REFERENCES

Bergstra, J., & Bengio, Y. (2012). Random Search for Hyper-Parameter Optimization. *Journal of Machine Learning Research*, 13, 281-305.

Bishop, C. (2006). Pattern recognition and machine learning. *Springer google schola*, *2*, 5-43.

Brown, C., & Green, D. (2021). Financial implications of cybersecurity breaches in organizations. *Journal of Financial Management*, 49(4), 789-806.

Confido, A., Ntagiou, E. V., & Wallum, M. (2022). *Reinforcing Penetration Testing Using AI*. In 2022 IEEE Aerospace Conference (AERO). IEEE.

Curphey, M., & Araujo, R. (2020). XSS vulnerabilities in e-commerce platforms: A case study. *Journal of Cybersecurity and Privacy*, 1(1), 15-27.

Cvitkovic, M., Singh, B., & Anandkumar, A. (2018). Deep learning on code with an unbounded vocabulary. In *Machine Learning for Programming (ML4P) Workshop at Federated Logic Conference (FLoC)*.

Dahse, J., & Holz, T. (2014). *Static Detection of Second-Order Vulnerabilities in Web Applications*. In Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14).

Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2019). *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding*. NAACL HLT 2019.

Feng, Z., Guo, D., Tang, D., Duan, N., Feng, X., Gong, M., ... & Zhou, M. (2020). Codebert: A pre-trained model for programming and natural languages. *arXiv preprint arXiv:2002.08155*.

Fogie, S., Grossman, J., Hansen, R., Rager, A., & Petkov, P. D. (2007*). XSS Attacks: Cross Site Scripting Exploits and Defense*. Syngress Publishing.

Goswami, S., et al. (2017). An unsupervised method for detection of XSS attack. *International Journal of Network Security*, 19(5), 761-775.

Guyon, I., & Elisseeff, A. (2003). An Introduction to Variable and Feature Selection. *Journal of Machine Learning Research*.

Halfond, W. G. J., Choudhary, S. R., & Orso, A. (2011). *Improving penetration testing through static and dynamic analysis*. Software Testing, Verification and Reliability, 21(3), 195-214.

Hansen, M. (2020). The impact of XSS attacks on user privacy and security. *Journal of Cybersecurity*, 6(1), 45-58.

Howard, J., & Ruder, S. (2018). *Universal Language Model Fine-tuning for Text Classification*. ACL 2018.

IBM Corporation. (2020). *IBM Security AppScan Standard*. Retrieved from IBM Security AppScan

Jones, R., & Gupta, S. (2021). Psychological effects of cyber attacks on individuals. *International Journal of Information Security*, 20(2), 231-240.

Jovanovic, N., Kruegel, C., & Kirda, E. (2006). *Pixy: A static analysis tool for detecting Web application vulnerabilities*. In Proceedings of the 2006 IEEE Symposium on Security and Privacy (SP '06).

Kirda, E., Kruegel, C., Vigna, G., & Jovanovic, N. (2006). *Noxes: A client-side solution for mitigating cross-site scripting attacks*. ACM Symposium on Applied Computing.

Le Goues, C., Dewey-Vogt, M., Forrest, S., & Weimer, W. (2019). *A Systematic Study of Automated Program Repair: Fixing 55 out of 105 bugs for $8 each*. In Proceedings of the 34th International Conference on Software Engineering (ICSE '12).

Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., Levy, O., Lewis, M., Zettlemoyer, L., & Stoyanov, V. (2019). *RoBERTa: A Robustly Optimized BERT Pretraining Approach*. arXiv preprint arXiv:1907.11692.

Martin, L., Nurse, J. R., & Erola, A. (2019). *The anatomy of web attacks: A comprehensive study of the exploitation of web vulnerabilities. Computers & Security*, 84, 93-108.

Mashhadi, E., & Hemmati, H. (2021, May). *Applying codebert for automated program repair of java simple bugs*. In 2021 IEEE/ACM 18th International Conference on Mining Software Repositories (MSR) (pp. 505-509). IEEE.

Maurel, H., Vidal, S., & Rezk, T. (2021). *Statically identifying XSS using deep learning*. [Online]. Available: https://gitlab.inria.fr/deep-learning-appliedon-web-and-iot-security/statically-identifying-xss-using-deep-learning

OWASP Foundation. (2013). *The OWASP Top Ten Project*.[Online].Available: https://owasp.org/www-project-top-ten/2013/

Pan, C., Lu, M., & Xu, B. (2021). *An empirical study on software defect prediction using CodeBERT model*. Applied Sciences, 11(11), 4793.

Pan, S. J., & Yang, Q. (2010). A Survey on Transfer Learning. *IEEE Transactions on Knowledge and Data Engineering*, *10*(22), 1345-1359.

Pellegrino, G., Balzarotti, D., & Winter, S. (2017). A view on current approaches for web security. *International Journal on Advances in Security*.

Probst, P., Wright, M. N., & Boulesteix, A. L. (2019). *Hyperparameters and Tuning Strategies for Random Forest*. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 9(3), e1301.

Rathore, S., Sharma, P. K., & Park, J. H. (2017). XSSClassifier: An efficient XSS attack detection approach based on machine learning classifier on SNSs. *Journal of Information Processing Systems*, 13(4).

Sarmah, U., Bhattacharyya, D. K., & Kalita, J. K. (2018). A survey of detection methods for XSS attacks. *Journal of Network and Computer Applications*, 118, 113-143.

Sasaki, Y. (2007). *The truth of the F-measure*. Teach tutor mater, *1*(5), 1-5.

Sennrich, R., Haddow, B., & Birch, A. (2016). *Neural Machine Translation of Rare Words with Subword Units*. Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (ACL 2016).

Shalev-Shwartz, S., & Ben-David, S. (2014). *Understanding machine learning: From theory to algorithms*. Cambridge university press.

Smith, A., & Johnson, B. (2020). Customer trust and loyalty in the aftermath of web application attacks. *Journal of Business Ethics*, 164(2), 305-318.

Smith, J. (2020). XSS attack on Twitter demonstrates potential security risks. *Journal of Information Security*, 11(2), 123-132.

Smith, L. N. (2017). *Cyclical Learning Rates for Training Neural Networks*. IEEE Winter Conference on Applications of Computer Vision (WACV).

Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. (2014). Dropout: A Simple Way to Prevent Neural Networks from Overfitting. *Journal of Machine Learning Research*, 15, 1929-1958.

Stepien, B., Peyton, L., & Xiong, P. (2012). *Using TTCN-3 as a modeling language for web penetration testing*. In 2012 IEEE International Conference on Industrial Technology. IEEE.

Tan, P. N., Steinbach, M., & Kumar, V. (2016). *Introduction to data mining*. Pearson Education India.

Wang, Q., Yang, H., Wu, G., Choo, K. K. R., Zhang, Z., Miao, G., & Ren, Y. (2022). *Black-box adversarial attacks on XSS attack detection model*. Computers & Security, 113, 102554.

Wang, Y.-H., Mao, C.-H., & Lee, H.-M. (2010). *Structural learning of attack vectors for generating mutated XSS attacks*. arXiv preprint arXiv:1009.3711.

Williams, L. (2019). Legal consequences of XSS attacks under GDPR. *European Journal of Law and Technology*, 10(3), 1-15.

Witten, I. H., Frank, E., & Hall, M. A. (2011). *Data mining: practical machine learning tools and techniques* (No. 11030). Morgan Kaufmann.