algorithms in automated web security testing through a comparative analysis of the results generated by our proposed approach.

However, it is essential to acknowledge that while genetic algorithms can aid in detecting SQL injection vulnerabilities, they should not be relied upon as the sole defense mechanism. Best practices such as input validation, parameterized queries, and secure coding practices must also be implemented to effectively mitigate the risk of SQL injection attacks. The combination of these approaches ensures a robust and comprehensive web security strategy.

REFERENCES

[1] OWASP Top Ten Web Application Security Risks | OWASP, 2020. OWASP Top Ten page available online at https://owasp.org/www-project-top-ten/ (Access Date 17-05-2020).

[2] Appelt, D., Alshahwan, N. and Briand, L., 2013. Assessing the impact of firewalls and database proxies on sql injection testing, International Workshop on Future Internet Testing, pp. 32–47.

[3] Appelt, D., Nguyen, C.D., Briand, L.C. and Alshahwan, N., 2014. Automated testing for SQL injection vulnerabilities: an input mutation approach, Proceedings of the 2014 International Symposium on Software Testing and Analysis, pp. 259–269.

[4] Ceccato, M., Nguyen, C.D., Appelt, D. and Briand, L.C., 2016. SOFIA: An automated security oracle for black-box testing of SQL-injection vulnerabilities, 2016 31st IEEE/ACM International Conference on Automated Software Engineering (ASE), pp. 167–177.

[5] Fonseca, J., Vieira, M. and Madeira, H., 2013. Evaluation of web security mechanisms using vulnerability & attack injection. IEEE Transactions on dependable and secure computing, 11: 440–453.

[6] Skaruz, J. and Seredynski, F., 2009. Detecting web application attacks with use of Gene Expression Programming, 2009 IEEE Congress on Evolutionary Computation, pp. 2029–2035.

[7] Hlaing, Z.C.S.S. and Khaing, M., 2020. A Detection and Prevention Technique on SQL Injection Attacks, 2020 IEEE Conference on Computer Applications (ICCA), pp. 1–6.

[8] Priyadarshini, R., Jagadiswaree, D., Fareedha, A. and Janarthanan, M., 2011. A cross platform intrusion detection system using inter server communication technique, 2011 International Conference on Recent Trends in Information Technology (ICRTIT), pp. 1259–1264.

[9] Chandrasekhar, A.M. and Raghuveer, K., 2013. Intrusion detection technique by using k-means, fuzzy neural network and SVM classifiers, 2013 International Conference on Computer Communication and Informatics, pp. 1–7.

[10] Ross, K., Moh, M., Moh, T.-S. and Yao, J., 2017. Poster: Multi-source data analysis for SQL injection detection, 38th IEEE Symposium on Security and Privacy (IEEE S&P), San Jo-se, CA.

[11] Dharam, R. and Shiva, S.G., 2012. Runtime monitors for tautology based SQL injection attacks, Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp. 253–258.

[12] Dharam, R. and Shiva, S.G., 2013. Runtime monitors to detect and prevent union query based SQL injection attacks, 2013 10th International Conference on Information Technology: New Generations, pp. 357–362.

[13] Deb, K., 1998. Genetic algorithm in search and optimization: the technique and applications, Proceedings of international workshop on soft computing and intelligent systems, pp. 58–87.

[14] Angelo Ciampa, C. A. (2010). A heuristic-based approach for detecting SQL-injection vulnerabilities in web applications. SESS '10: Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems, 43-49.

[15] Mohd Ehmer Khan, F. K. (2012). A Comparative Study of White Box, Black Box and Grey Box Testing Techniques. International Journal of Advanced Computer Science and Applications(IJACSA), 3(6).