I. List of the primary studies identified through the systematic literature review

The primary studies are [1]–[123]

References

[1] J. Thomé, L. K. Shar, D. Bianculli, and L. Briand, "Security slicing for auditing common injection vulnerabilities," *Journal of Systems and Software*, vol. 137, pp. 766–783, 2018.

[2] I. Medeiros, N. Neves, and M. Correia, "Detecting and removing web application vulnerabilities with static analysis and data mining," *IEEE Transactions on Reliability*, vol. 65, no. 1, pp. 54–69, 2016. [Online]. Available: https://ieeexplore.ieee.org/ielx7/24/7422884/07206620.pdf?tp=&arnumber=7206620&isnumber=7422884

[3] D. Muthukumaran, D. O'Keeffe, C. Priebe, D. Eyers, B. Shand, and P. Pietzuch, "Flowwatcher: Defending against data disclosure vulnerabilities in web applications," in *Proc. of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 2813639: ACM, 2015, Conference Proceedings, pp. 603–615.

[4] A. Amira, A. Ouadjaout, A. Derhab, and N. Badache, "Sound and static analysis of session fixation vulnerabilities in php web applications," in *Proc. of the 7th ACM on Conference on Data and Application Security and Privacy*. 3029838: ACM, 2017, Conference Proceedings, pp. 139–141.

[5] X. X. Yan, H. T. Ma, and Q. X. Wang, "A static backward taint data analysis method for detecting web application vulnerabilities," in *Proc. of the IEEE 9th International Conference on Communication Software and Networks*, 2017, Conference Proceedings, pp. 1138–1141.

[6] C. Catal, A. Akbulut, E. Ekenoglu, and M. Alemdaroglu, "Development of a software vulnerability prediction web service based on artificial neural networks," in *Proc. of the 2017 Pacific-Asia Conference on Knowledge Discovery and Data Mining Workshops*, U. Kang, E.-P. Lim, J. X. Yu, and Y.-S. Moon, Eds. Springer International Publishing, 2017, Conference Proceedings, pp. 59–67.

[7] S. Wen, Y. Xue, J. Xu, H. J. Yang, X. H. Li, W. L. Song, and G. N. Si, "Toward exploiting access control vulnerabilities within mongodb backend web applications," in *Proc. of the 2016 IEEE 40th Annual Computer Software and Applications Conference Workshops*, 2016, Conference Proceedings, pp. 143–153. [Online]. Available: https://ieeexplore.ieee.org/ielx7/7551592/7551973/07552002.pdf?tp=&arnumber=7552002&isnumber=7551973

[8] M. N. Khalid, M. Iqbal, M. T. Alam, V. Jain, H. Mirza, and K. Rasheed, "Web unique method (wum): An open source blackbox scanner for detecting web vulnerabilities," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 12, pp. 411–417, 2017.

[9] N. F. Awang and A. A. Manaf, "Automated security testing framework for detecting sql injection vulnerability in web application," in *International Conference on Global Security*, H. Jahankhani, A. Carlile, B. Akhgar, A. Taal, A. G. Hessami, and A. Hosseinian-Far, Eds. Springer International Publishing, 2015, Conference Proceedings, pp. 160–171.

[10] A. Ciampa, C. A. Visaggio, and M. D. Penta, "A heuristic-based approach for detecting sql-injection vulnerabilities in web applications," in *Pro. of the 2010 ICSE Workshop on Software Engineering for Secure Systems*. ACM, 2010, Conference Proceedings, pp. 43–49.

[11] O. Olivo, I. Dillig, and C. Lin, "Detecting and exploiting second order denial-of-service vulnerabilities in web applications," in *Proc. of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, Conference Paper, pp. 616–628.

[12] M. K. Gupta, M. C. Govil, G. Singh, and P. Sharma, "Xssdm: Towards detection and mitigation of cross-site scripting vulnerabilities in web applications," in *Proc. of the 2015 International Conference on Advances in Computing, Communications and Informatics*, 2015, Conference Proceedings, pp. 2010–2015. [Online]. Available: https://ieeexplore.ieee.org/ielx7/7259950/7275573/07275912.pdf?tp=&arnumber=7275912&isnumber=7275573

[13] S. Gupta, B. B. Gupta, and P. Chaudhary, "Hunting for dom-based xss vulnerabilities in mobile cloud-based online social network," *Future Generation Computer Systems*, vol. 79, pp. 319–336, 2018.

[14] B. Eshete, A. Villafiorita, K. Weldemariam, and M. Zulkernine, "Confeagle: Automated analysis of configuration vulnerabilities in web applications," in *Proc. of the IEEE 7th International Conference on Software Security and Reliability*, 2013, Conference Paper, pp. 188–197. [Online]. Available: https://ieeexplore.ieee.org/ielx7/6570841/6571676/06571709.pdf?tp=&arnumber=6571709&isnumber=6571676

[15] R. Akrout, E. Alata, M. Kaaniche, and V. Nicomette, "An automated black box approach for web vulnerability identification and attack scenario generation," *Journal of the Brazilian Computer Society*, vol. 20, no. 1, p. 4, 2014. [Online]. Available: https://doi.org/10.1186/1678-4804-20-4

[16] I. Medeiros, N. Neves, and M. Correia, "Dekant: a static analysis tool that learns to detect web application vulnerabilities," in *Proc. of the 25th International Symposium on Software Testing and Analysis*. ACM, 2016, Conference Paper, pp. 1–11.

[17] T. Jensen, H. Pedersen, M. C. Olesen, and R. R. Hansen, "Thaps: Automated vulnerability scanning of php applications," in *Nordic Conference on Secure IT Systems*, A. Jøsang and B. Carlsson, Eds. Springer Berlin Heidelberg, 2012, Conference Proceedings, pp. 31–46.

[18] M. Monga, R. Paleari, and E. Passerini, "A hybrid analysis framework for detecting web application vulnerabilities," in *Proc. of the 2009 ICSE Workshop on Software Engineering for Secure Systems*. IEEE Computer Society, 2009, Conference Paper, pp. 25–32. [Online]. Available: https://ieeexplore.ieee.org/ielx5/5054533/5068439/05068455.pdf?tp=&arnumber=5068455&isnumber=5068439

[19] G. Wassermann and Z. Su, "Static detection of cross-site scripting vulnerabilities," in *Proc. of the ACM/IEEE 30th international conference on Software engineering*. ACM, 2008, Conference Paper, pp. 171–180.

[20] L. K. Shar, L. C. Briand, and H. B. K. Tan, "Web application vulnerability prediction using hybrid program analysis and machine learning," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 6, pp. 688–707, 2015. [Online]. Available: https://ieeexplore.ieee.org/ielx7/8858/7322332/06963442.pdf?tp=&arnumber=6963442&isnumber=7322332

[21] Y. H. Zheng and X. Y. Zhang, "Path sensitive static analysis of web applications for remote code execution vulnerability detection," in *Proc. of the 35th ACM/IEEE International Conference on Software Engineering*, 2013, Conference Proceedings, pp. 652–661.

[22] S. Gupta and B. B. Gupta, "Enhanced xss defensive framework for web applications deployed in the virtual machines of cloud computing environment," *Procedia Technology*, vol. 24, pp. 1595–1602, 2016.

[23] G. Shashank and B. B. Gupta, "Php-sensor: A prototype method to discover workflow violation and xss vulnerabilities in php web applications," in *Proceedings of the 12th ACM International Conference on Computing Frontiers*, ser. CF '15. New York, NY, USA: ACM, 2015. [Online]. Available: https://doi.org/10.1145/2742854.2745719

[24] J. Dahse and R.-U. B. Thorsten Holz, "Static detection of second-order vulnerabilities in web applications," in *Proc. of the 23rd USENIX Security Symposium.*, 2014, Conference Proceedings.

[25] J. Dahse, "Simulation of built-in php features for precise static code analysis," in *Annual Network and Distributed System Security Symposium (NDSS)*, 2014, Conference Paper.

[26] X. Li and Y. Xue, "Block: a black-box approach for detection of state violation attacks towards web applications," in *Proc. of the 27th Annual Computer Security Applications Conference*. ACM, 2011, Conference Paper, pp. 247–256.

[27] F. Yu, M. Alkhalaf, T. Bultan, and O. H. Ibarra, "Automata-based symbolic string analysis for vulnerability detection," *Formal Methods in System Design*, vol. 44, no. 1, pp. 44–70, 2014. [Online]. Available: https://doi.org/10.1007/s10703-013-0189-1

[28] A. Kiezun, P. J. Guo, K. Jayaraman, and M. D. Ernst, "Automatic creation of sql injection and cross-site scripting attacks," in *Proc. of the 31st International Conference on Software Engineering*, 2009, Conference Proceedings, p. 199. [Online]. Available: https://ieeexplore.ieee.org/ielx5/5062304/5070493/05070521.pdf?tp=&arnumber=5070521&isnumber=5070493

[29] L. K. Shar and H. B. K. Tan, "Predicting sql injection and cross site scripting vulnerabilities through mining input sanitization patterns," *Information and Software Technology*, vol. 55, no. 10, pp. 1767–1780, 2013.

[30] X. Li and Y. Xue, "Logicscope: automatic discovery of logic vulnerabilities within web applications," in *Proc. of the 8th ACM SIGSAC*

symposium on Information, computer and communications security. ACM, 2013, Conference Paper, pp. 481–486.

[31] V. S. Sooel Son, Kathryn S. Mckinley, "Fix me up: Repairing access-control bugs in web applications," *In Network and Distributed System Security Symposium*, 2013.

[32] F. S. L. X. Z. Su, "Static detection of access control vulnerabilities in web applications," *20th USENIX Security Symposium*, 2011.

[33] S. Son and V. Shmatikov, "Saferphp: Finding semantic vulnerabilities in php applications," in *Proc. of the ACM SIGPLAN 6th Workshop on Programming Languages and Analysis for Security*. New York, NY, USA: ACM, 2011. [Online]. Available: https://doi.org/10.1145/2166956.2166964

[34] X. Li, W. Yan, and Y. Xue, "Sentinel: securing database from logic flaws in web applications," in *Proc. of the 2nd ACM conference on Data and Application Security and Privacy*. ACM, 2012, Conference Paper, pp. 25–36.

[35] A. Møller and M. Schwarz, "Automated detection of client-state manipulation vulnerabilities," in *Proc. of the 34th International Conference on Software Engineering*, 2012, Conference Proceedings, pp. 749–759. [Online]. Available: https://ieeexplore.ieee.org/ielx5/6218989/6227015/06227143.pdf?tp=&arnumber=6227143&isnumber=6227015

[36] W. G. J. Halfond, A. Orso, and P. Manolios, "Wasp: Protecting web applications using positive tainting and syntax-aware evaluation," *IEEE Transactions on Software Engineering*, vol. 34, no. 1, pp. 65–81, 2008. [Online]. Available: https://ieeexplore.ieee.org/ielx5/32/4444339/04359474.pdf?tp=&arnumber=4359474&isnumber=4444339

[37] G. Deepa, P. S. Thilagam, A. Praseed, and A. R. Pais, "Detlogic: A black-box approach for detecting logic vulnerabilities in web applications," *Journal of Network and Computer Applications*, vol. 109, pp. 89–109, 2018.

[38] G. Deepa, P. S. Thilagam, F. A. Khan, A. Praseed, A. R. Pais, and N. Palsetia, "Black-box detection of xquery injection and parameter tampering vulnerabilities in web applications," *International Journal of Information Security*, vol. 17, no. 1, pp. 105–120, 2018. [Online]. Available: https://link.springer.com/content/pdf/10.1007%2Fs10207-016-0359-4.pdf

[39] L. K. Shar and F. B. K. Tan, "Automated removal of cross site scripting vulnerabilities in web applications," *Information and Software Technology*, vol. 54, no. 5, pp. 467–478, 2012.

[40] L. K. Shar and H. B. K. Tan, "Auditing the xss defence features implemented in web application programs," *IET Software*, vol. 6, no. 4, pp. 377–390, 2012. [Online]. Available: https://ieeexplore.ieee.org/ielx5/4124007/6322849/06322860.pdf?tp=&arnumber=6322860&isnumber=6322849

[41] P. Bisht, P. Madhusudan, and V. N. Venkatakrishnan, "Candid: Dynamic candidate evaluations for automatic prevention of sql injection attacks," *ACM Transactions on Information and System Security*, vol. 13, no. 2, 2010.

[42] L. M. S. Martin M, "Automatic generation of xss and sql injection attacks with goal-directed model checking," in *Proc. of the 17th conference on Security symposium*, 2008, Conference Proceedings, pp. 31–43.

[43] M. Alkhalaf, S. R. Choudhary, M. Fazzini, T. Bultan, A. Orso, and C. Kruegel, "Viewpoints: differential string analysis for discovering client- and server-side input validation inconsistencies," in *Proc. of the 2012 International Symposium on Software Testing and Analysis*. ACM, 2012, Conference Paper, pp. 56–66.

[44] Q. Binbin, L. Beihai, J. Sheng, and Y. Chutian, "Design of automatic vulnerability detection system for web application program," in *Proc. of the IEEE 4th International Conference on Software Engineering and Service Science*, 2013, Conference Proceedings, pp. 89–92.

[45] M.-T. Trinh, D.-H. Chu, and J. Jaffar, "S3: A symbolic string solver for vulnerability detection in web applications," in *Proc. of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, Conference Paper, pp. 1232–1243.

[46] Y.-S. Jang and J.-Y. Choi, "Detecting sql injection attacks using query result size," *Computers Security*, vol. 44, pp. 104–118, 2014.

[47] L. Lei, X. Jing, L. Minglei, and Y. Jufeng, "A dynamic sql injection vulnerability test case generation model based on the multiple phases detection approach," in *Proc. of the IEEE 37th Annual Computer Software and Applications Conference*, 2013, Conference Proceedings, pp. 256–261. [Online]. Available: https://ieeexplore.ieee.org/ielx7/6605717/6649781/06649829.pdf?tp=&arnumber=6649829&isnumber=6649781

[48] H. He, L. L. Chen, and W. P. Guo, "Research on web application vulnerability scanning system based on fingerprint feature," in *Proc. of the 2017 International Conference on Mechanical, Electronic, Control and Automation Engineering*, vol. 61, 2017, Conference Proceedings, pp. 150–155.

[49] V.-G. Le, H.-T. Nguyen, D.-N. Lu, and N.-H. Nguyen, "A solution for automatically malicious web shell and web application vulnerability detection," in *International Conference on Computational Collective Intelligence*, N.-T. Nguyen, L. Iliadis, Y. Manolopoulos, and B. Trawiński, Eds. Springer International Publishing, 2016, Conference Proceedings, pp. 367–378.

[50] H. Shahriar and H. Haddad, "Object injection vulnerability discovery based on latent semantic indexing," in *Proc. of the 31st Annual ACM Symposium on Applied Computing*. ACM, 2016, Conference Paper, pp. 801–807.

[51] V. Felmetsger, L. Cavedon, C. Kruegel, and G. Vigna, "Toward automated detection of logic vulnerabilities in web applications," in *Proc. of the 19th USENIX conference on Security*. 1929834: USENIX Association, 2010, Conference Paper, pp. 10–10.

[52] B. D. Pellegrino G, "Toward black-box detection of logic flaws in web applications," in *Annual Network Distributed System Security Symposium (NDSS)*, 2014, Conference Proceedings.

[53] D. Kavitha, S. Chandrasekaran, and S. K. Rani, "Hdtcv: Hybrid detection technique for clickjacking vulnerability," *Advances in Intelligent Systems and Computing*, pp. 607–620, 2016.

[54] V. Sunkari and C. V. G. Rao, "Preventing input type validation vulnerabilities using network based intrusion detection systems," in *Proc. of the 2014 International Conference on Contemporary Computing and Informatics*, 2014, Conference Proceedings, pp. 702–706. [Online]. Available: https://ieeexplore.ieee.org/ielx7/7005967/7019573/07019679.pdf?tp=&arnumber=7019679&isnumber=7019573

[55] L. Lei, X. Jing, G. Chenkai, K. Jiehui, X. Sihan, and Z. Biao, "Exposing sql injection vulnerability through penetration test based on finite state machine," in *Proc. of the 2nd IEEE International Conference on Computer and Communications*, 2016, Conference Proceedings, pp. 1171–1175. [Online]. Available: https://ieeexplore.ieee.org/ielx7/7916867/7924647/07924889.pdf?tp=&arnumber=7924889&isnumber=7924647

[56] L. Liu, J. Xu, H. Yang, C. Guo, J. Kang, S. Xu, B. Zhang, and G. Si, "An effective penetration test approach based on feature matrix for exposing sql injection vulnerability," in *Proc. of the IEEE 40th Annual Computer Software and Applications Conference*, vol. 1, 2016, Conference Proceedings, pp. 123–132. [Online]. Available: https://ieeexplore.ieee.org/ielx7/7551592/7551973/07552000.pdf?tp=&arnumber=7552000&isnumber=7551973

[57] M. E. Ruse and S. Basu, "Detecting cross-site scripting vulnerability using concolic testing," in *Proc. of the 10th International Conference on Information Technology: New Generations*, 2013, Conference Proceedings, pp. 633–638.

[58] T. Scholte, W. Robertson, D. Balzarotti, and E. Kirda, "Preventing input validation vulnerabilities in web applications through automated type analysis," in *Proc. of the IEEE 36th Annual Computer Software and Applications Conference*, 2012, Conference Proceedings, pp. 233–243. [Online]. Available: https://ieeexplore.ieee.org/ielx5/6340121/6340122/06340148.pdf?tp=&arnumber=6340148&isnumber=6340122

[59] I. Lee, S. Jeong, S. Yeo, and J. Moon, "A novel method for sql injection attack detection based on removing sql query attribute values," *Mathematical and Computer Modelling*, vol. 55, no. 1, pp. 58–68, 2012.

[60] X. Li, X. Si, and Y. Xue, "Automated black-box detection of access control vulnerabilities in web applications," in *Proc. of the 4th ACM conference on Data and application security and privacy*. ACM, 2014, Conference Paper, pp. 49–60.

[61] K. H. Zhang, Z. Li, R. Wang, X. F. Wang, and S. Chen, "Sidebuster: Automated detection and quantification of side-channel leaks in web application development," in *Proc. of the 17th ACM Conference on Computer and Communications Security*, 2010, Conference Proceedings, pp. 595–606.

[62] P. Chapman and D. Evans, "Automated black-box detection of side-channel vulnerabilities in web applications," in *Proc. of the 18th ACM conference on Computer and communications security*. 2046737: ACM, 2011, Conference Paper, pp. 263–274.

[63] M. Monshizadeh, P. Naldurg, and V. N. Venkatakrishnan, "Mace: Detecting privilege escalation vulnerabilities in web applications,"

in *Proc. of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, Conference Paper, pp. 690–701.

[64] A. Avancini and M. Ceccato, “Comparison and integration of genetic algorithms and dynamic symbolic execution for security testing of cross-site scripting vulnerabilities,” *Information and Software Technology*, vol. 55, no. 12, pp. 2209–2222, 2013.

[65] L. K. Shar, H. B. K. Tan, and L. C. Briand, “Mining sql injection and cross site scripting vulnerabilities using hybrid program analysis,” in *Proc. of the 35th ACM/IEEE International Conference on Software Engineering*, 2013, Conference Proceedings, pp. 642–651. [Online]. Available: https://ieeexplore.ieee.org/ielx7/6596173/6606539/06606610.pdf?tp=&arnumber=6606610&isnumber=6606539&ref=

[66] A. Doupe, B. Boe, C. Kruegel, and G. Vigna, “Fear the ear: Discovering and mitigating execution after redirect vulnerabilities,” in *Proc. of the 18th ACM Conference on Computer Communications Security*, 2011, Conference Proceedings, pp. 251–261.

[67] P. Bisht, T. Hinrichs, N. Skrupsky, and V. N. Venkatakrishnan, “Waptec: Whitebox analysis of web applications for parameter tampering exploit construction,” in *Proc. of the 18th ACM Conference on Computer Communications Security*, 2011, Conference Proceedings, pp. 575–586.

[68] N. Antunes and M. Vieira, “Designing vulnerability testing tools for web services: approach, components, and tools,” *International Journal of Information Security*, vol. 16, no. 4, pp. 435–457, 2017. [Online]. Available: https://link.springer.com/content/pdf/10.1007%2Fs10207-016-0334-0.pdf

[69] X. Guo, S. Jin, and Y. Zhang, “Xss vulnerability detection using optimized attack vector repertory,” in *Proc. of the 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, 2015, Conference Proceedings, pp. 29–36. [Online]. Available: https://ieeexplore.ieee.org/ielx7/7307709/7307766/07307783.pdf?tp=&arnumber=7307783&isnumber=7307766

[70] Z. Djuric, “A black-box testing tool for detecting sql injection vulnerabilities,” in *Proc. of the 2nd International Conference on Informatics Applications*, 2013, Conference Proceedings, pp. 216–221. [Online]. Available: https://ieeexplore.ieee.org/ielx7/6634597/6650219/06650259.pdf?tp=&arnumber=6650259&isnumber=6650219

[71] A. K. Singh and S. Roy, “A network based vulnerability scanner for detecting sqli attacks in web applications,” in *Proc. of the 1st International Conference on Recent Advances in Information Technology*, 2012, Conference Proceedings, pp. 585–590. [Online]. Available: https://ieeexplore.ieee.org/ielx5/6188804/6194433/06194594.pdf?tp=&arnumber=6194594&isnumber=6194433

[72] V. Shanmughaneethi, R. Y. Pravin, C. E. Shyni, and S. Swamynathan, “Sqlivd - aop: Preventing sql injection vulnerabilities using aspect oriented programming through web services,” *High Performance Architecture and Grid Computing*, vol. 169, pp. 327–337, 2011.

[73] W. Haiyan, G. Guozhu, and M. chunyu, “Test sql injection vulnerabilities in web applications based on structure matching,” in *Proc. of 2011 International Conference on Computer Science and Network Technology*, vol. 2, 2011, Conference Proceedings, pp. 935–938. [Online]. Available: https://ieeexplore.ieee.org/ielx5/6175418/6182035/06182115.pdf?tp=&arnumber=6182115&isnumber=6182035

[74] L. Zhang, Q. Gu, S. Peng, X. Chen, H. Zhao, and D. Chen, “D-wav: A web application vulnerabilities detection tool using characteristics of web forms,” in *Proc. of the 5th International Conference on Software Engineering Advances*, 2010, Conference Proceedings, pp. 501–507. [Online]. Available: https://ieeexplore.ieee.org/ielx5/5613991/5614909/05615484.pdf?tp=&arnumber=5615484&isnumber=5614909

[75] 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.

[76] J. M. Chen and C. L. Wu, “An automated vulnerability scanner for injection attack based on injection point,” in *Proc. of the 2010 International Computer Symposium*, 2010, Conference Proceedings, pp. 113–118. [Online]. Available: https://ieeexplore.ieee.org/ielx5/5678855/5685355/05685537.pdf?tp=&arnumber=5685537&isnumber=5685355

[77] D. B. E. K. Marco Balduzzi, Carmen Torrano Gimenez, “Automated discovery of parameter pollution vulnerabilities in web applications,” in *Annual Network Distributed System Security Symposium (NDSS)*, 2011, Conference Proceedings.

[78] P. Bisht, T. Hinrichs, N. Skrupsky, R. Bobrowicz, and V. N. Venkatakrishnan, “Notamper: Automatic blackbox detection of parameter tampering opportunities in web applications,” in *Proc. of the 17th ACM Conference on Computer and Communications Security*, 2010, Conference Proceedings, pp. 607–618.

[79] D. Balzarotti, M. Cova, V. Felmetsger, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna, “Saner: Composing static and dynamic analysis to validate sanitization in web applications,” in *Proc. of the 2008 IEEE Symposium on Security and Privacy*, 2008, Conference Proceedings, pp. 387–401. [Online]. Available: https://ieeexplore.ieee.org/ielx5/4531131/4531132/04531166.pdf?tp=&arnumber=4531166&isnumber=4531132

[80] N. Antunes and M. Vieira, “Enhancing penetration testing with attack signatures and interface monitoring for the detection of injection vulnerabilities in web services,” in *Proc. of the 2011 IEEE International Conference on Services Computing*, 2011, Conference Paper.

[81] Y. Zheng, X. Zhang, and V. Ganesh, “Z3-str: a z3-based string solver for web application analysis,” in *Proc. of the 9th Joint Meeting on Foundations of Software Engineering*, 2013, Conference Proceedings, p. 114.

[82] H. Asghar, Z. Anwar, and K. Latif, “A deliberately insecure rdf-based semantic web application framework for teaching sparql/sparul injection attacks and defense mechanisms,” *Computers Security*, vol. 58, pp. 63–82, 2016.

[83] M. A. Ahmed and F. Ali, “Multiple-path testing for cross site scripting using genetic algorithms,” *Journal of Systems Architecture*, vol. 64, pp. 50–62, 2016.

[84] N. Patel and N. Shekokar, “Implementation of pattern matching algorithm to defend sqlia,” *Procedia Computer Science*, vol. 45, pp. 453–459, 2015.

[85] A. Liu, Y. Yuan, D. Wijesekera, and A. Stavrou, “Sqlprob: A proxy-based architecture towards preventing sql injection attacks,” in *Proc. of the ACM Symposium on Applied Computing, SAC 2009*, 2009, Conference Paper.

[86] P. Zech, M. Felderer, and R. Breu, “Knowledge-based security testing of web applications by logic programming,” *International Journal on Software Tools for Technology Transfer*, vol. 21, no. 2, pp. 221–246, 2019. [Online]. Available: https://link.springer.com/content/pdf/10.1007%2Fs10009-017-0472-3.pdf

[87] M. N. Khalid, H. Farooq, M. Iqbal, M. T. Alam, and K. Rasheed, “Predicting web vulnerabilities in web applications based on machine learning,” in *Intelligent Technologies and Applications, Intap 2018*, vol. 932, 2018, Conference Proceedings, pp. 473–484.

[88] I. Medeiros, M. Beatriz, N. Neves, and M. Correia, “Septic: Detecting injection attacks and vulnerabilities inside the dbms,” *IEEE Transactions on Reliability*, pp. 1–21, 2019. [Online]. Available: https://ieeexplore.ieee.org/ielx7/24/4378406/08672505.pdf?tp=&arnumber=8672505&isnumber=4378406&ref=

[89] D. Ying, Z. Yuqing, M. Hua, W. Qianru, L. Qixu, W. Kai, and W. Wenjie, “An adaptive system for detecting malicious queries in web attacks,” *Science China (Information Sciences)*, 2018.

[90] J. Thom, x00E, L. K. Shar, D. Bianculli, and L. Briand, “An integrated approach for effective injection vulnerability analysis of web applications through security slicing and hybrid constraint solving,” *IEEE Transactions on Software Engineering*, pp. 1–1, 2018. [Online]. Available: https://ieeexplore.ieee.org/ielx7/32/4359463/08373739.pdf?tp=&arnumber=8373739&isnumber=4359463&ref=

[91] G. Shashank and B. G. B., “Xss-secure as a service for the platforms of online social network-based multimedia web applications in cloud,” *Multimedia Tools and Applications*, 2018.

[92] V. Patil, P. Thakkar, C. Shah, T. Bhat, and S. P. Godse, “Detection and prevention of phishing websites using machine learning approach,” in *Proc. of the 4th International Conference on Computing Communication Control and Automation*, 2018, Conference Proceedings, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/ielx7/8681925/8697217/08697412.pdf?tp=&arnumber=8697412&isnumber=8697217&ref=

[93] A. Kurniawan, B. S. Abbas, A. Trisetyarso, and S. M. Isa, “Static taint analysis traversal with object oriented component for web file injection vulnerability pattern detection,” *Procedia Computer Science*, vol. 135, pp. 596–605, 2018.

[94] M. K. Gupta, M. C. Govil, and G. Singh, “Text-mining and pattern-matching based prediction models for detecting vulnerable files in web applications,” *Journal of Web Engineering*, vol. 17, no. 1-2, pp. 28–44, 2018.

[95] P. Li, L. Liu, J. Xu, H. Yang, L. Yuan, C. Guo, and X. Ji, “Application of hidden markov model in sql injection detection,” in *Proc. of the*

IEEE 41st Annual Computer Software and Applications Conference, 2017, Conference Proceedings, pp. 578–583.

[96] D. Kar, S. Panigrahi, and S. Sundararajan, "Sqlidds: Sql injection detection using document similarity measure," *Journal of Computer Security*, vol. 24, no. 4, pp. 507–539, 2016.

[97] N. M. Vithanage and N. Jeyamohan, "Webguardia - an integrated penetration testing system to detect web application vulnerabilities," in *Proc. of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking*, 2016, Conference Proceedings, pp. 221–227.

[98] S. Anil, S. G. Manoj, L. Vijay, and C. Mauro, "You click, i steal: analyzing and detecting click hijacking attacks in web pages," *International Journal of Information Security*, 2018.

[99] G. Agosta, A. Barenghi, A. Parata, and G. Pelosi, "Automated security analysis of dynamic web applications through symbolic code execution," in *Proc. of the Ninth International Conference on Information Technology - New Generations*, 2012, Conference Paper, pp. 189–194.

[100] Y. Zhong, H. Asakura, H. Takakura, and Y. Oshima, "Detecting malicious inputs of web application parameters using character class sequences," in *Proc. of the IEEE 39th Annual International Computers, Software Applications Conference*, 2015, Conference Proceedings, pp. 525–532.

[101] H. Shahriar, V. K. Devendran, and H. Haddad, "Proclick: a framework for testing clickjacking attacks in web applications," in *Proc. of the 6th International Conference on Security of Information and Networks*. ACM, 2013, Conference Paper, pp. 144–151.

[102] M. Ceccato, C. D. Nguyen, D. Appelt, and L. C. Briand, "Sofia: an automated security oracle for black-box testing of sql-injection vulnerabilities," in *Proc. of the 31st IEEE/ACM International Conference on Automated Software Engineering*. 2970343: ACM, 2016, Conference Paper, pp. 167–177.

[103] S. Gupta and B. B. Gupta, "Xss-safe: A server-side approach to detect and mitigate cross-site scripting (xss) attacks in javascript code," *Arabian Journal for Science and Engineering*, vol. 41, no. 3, pp. 897–920, 2015.

[104] L. Zhang, D. Zhang, C. Wang, J. Zhao, and Z. Zhang, "Art4sqli: The art of sql injection vulnerability discovery," *IEEE Transactions on Reliability*, pp. 1–20, 2019. [Online]. Available: https://ieeexplore.ieee.org/ielx7/24/4378406/08716725.pdf?tp=&arnumber=8716725&isnumber=4378406&ref=

[105] D. E. Simos, J. Zivanovic, and M. Leithner, "Automated combinatorial testing for detecting sql vulnerabilities in web applications," in *Proc. of the IEEE/ACM 14th International Workshop on Automation of Software Test*, 2019, pp. 55–61.

[106] W. Ze, "Design and implementation of core modules of web application vulnerability detection model," in *Proc. of the 11th International Conference on Measuring Technology and Mechatronics Automation*, 2019, pp. 10–14.

[107] F. M. M. Mokbal, W. Dan, A. Imran, L. Jiuchuan, F. Akhtar, and W. Xiaoxi, "Mlpxss: An integrated xss-based attack detection scheme in web applications using multilayer perceptron technique," *IEEE Access*, vol. 7, pp. 100 567–100 580, 2019.

[108] I. Jana and A. Oprea, "Appmine: Behavioral analytics for web application vulnerability detection," in *Proc. of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop*. New York, NY, USA: ACM, 2019, p. 69–80. [Online]. Available: https://doi.org/10.1145/3338466.3358923

[109] C. Lv, L. Zhang, F. Zeng, and J. Zhang, "Adaptive random testing for xss vulnerability," in *Proc. of the 26th Asia-Pacific Software Engineering Conference*, 2019, pp. 63–69.

[110] H. Gu, J. Zhang, T. Liu, M. Hu, J. Zhou, T. Wei, and M. Chen, "Diava: A traffic-based framework for detection of sql injection attacks and vulnerability analysis of leaked data," *IEEE Transactions on Reliability*, vol. 69, no. 1, pp. 188–202, 2020.

[111] Y. Pan, F. Sun, Z. Teng, J. White, D. C. Schmidt, J. Staples, and L. Krause, "Detecting web attacks with end-to-end deep learning," *Journal of Internet Services and Applications*, vol. 10, no. 1, p. 16, Aug 2019. [Online]. Available: https://doi.org/10.1186/s13174-019-0115-x

[112] R. Padmanaban, M. Thirumaran, V. Sanjana, and A. Moshika, "Security analytics for heterogeneous web," in *Proc. of the 2019 IEEE International Conference on System, Computation, Automation and Networking*, 2019, pp. 1–6.

[113] S. Calzavara, M. Conti, R. Focardi, A. Rabitti, and G. Tolomei, "Machine learning for web vulnerability detection: The case of cross-site request forgery," *IEEE Security and Privacy*, vol. 18, no. 3, pp. 8–16, 2020.

[114] C. Liu, J. Yang, and J. Wu, "Web intrusion detection system combined with feature analysis and svm optimization," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, p. 33, Feb 2020. [Online]. Available: https://doi.org/10.1186/s13638-019-1591-1

[115] S. Jan, A. Panichella, A. Arcuri, and L. Briand, "Search-based multi-vulnerability testing of xml injections in web applications," *Empirical Software Engineering*, vol. 24, no. 6, pp. 3696–3729, Dec 2019. [Online]. Available: https://doi.org/10.1007/s10664-019-09707-8

[116] D. M. Stallenberg and A. Panichella, "Jcomix: A search-based tool to detect xml injection vulnerabilities in web applications," in *Proc. of the 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. New York, NY, USA: ACM, 2019, p. 1090–1094. [Online]. Available: https://doi.org/10.1145/3338906.3341178

[117] I. Medeiros, M. Beatriz, N. Neves, and M. Correia, "Septic: Detecting injection attacks and vulnerabilities inside the dbms," *IEEE Transactions on Reliability*, vol. 68, no. 3, pp. 1168–1188, 2019.

[118] M. S. Aliero, I. Ghani, K. N. Qureshi, and M. F. Rohani, "An algorithm for detecting sql injection vulnerability using black-box testing," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 1, pp. 249–266, Jan 2020. [Online]. Available: https://doi.org/10.1007/s12652-019-01235-z

[119] Y. Fang, C. Huang, Y. Xu, and Y. Li, "Rlxss: Optimizing xss detection model to defend against adversarial attacks based on reinforcement learning," *Future Internet*, vol. 11, no. 8, p. 177, Aug 2019. [Online]. Available: http://dx.doi.org/10.3390/fi11080177

[120] D.-P. P. V.-O. P. N.-H. N. Van-Giap Le, Huu-Tung Nguyen, "Guruws: A hybrid platform for detecting malicious web shells and web application vulnerabilities," in *Transactions on Computational Collective Intelligence XXXII, Lecture Notes in Computer Science, vol 11370*. Springer, Berlin, Heidelberg, 2019. [Online]. Available: https://doi.org/10.1007/978-3-662-58611-2_5

[121] H. Y. Y. G. Ning Guo, Xiaoyong Li, "Vulhunter: An automated vulnerability detection system based on deep learning and bytecode," in *Proc. of the 2019 Information and Communications Security Conference. Lecture Notes in Computer Science, vol 11999*. Springer, Cham, 2019, pp. 199–218. [Online]. Available: https://doi.org/10.1007/978-3-030-41579-2_12

[122] C. H. J. B. Katherine Hough, Gebrehiwet Biyane Welearegai, "Revealing injection vulnerabilities by leveraging existing tests," in *Proc. of the 2020 ACM/IEEE International Conference on Software Engineering*. ACM, 2020.

[123] F. Spoto, E. Burato, M. D. Ernst, P. Ferrara, A. Lovato, D. Macedonio, and C. Spiridon, "Static identification of injection attacks in java," *ACM Trans. Program. Lang. Syst.*, vol. 41, no. 3, Jul. 2019.