal structure. It increases the testing exposure by focusing on all layers of the system by combining the white-box and black-box techniques.

#### *4.2.4 Other Testing Techniques*

This category includes the techniques that could not be classified into any of the above-mentioned categories. They include:

- Penetration Testing: In the penetration testing technique, the tester attempts to find vulnerabilities in a system by mimicking the actual attacker's behavior to infect or damage the system.
- Ethical Hacking: Ethical Hacking comprises using penetration testing along with other hacking techniques to access a system in an unauthorized manner. While penetration testing involves the testing of vulnerabilities in the system, ethical hacking focuses on finding weak points in the whole environment including the clients and workers that interact with the system.
- Security Regression Testing: These techniques are used to identify vulnerabilities caused due to changes or up-gradation to the system and its functionalities.

### *4.3 Reporting*

#### *4.3.1 Risk Assessment*

Risk Assessment techniques are used to analyze the risks involved in the malicious use of the system and the potential damages. This technique utilizes various instruments for assessment, e.g., questionnaires, discussions, interviews.

#### *4.3.2 Security Auditing*

In Security Auditing, information systems are assessed by determining how well they follow the established guidelines.

#### *4.3.3 Posture Assessment*

Poster Assessment is a method for measuring and analyzing the overall security posture of an organization. It is a combination of security testing, vulnerability scanning, and risk assessment.

## 5 Research Questions

We investigate the following research questions in this paper.

- **RQ-1** How is the distribution of papers in security testing categories (Level 1)?

In this research question, we analyze the distribution of papers in the three main categories (Level 1) of our taxonomy, i.e., Identification, Testing, and Reporting.

- **RQ-2** What is the year-wise research publication trend in each security testing category (Level 1) over the last 10 years?
- **RQ-3** What is the importance of each security testing technique (Level 2)?

## 6 Results & Discussion

This section discusses the results of our analysis during the systematic literature review. Tab. 3 lists the papers that were collected in our initial data set and the assigned categories in Levels 1 and 2 of our proposed taxonomy for each paper. The results are presented in the form of answers to our formulated research questions.

**Table 3:** Classification of security testing papers

| Level 1 | Level 2 | ID |
|---|---|---|
| Identification | Vulnerability Scanning | [17–43] |
| Reporting | Posture Assessment | [44–50] |
| | Risk Assessment | [51–66] |
| | Security Auditing | [67–71] |
| Survey Paper | Literature Review | [2,3,16,72–90] |
| | Tools Review | [91–97] |
| Testing | Black-Box Testing | [98–108] |
| | Gray-Box Testing | [109–111] |
| | Other Testing | [112–118] |
| | White-Box Testing | [119–131] |

### *6.1 How is the Distribution of Papers in Security Testing Categories (Level 1)?*

To ascertain the use of each security testing technique, we have thoroughly analyzed the published work. Although we have 3 major categories in our proposed taxonomy, we also consider the survey papers as they constitute a good portion of our total collected papers.

Fig. 2 shows the number of papers in each category of our taxonomy. As depicted in the figure, a total of 146 papers (i.e., 49%), in our dataset, published between 2010–2019 are related to the Identification category. The second-largest pool of papers, i.e., 85 (29%), belongs to the category of Testing. The last two categories Reporting and Survey consist of 37 and 29 papers respectively.

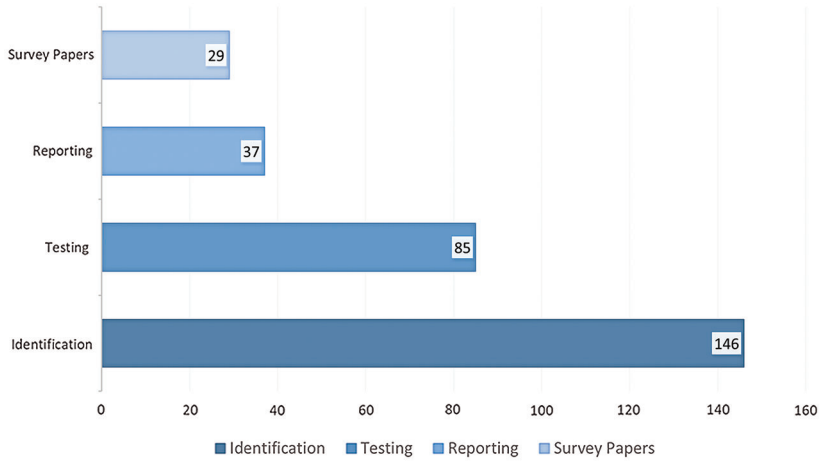


**Figure 2:** Total number of papers in each category

Fig. 3 depicts the total number of citations in each category of our proposed taxonomy. As depicted in the figure, the Identification category consists of approximately 50% of all the studies discovered during our literature review. The Testing category includes 22% of all the papers, followed by 21% of the Reporting category. Finally, Surveys make up only 7% of papers published in the selected period. The two figures demonstrate that identification techniques have been the major focus of the researchers.

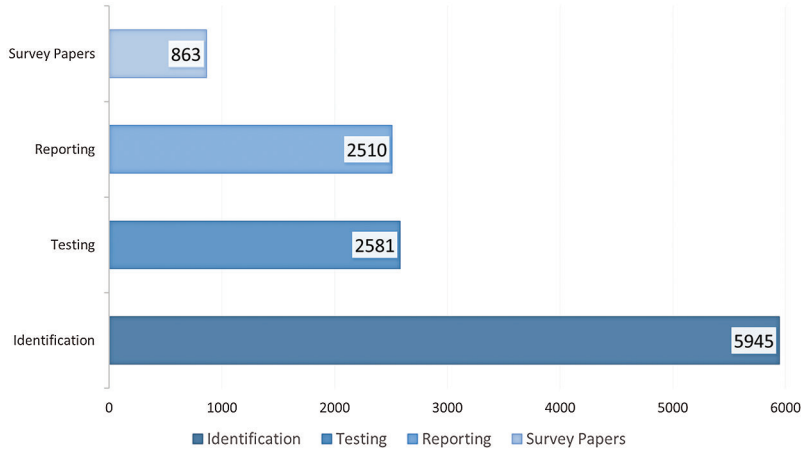


**Figure 3:** Total number of citations in each category

### *6.2 What is the Year-wise Research Publication Trend in Each Security Testing Category (Level 1) over the Last 10 Years?*

As previously discussed, papers classified in the identification category make up approximately 50% of our dataset. For further analysis, we also looked at the year-wise distribution of these papers in each technique as shown in Fig. 4. As expected, the number of papers in the Identification category is more than any of the other categories in each year except 2014 where an equal number of papers were published in Identification and Testing categories. This further shows that the Testing techniques received more attention from researchers in 2014 compared to the Reporting and Survey categories.

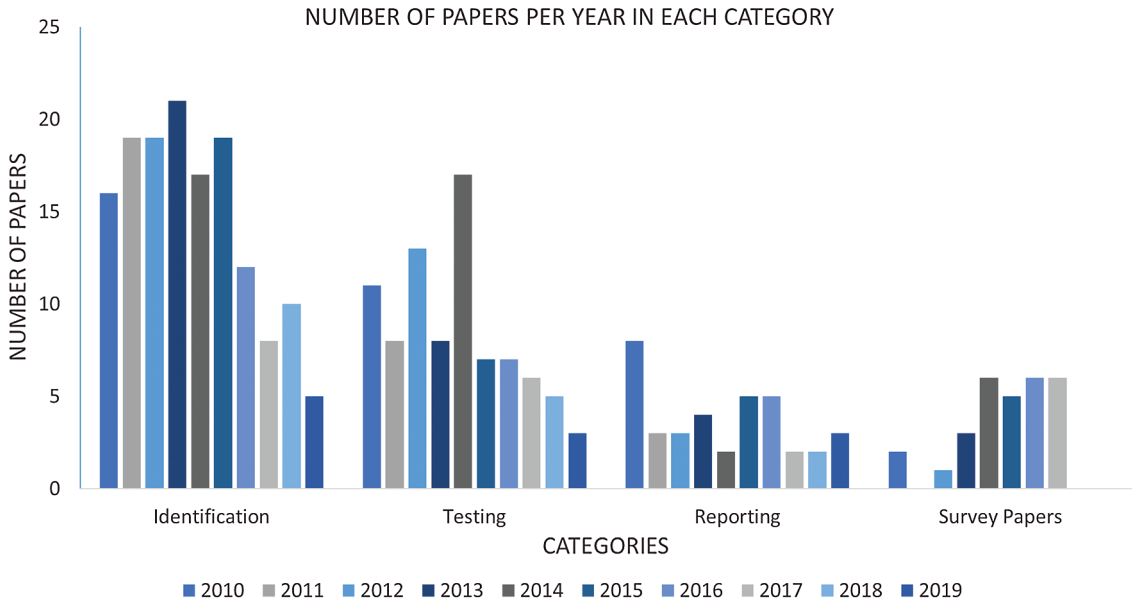


**Figure 4:** Number of papers based on year of publication

### *6.3 What is the Importance of Each Security Testing Technique (Level 2)?*

Fig. 5 shows a comparison of different testing techniques of the subcategories (level 2) in our proposed taxonomy. The highest number of citations belongs to the Vulnerability Scanning, i.e., 2410, while the Risk Assessment category is at the second-highest position with 1103 citations. The trend is followed by the White-box Testing techniques having 595 citations, Security Auditing with 555, and 136 citations for the Gray-box Testing Techniques.

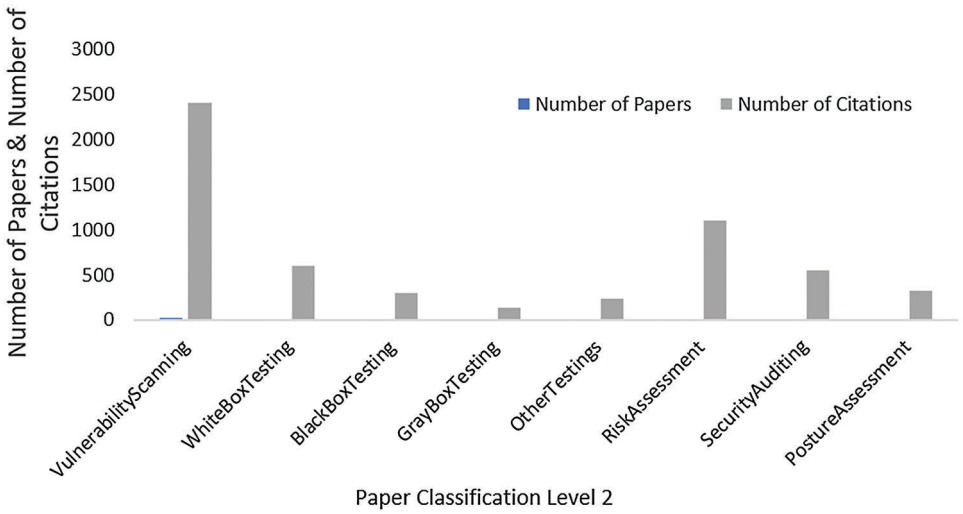


**Figure 5:** Importance of each technique based on the number of papers & citations

## 7 Conclusion

In this paper, we have presented a comprehensive Systematic Literature Review (SLR) of the security testing techniques. The SLR has been carried out using the principles/guidelines of the widely used method of Kitchenham and Charters. Our dataset consists of the papers published in the recent ten years (2010–2019). We found a total of 292 papers relevant to Security Testing and thoroughly analyzed and discussed these papers from various aspects.

We proposed a new taxonomy for the classification of security testing techniques which consists of three major categories at level 1 (Identification, Testing, and Reporting), 8 security testing techniques at level 2, and 9 categories at level 3, e.g., Black-box testing, risk assessment. We assigned each studied paper to one of these categories based on the methods proposed/discussed in the paper. Our results demonstrate that, over the last 10 years, the highest number of papers and citations belong to the vulnerability scanning category. In addition, the papers published in the last 2–3 years have a very limited number of citations. Moreover, we also found a trend of using the older studies/techniques for security testing despite the fact that new studies have been conducted on yearly basis. Researchers and developers are still adapting the leading-edge techniques for the detection of new vulnerabilities. This research work is beneficial for future researchers of security testing as it provides a comprehensive analysis of the state-of-the-art in the field of security testing.

**Funding Statement:** This research is funded by the Higher Education Commission (HEC), Pakistan through its initiative of National Center for Cyber Security for the affiliated Security Testing- Innovative Secured Systems Lab (ISSL) established at University of Engineering & Technology (UET) Peshawar, Grant No: 2(1078)/HEC/M&E/2018/707.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] D. Wichers and J. Williams, "OWASP Top-10 2017," *OWASP Foundation,* 2017. [Online]. Available: https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/.

[2] M. M. Noor and W. H. Hassan, "Wireless networks: Developments, threats and countermeasures," *International Journal of Digital Information and Wireless Communications (IJDIWC)*, vol. 3, pp. 119–134, 2013.

[3] R. Latif, H. Abbas, S. Assar and Q. Ali, "Cloud computing risk assessment: A systematic literature review, " in *Future Information Technology*, pp. 285–295, 2014.

[4] S. Doğan, A. Betin-Can and V. Garousi, "Web application testing: A systematic literature review," *Journal of Systems and Software*, vol. 91, no. 3, pp. 174–201, 2014.

[5] S. Rafique, M. Humayun, Z. Gul, A. Abbas and H. Javed, "Systematic review of web application security vulnerabilities detection methods," *Journal of Computer and Communications*, vol. 3, no. 09, pp. 28–40, 2015.

[6] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," UK: EBSE Technical Report, Keele University, 2007.

[7] F. de Franco Rosa and M. Jino, "A survey of security assessment ontologies," in *Proc. 5th World Conf. on Information Systems and Technologies (WorldCist'17)*, Porto Santo Island, Madeira, Portugal, pp. 166–173, 2017.

[8] G. Erdogan, Y. Li, R. K. Runde, F. Seehusen and K. Stølen, "Approaches for the combined use of risk analysis and testing: A systematic literature review," *International Journal on Software Tools for Technology Transfer*, vol. 16, no. 5, pp. 627–642, 2014.

[9] M. A. Jamil, M. Arif, N. S. A. Abubakar and A. Ahmad, "Software testing techniques: A literature review," in *Proc. 2016 6th Int. Conf. on Information and Communication Technology for The Muslim World (ICT4M)*, Jakarta, Indonesia, 2016.

[10] A. Jaiswal, G. Raj and D. Singh, "Security testing of web applications: Issues and challenges," *International Journal of Computer Applications*, vol. 88, no. 3, pp. 26–32, 2014.

[11] V. Garousi and M. V. Mäntylä, "A systematic literature review of literature reviews in software testing," *Information and Software Technology*, vol. 80, no. 1, pp. 195–216, 2016.

[12] D. D. Bertoglio and A. F. Zorzo, "Overview and open issues on penetration test," *Journal of the Brazilian Computer Society*, vol. 23, no. 1, pp. 49, 2017.

[13] M. Howard and S. Lipner, "The security development lifecycle," *Redmond: Microsoft Press. Google Scholar Google Scholar Digital Library Digital Library.* Vol. 8, 2006.

[14] P. Herzog, "OSSTMM 3 - the open source security testing methodology manual: Contemporary security testing and analysis," *ISECOM-Institute for Security and Open Methodologies*, 2010. [Online]. Available: https://www.isecom.org/OSSTMM.3.pdf.

[15] J. T. F. T. Initiative, "Guide for conducting risk assessments (SP 800-30 Rev. 1)," National Institute of Standards and Technology Special Publication, 2012.

[16] M. Felderer, M. Büchler, M. Johns, A. D. Brucker, R. Breu *et al.,* "Security testing: A survey," *Advances in Computers*, vol. 101, pp. 1–51, 2016.

[17] C. J. Chung, P. Khatkar, T. Xing, J. Lee and D. Huang, "Network intrusion detection and countermeasure selection in virtual network systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 198–211, 2013.

[18] A. Almadhoob and R. Valverde, "Cybercrime prevention in the Kingdom of Bahrain via IT security audit plans," *Journal of Theoretical and Applied Information Technology*, vol. 65, pp. 274–292, 2014.

[19] A. Stasinopoulos, C. Ntantogian and C. Xenakis, "Commix: Automating evaluation and exploitation of command injection vulnerabilities in Web applications," *International Journal of Information Security*, vol. 18, no. 1, pp. 49–72, 2019.

[20] L. Zhang, D. Zhang, C. Wang, J. Zhao and Z. Zhang, "ART4SQLi: The art of SQL injection vulnerability discovery," *IEEE Transactions on Reliability*, vol. 68, no. 4, pp. 1–20, 2019.

[21] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey and J. A. Halderman, "A search engine backed by Internet-wide scanning," in *Proc. the 22nd ACM SIGSAC Conf. on Computer and Communications Security*, New York, NY, USA, 2015.

[22] Z. Durumeric, M. Bailey and J. A. Halderman, "An internet-wide view of internet-wide scanning," in *Proc. 23rd USENIX Security Sym. (USENIX Security 14)*, San Diego, CA, USA, 2014.

[23] F. Palmieri, U. Fiore and A. Castiglione, "Automatic security assessment for next generation wireless mobile networks," *Mobile Information Systems*, vol. 7, no. 3, pp. 217–239, 2011.

[24] S. Skorobogatov and C. Woods, "Breakthrough silicon scanning discovers backdoor in military chip," in *Proc. 14th Int. Workshop on Cryptographic Hardware and Embedded Systems*, Leuven, Belgium, 2012.

[25] T. Unruh, B. Shastry, M. Skoruppa, F. Maggi, K. Rieck *et al.,* "Leveraging flawed tutorials for seeding large-scale web vulnerability discovery," in *Proc. 11th USENIX Workshop on Offensive Technologies (WOOT 17)*, Vancouver, BC, Canada, 2017.

[26] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan *et al.,* "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 235–244, 2013.

[27] H. Holm, M. Ekstedt and D. Andersson, "Empirical analysis of system-level vulnerability metrics through actual attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 825–837, 2012.

[28] A. Doupé, L. Cavedon, C. Kruegel and G. Vigna, "Enemy of the state: A state-aware black-box web vulnerability scanner," in *Proc. 21st USENIX Security Sym. (USENIX Security 12)*, Bellevue, WA, 2012.

[29] F. Baiardi, F. Corò, F. Tonelli and L. Guidi, "GVScan: Scanning networks for global vulnerabilities," in *Proc. 2013 Int. Conf. on Availability, Reliability and Security*, Hamburg, Germany, 2013.

[30] B. Stock, G. Pellegrino, C. Rossow, M. Johns and M. Backes, "Hey, you have a problem: On the feasibility of large-scale web vulnerability notification," in *Proc. 25th USENIX Security Sym. (USENIX Security 16)*, Austin, TX, USA, 2016.

[31] J. O'Hare, R. Macfarlane and O. Lo, "Identifying vulnerabilities using internet-wide scanning data," in *Proc. 2019 IEEE 12th Int. Conf. on Global Security, Safety and Sustainability (ICGS3)*, London, England, 2019.

[32] S. Taubenberger, J. Jürjens, Y. Yu and B. Nuseibeh, "Resolving vulnerability identification errors using security requirements on business process models," *Information Management & Computer Security*, vol. 21, no. 3, pp. 202–223, 2013.

[33] A. Tsuchiya, F. Fraile, I. Koshijima, A. Ortiz and R. Poler, "Software defined networking firewall for industry 4.0 manufacturing systems," *Journal of Industrial Engineering and Management*, vol. 11, no. 2, pp. 318–333, 2018.

[34] A. Algarni and Y. Malaiya, "Software vulnerability markets: Discoverers and buyers," *International Journal of Computer, Information Science and Engineering*, vol. 8, pp. 71–81, 2014.

[35] G. Wassermann and Z. Su, "Sound and precise analysis of web applications for injection vulnerabilities," in *ACM Sigplan Notices*, California, USA, pp. 32–41, 2007.

[36] A. D. Householder, G. Wassermann, A. Manion and C. King, "The CERT guide to coordinated vulnerability disclosure," *Special Report by Software Engineering Institute*, Pittsburgh, USA, Carnegie Mellon University, 2017.

[37] T. Sommestad, M. Ekstedt and H. Holm, "The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures," *IEEE Systems Journal*, vol. 7, no. 3, pp. 363–373, 2013.

[38] B. Grobauer, T. Walloschek and E. Stocker, "Understanding cloud computing vulnerabilities," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 50–57, 2011.

[39] M. Papadaki and S. Furnell, "Vulnerability management: An attitude of mind?," *Network Security*, vol. 2010, no. 10, pp. 4–8, 2010.

[40] A. Doupé, M. Cova and G. Vigna, "Why johnny can't pentest: An analysis of black-box web vulnerability scanners," *Detection of Intrusions and Malware, and Vulnerability Assessment*, vol. 6201, pp. 111–131, 2010.

[41] F. Li, Z. Durumeric, J. Czyz, M. Karami, M. Bailey *et al.,* "You've got vulnerability: exploring effective vulnerability notifications," in *Proc. 25th USENIX Security Sym. (USENIX Security 16)*, Austin, TX, USA, 2016.

[42] N. Suteva, D. Zlatkovski and A. Mileva, "Evaluation and testing of several free/open source web vulnerability scanners," in *Proc. The 10th Conf. for Informatics and Information Technology (CIIT 2013)*, Bitola Macedonia, 2013.

[43] H. Holm, T. Sommestad, J. Almroth and M. Persson, "A quantitative evaluation of vulnerability scanning," *Information Management & Computer Security*, vol. 19, no. 4, pp. 231–247, 2011.

[44] K. R. Sarkar, "Assessing insider threats to information security using technical, behavioural and organisational measures," *Information Security Technical Report*, vol. 15, no. 3, pp. 112–133, 2010.

[45] J. Chen, Y. Wang and X. Wang, "On-demand security architecture for cloud computing," *Computer*, vol. 45, no. 7, pp. 73–78, 2012.

[46] N. Rjaibi, L. B. A. Rabai, A. B. Aissa and M. Louadi, "Cyber security measurement in depth for e-learning systems," *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, vol. 2, pp. 107–120, 2012.

[47] E. Panaousis, A. Fielder, P. Malacaria, C. Hankin and F. Smeraldi, "Cybersecurity games and investments: A decision support approach," in *Proc. Int. Conf. on Decision and Game Theory for Security*, Los Angeles, CA, USA, 2014.

[48] C. Pham, D. Tang, K. i Chinen and R. Beuran, "Cyris: A cyber range instantiation system for facilitating security training," in *Proc. the Seventh Sym. on Information and Communication Technology (SOICT 16)*, Vietnam: Ho Chi Minh City, 2016.

[49] G. A. Francia III, D. Thornton and J. Dawson, "Security best practices and risk assessment of SCADA and industrial control systems," in *Proc. The 2012 Int. Conf. on Security and Management (SAM)*, Las Vegas, USA, 2012.

[50] Z. Zhang and B. B. Gupta, "Social media security and trustworthiness: Overview and new direction," *Future Generation Computer Systems*, vol. 86, no. 2, pp. 914–925, 2018.

[51] S. Patel and J. Zaveri, "A risk-assessment model for cyber attacks on information systems," *Journal of Computers*, vol. 5, no. 3, pp. 352–359, 2010.

[52] N. Feng and M. Li, "An information systems security risk assessment model under uncertain environment," *Applied Soft Computing*, vol. 11, no. 7, pp. 4332–4340, 2011.

[53] N. Zahadat, P. Blessner, T. Blackburn and B. A. Olson, "BYOD security engineering: A framework and its analysis," *Computers & Security*, vol. 55, no. 4, pp. 81–99, 2015.

[54] F. Baiardi, F. Tonelli and L. Isoni, "Considering application vulnerabilities in risk assessment and management," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 7, pp. 41–59, 2016.

[55] M. Anastacio, J. A. Blanco, L. Villalba and A. Dahoud, "E-Government: benefits, risks and a proposal to assessment including cloud computing and critical infrastructure," in *Proc. The 6th Int. Conf. on Information Technology*, Amman, Jordan, 2013.

[56] J. Dawson and J. T. McDonald, "Improving penetration testing methodologies for security-based risk assessment," in *Proc. 2016 Cybersecurity Sym. (CYBERSEC)*, Coeur d'Alene, ID, USA, 2016.

[57] Z. Xinlan, H. Zhifang, W. Guangfu and Z. Xin, "Information security risk assessment methodology research: Group decision making and analytic hierarchy process," in *Proc. 2010 Second World Congress on Software Engineering*, Wuhan, China, 2010.

[58] X. Zhang, N. Wuwong, H. Li and X. Zhang, "Information security risk management framework for the cloud computing environments," in *Proc. 2010 10th IEEE Int. Conf. on Computer and Information Technology*, Bradford, UK, 2010.

[59] S. Papastergiou and N. Polemi, "MITIGATE: A dynamic supply chain cyber risk assessment methodology, Smart Trends in Systems," *Security and Sustainability*, vol. 18, pp. 1–9, 2018.

[60] J. Henriksen-Bulmer, S. Faily and S. Jeary, "Privacy risk assessment in context: A meta-model based on contextual integrity," *Computers & Security*, vol. 82, no. 1/2, pp. 270–283, 2019.

[61] J. Hughes and G. Cybenko, "Quantitative metrics and risk assessment: The three tenets model of cybersecurity," *Technology Innovation Management Review*, vol. 3, no. 8, pp. 15–24, 2013.

[62] P. Saripalli and B. Walters, "Quirc: A quantitative impact and risk assessment framework for cloud security," in *Proc. 2010 IEEE 3rd Int. Conf. on Cloud Computing*, Miami, Florida, 2010.

[63] B. Edwards, J. Jacobs and S. Forrest, "Risky business: Assessing security with external measurements," arXiv preprint arXiv:1904.11052, 2019.

[64] G. Macher, H. Sporer, R. Berlach, E. Armengaud and C. Kreiner, "SAHARA: A security-aware hazard and risk analysis method," in *Proc. The 2015 Design, Automation & Test in Europe Conf. & Exhibition (DATE '15)*, Grenoble, France, 2015.

[65] H. Shahriar and H. Haddad, "Security assessment of clickjacking risks in web applications: Metrics based approach," in *Proc. The 30th Annual ACM Sym. on Applied Computing (SAC 2015)*, Salamanca Spain, 2015.

[66] N. Poolsappasit, R. Dewri and I. Ray, "Dynamic security risk management using bayesian attack graphs," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61–74, 2012.

[67] L. M. Kaufman, "Can a trusted environment provide security?," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 50–52, 2010.

[68] A. Hahn, A. Ashok, S. Sridhar and M. Govindarasu, "Cyber-physical security testbeds: architecture, application, and evaluation for smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, 2013.

[69] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision Support Systems*, vol. 86, no. 6, pp. 13–23, 2016.

[70] M. E. Dawson Jr, M. Crespo and S. Brewster, "DoD cyber technology policies to secure automated information systems," *International Journal of Business Continuity and Risk Management*, vol. 4, no. 1, pp. 1–22, 2013.

[71] J. J. Zhao and S. Y. Zhao, "Opportunities and threats: A security assessment of state e-government websites," *Government Information Quarterly*, vol. 27, no. 1, pp. 49–56, 2010.

[72] A. Gupta, A. Jain, S. Yadav and H. Taneja, "Literature survey on detection of web attacks using machine learning," *International Journal of Scientific Research Engineering & Information Technology*, vol. 3, pp. 1845–1853, 2018.

[73] S. Shah and B. M. Mehtre, "An overview of vulnerability assessment and penetration testing techniques," *Journal of Computer Virology and Hacking Techniques*, vol. 11, no. 1, pp. 27–49, 2015.

[74] M. Khari and P. Kumar, "An extensive evaluation of search-based software testing: A review," *Soft Computing*, vol. 23, no. 6, pp. 1933–1946, 2019.

[75] M. E. Khan and F. Khan, "A comparative study of white box, black box and grey box testing techniques," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 3, pp. 12–19, 2012.

[76] A. Austin, C. Holmgreen and L. Williams, "A comparison of the efficiency and effectiveness of vulnerability discovery techniques," *Information and Software Technology*, vol. 55, no. 7, pp. 1279–1288, 2013.

[77] R. Johari and P. Sharma, "A survey on web application vulnerabilities (SQLIA, XSS) exploitation and security engine for SQL injection," in *Proc. 2012 Int. Conf. on Communication Systems and Network Technologies (CSNT 2012)*, Rajkot, India, 2012.

[78] M. Felderer and E. Fourneret, "A systematic classification of security regression testing approaches," *International Journal on Software Tools for Technology Transfer*, vol. 17, no. 3, pp. 305–319, 2015.

[79] S. Acharya and V. Pandya, "Bridge between black box and white box-gray box testing technique," *International Journal of Electronics and Computer Science Engineering*, vol. 2, pp. 175–185, 2012.

[80] M. Felderer and I. Schieferdecker, "A taxonomy of risk-based testing," *International Journal on Software Tools for Technology Transfer*, vol. 16, no. 5, pp. 559–568, 2014.

[81] E. Bou-Harb, M. Debbabi and C. Assi, "Cyber scanning: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1496–1519, 2014.

[82] M. E. Khan, "Different forms of software testing techniques for finding errors," *International Journal of Computer Science Issues (IJCSI)*, vol. 7, pp. 11–16, 2010.

[83] F. Bouquet, F. Peureux and F. Ambert, "Model-based testing for functional and security test generation," *Foundations of Security Analysis and Design VII*. Springer, Cham, pp. 1–33, 2013.

[84] M. Khari and C. Bajaj, "Motivation for security testing," *Journal of Global Research in Computer Science*, vol. 5, pp. 26–32, 2014.

[85] N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya and J. K. Kalita, "Network attacks: Taxonomy, tools and systems," *Journal of Network and Computer Applications*, vol. 40, no. 3, pp. 307–324, 2014.

[86] A. Austin and L. Williams, "One technique is not enough: A comparison of vulnerability discovery techniques," in *Proc. 2011 Int. Sym. on Empirical Software Engineering and Measurement*, Alberta, Canada, 2011.

[87] E. Amoroso, "Recent progress in software security," *IEEE Software*, vol. 35, no. 2, pp. 11–13, 2018.

[88] G. Tian-yang, S. Yin-sheng and F. You-yuan, "Research on software security testing," *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 70, pp. 647–651, 2010.

[89] R. Montesino, S. Fenz and W. Baluja, "SIEM-based framework for security controls automation," *Information Management & Computer Security*, vol. 20, no. 4, pp. 248–263, 2012.

[90] B. Liu, L. Shi, Z. Cai and M. Li, "Software vulnerability discovery techniques: a survey," in *Proc. 2012 Fourth Int. Conf. on Multimedia Information Networking and Security (MINES '12)*, Nanjing, Jiangsu, China, 2012.

[91] Y. Makino and V. Klyuev, "Evaluation of web vulnerability scanners," in *Proc. 2015 IEEE 8th Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS' 2015)*, Warsaw, Poland, 2015.

[92] D. Esposito, M. Rennhard, L. Ruf and A. Wagner, "Exploiting the potential of web application vulnerability scanning," in *Proc. ICIMP, 2018 - The Thirteenth Int. Conf. on Internet Monitoring and Protection*, Barcelona, Spain, pp. 22–29, 2018.

[93] A. Bansal, "A comparative study of software testing yechniques," *International Journal of Computer Science and Mobile Computing*, vol. 36, pp. 579–584, 2014.

[94] Y. Martirosyan, "Security evaluation of web application vulnerability scanners strengths and limitations using custom web application," M.S Thesis. California State University, East Bay, CA, USA, 2012.

[95] R. Scandariato, J. Walden and W. Joosen, "Static analysis versus penetration testing: A controlled experiment," in *Proc. 2013 IEEE 24th Int. Sym. on Software Reliability Engineering (ISSRE)*, Pasadena, CA, USA, 2013.

[96] D. Sagar, S. Kukreja, J. Brahma, S. Tyagi and P. Jain, "Studying open source vulnerability scanners for vulnerabilities in web applications," *IIOAB JOURNAL*, vol. 9, pp. 43–49, 2018.

[97] Z. Durumeric, E. Wustrow and J. A. Halderman, "ZMap: Fast internet-wide scanning and its security applications," in *Proc. The 22nd USENIX Security Sym. (USENIX Security 13)*, Washington, D.C., USA, 2013.

[98] F. Duchene, S. Rawat, J.-L. Richier and R. Groz, "KameleonFuzz: Evolutionary fuzzing for black-box XSS detection," in *Proc. The 4th ACM conf. on Data and Application Security and Privacy*, San Antonio, Texas, USA, 2014.

[99] V. Ganesh, A. Kieżun, S. Artzi, P. J. Guo, P. Hooimeijer *et al.,* "HAMPI: A string solver for testing, analysis and vulnerability detection," in *Proc. 23rd Int. Conf. on Computer Aided Verification (CAV 11)*, Snowbird, UT, USA, 2011.

[100] S. Ninawe and P. R. Wajgi, "An enhanced approach for XSS attack detection on web applications," *International Journal of Scientific Research in Science and Technology (IJSRST)*, vol. 6, no. 2, pp. 562–567, 2019.

[101] A. Ciampa, C. A. Visaggio and M. D. Penta, "A heuristic-based approach for detecting SQL-injection vulnerabilities in web applications," in *Proc. The 2010 ICSE Workshop on Software Engineering for Secure Systems*, Cape Town, South Africa, 2010.

[102] D. Appelt, C. D. Nguyen, L. C. Briand and N. Alshahwan, "Automated testing for SQL injection vulnerabilities: An input mutation approach," in *Proc. The 2014 Int. Sym. on Software Testing and Analysis*, San Jose, CA, USA, 2014.

[103] K. Vijayakumar and C. Arun, "Continuous security assessment of cloud based applications using distributed hashing algorithm in SDLC," *Cluster Computing*, vol. 22, no. S5, pp. 10789–10800, 2019.

[104] B. K. Ayeni, J. B. Sahalu and K. R. Adeyanju, "Detecting cross-site scripting in web applications using fuzzy inference system," *Journal of Computer Networks and Communications*, vol. 2018, no. 12, pp. 1–10, 2018.

[105] N. Li, T. Xie, M. Jin and C. Liu, "Perturbation-based user-input-validation testing of web applications," *Journal of Systems and Software*, vol. 83, no. 11, pp. 2263–2274, 2010.

[106] A. Avancini and M. Ceccato, "Security testing of web applications: a search-based approach for cross-site scripting vulnerabilities," in *Proc. 2011 IEEE 11th Int. Working Conf. on Source Code Analysis and Manipulation*, Williamsburg, VA, USA, 2011.

[107] M. Mahdi and A. H. Mohammad, "Using hash algorithm to detect SQL injection vulnerability," *International Journal of Research in Computer Applications and Robotics*, vol. 4, pp. 26–32, 2016.

[108] J. Bau, E. Bursztein, D. Gupta and J. Mitchell, "State of the art: Automated black-box web application vulnerability testing," in *Proc. 2010 IEEE Sym. on Security and Privacy*, Oakland, CA, USA, 2010.

[109] W. G. J. Halfond, S. R. Choudhary and A. Orso, "Improving penetration testing through static and dynamic analysis, Software Testing," *Verification and Reliability*, vol. 21, no. 3, pp. 195–214, 2011.

[110] O. Pieczul and S. N. Foley, "Runtime detection of zero-day vulnerability exploits in contemporary software systems," in *Proc. IFIP Annual Conf. on Data and Applications Security and Privacy*, Trento, Italy, 2016.

[111] M. I. P. Salas and E. Martins, "Security testing methodology for vulnerabilities detection of XSS in web services and WS-security," *Electronic Notes in Theoretical Computer Science*, vol. 302, no. 8, pp. 133–154, 2014.

[112] D. E. Simos, J. Zivanovic and M. Leithner, "Automated combinatorial testing for detecting SQL vulnerabilities in web applications," in *Proc. The 14th Int. Workshop on Automation of Software Test*, Montreal, Quebec, Canada, 2019.

[113] N. Antunes and M. Vieira, "Penetration testing for web services," *Computer*, vol. 47, no. 2, pp. 30–36, 2014.

[114] C. Mainka, J. Somorovsky and J. Schwenk, "Penetration testing tool for web services security," in *Proc. of 2012 IEEE Eighth World Congress on Services*, Honolulu, Hawaii, USA, 2012.

[115] C. Sarraute, O. Buffet and J. Hoffmann, "POMDPs make better hackers: accounting for uncertainty in penetration testing," in *Proc. Twenty-Sixth AAAI Conf. on Artificial Intelligence*, Toronto, Ontario, Canada, 2012.

[116] T. W. Thomas, M. Tabassum, B. Chu and H. Lipford, "Security during application development: An application security expert perspective," in *Proc. The 2018 CHI Conf. on Human Factors in Computing Systems*, New York, NY, USA, 2018.

[117] J. Hoffmann, "Simulated penetration testing: from dijkstra to turing test++," in *Proc. Twenty-Fifth Int. Conf. on Automated Planning and Scheduling*, Jerusalem, Israel, 2015.

[118] T. Farah, D. Alam, M. A. Kabir and T. Bhuiyan, "SQLi penetration testing of financial web applications: Investigation of Bangladesh region," in *Proc. 2015 World Congress on Internet Security (WorldCIS)*, Dublin, Ireland, 2015.

[119] O. El Ariss and D. Xu, "Modeling security attacks with statecharts," in *Proc. The Joint ACM SIGSOFT Conference-QoSA and ACM SIGSOFT Symposium-ISARCS on Quality of Software Architectures-QoSA and Architecting Critical Systems-ISARCS*, Boulder Colorado USA, 2011.

[120] I. Schieferdecker, J. Grossmann and M. Schneider, "Model-based security testing," arXiv Preprint arXiv:1202.6118, pp. 1–12, 2012.

[121] M. Felderer, P. Zech, R. Breu, M. Büchler and A. Pretschner, "Model-based security testing: A taxonomy and systematic classification," *Software Testing, Verification and Reliability*, vol. 26, no. 2, pp. 119–148, 2016.

[122] D. Xu, M. Tu, M. Sanford, L. Thomas, D. Woodraska *et al.,* "Automated security test generation with formal threat models," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp. 526–540, 2012.

[123] J. Savaglia and P. Wang, "Cybersecurity vulnerability analysis via virtualization," *Issues in Information Systems*, vol. 18, pp. 91–98, 2017.

[124] A. Hahn, B. Kregel, M. Govindarasu, J. Fitzpatrick, R. Adnan *et al.,* "Development of the powercyber SCADA security testbed," in *Proc. The Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, Oak Ridge, Tennessee, USA, 2010.

[125] A. B. Ibrahim and S. Kant, "Penetration testing using SQL injection to recognize the vulnerable point on web pages," *International Journal of Applied Engineering Research*, vol. 13, pp. 5935–5942, 2018.

[126] M. M. Hassan, T. Bhuyian, M. K. Sohel, M. H. Sharif, S. Biswas *et al.,* "An automated local file inclusion vulnerability detection model," *International Journal of Engineering & Technology*, vol. 7, no. 23, pp. 4–8, 2018.

[127] A. Singhal and X. Ou, "Security risk analysis of enterprise networks using probabilistic attack graphs," *Network Security Metrics*. Cham: Springer, pp. 53–73, 2017.

[128] M. Büchler, J. Oudinet and A. Pretschner, "Semi-automatic security testing of web applications from a secure model," in *Proc. 2012 IEEE Sixth Int. Conf. on Software Security and Reliability*, Gaithersburg, Maryland, USA, 2012.

[129] Y. Zhou and D. Evans, "SSOScan: Automated testing of web applications for single sign-on vulnerabilities," in *Proc. 23rd USENIX Security Sym. (USENIX Security 14)*, San Diego, USA, 2014.

[130] G. Díaz and J. R. Bermejo, "Static analysis of source code security: Assessment of tools against SAMATE tests," *Information and Software Technology*, vol. 55, no. 8, pp. 1462–1476, 2013.

[131] P. Li and B. Cui, "A comparative study on software vulnerability static analysis techniques and tools," in *Proc. 2010 IEEE Int. Conf. on Information Theory and Information Security*, Beijing, China, 2010.