International Journal of Engineering and Techniques - Volume 10 Issue 2, March 2024

RESEARCH ARTICLE OPEN ACCESS

# APPLICATION SECURITY AND PRODUCT RESEARCH

**UJJAVAL PAREKH | 200305126901@PARULUNICERSITY.AC.IN | Parul university**
**KUSUM LATA DHIMAN | kusumlata.dhiman21133@paruluniversity.ac.in | Parul university**

## ABSTRACT:

Web applications are ubiquitous in today's digital landscape, necessitating robust security measures. Traditional web application penetration testing (WAPT) approaches, while valuable, face limitations in speed, efficiency, and comprehensiveness. This paper explores the potential of Artificial Intelligence (AI) to revolutionize WAPT, offering faster, more comprehensive, and potentially self-learning security assessments. We delve into the current market landscape, the promising future potential of AI-powered WAPT, and the unique capabilities it offers. Additionally, we examine the feasibility of continuously updating test cases and address concerns regarding AI's role in replacing human expertise.

## I. INTRODUCTION

The proliferation of web applications has heightened the need for robust security measures. Web application penetration testing (WAPT) plays a crucial role in identifying and mitigating vulnerabilities before malicious actors exploit them. However, traditional WAPT approaches often suffer from limitations:

- **Time-consuming nature:** Manual testing can be laborious and slow, delaying vulnerability remediation and impacting development timelines.
- **Resource-intensive requirement:** Skilled penetration testers are in high demand, making it challenging for organizations to maintain comprehensive testing coverage.
- **Limited scope:** Traditional methods might miss emerging vulnerabilities due to their static nature and require constant updates to adapt to the evolving threat landscape.

## II. CURRENT MARKET STATUS AND FUTURE POTENTIAL

The global application security testing market is projected to reach a staggering **USD 15.4 billion by 2027**, with a Compound Annual Growth Rate (CAGR) of 14.1% [1]. AI-powered WAPT tools are poised to be a significant driver of this growth, offering distinct advantages:

- **Automation:** AI can automate repetitive tasks such as vulnerability scanning and exploitation attempts, significantly accelerating the testing process.

- **Scalability:** AI-powered tools can efficiently handle large testing volumes, making them ideal for organizations with extensive web application portfolios.
- **Continuous learning:** AI algorithms possess the ability to learn from past data, including successful and unsuccessful exploits, continuously adapting their testing strategies to identify new vulnerabilities and attack vectors, leading to a more comprehensive and dynamic approach to security assessment.

## III. TARGET MARKET FOR AI-POWERED WAPT

AI-powered WAPT tools cater to a vast market, including:

- **Software development companies:** Streamlining the development process by enabling early identification and remediation of vulnerabilities.
- **Financial institutions:** Ensuring robust security for sensitive financial data.
- **E-commerce platforms:** Safeguarding customer information and transactions.
- **Healthcare organizations:** Protecting patient data and privacy.

## IV. UNIQUE CAPABILITIES OF AI IN WAPT

Beyond automation, AI offers several unique features that enhance WAPT:

- **Advanced vulnerability detection:** AI algorithms can analyze complex code structures and application behavior to identify subtle vulnerabilities missed by traditional methods, including zero-day vulnerabilities.
- **Prioritization of vulnerabilities:** AI can efficiently analyze the potential impact and exploitability of identified vulnerabilities, allowing developers to prioritize their efforts on mitigating the most critical threats.
- **Context-aware testing:** AI can consider the application's context, such as user roles and permissions, to tailor tests and prioritize vulnerabilities based on potential real-world attack scenarios.

## V. THE ROLE OF HUMAN EXPERTISE

While AI plays an increasingly important role, it is unlikely to completely replace human penetration testers. Human expertise remains essential for several key reasons:

- **Complex scenarios:** Complex scenarios and edge cases often require human judgment and expertise to make informed decisions and analyze the context surrounding test results.
- **Creativity:** Attackers constantly innovate, so human creativity is still crucial to stay ahead of evolving threats and design effective test scenarios.
- **Business context:** Understanding the specific business context and risk tolerance is essential for prioritizing vulnerabilities and making informed security decisions.

## VI. AI-POWERED WAPT: WORKING MODEL

AI-powered WAPT tools typically follow a multi-stage approach:

1. **Learning Phase:** The AI model is trained on historical data, including vulnerability databases, successful and unsuccessful exploit attempts, and code patterns associated with vulnerabilities.
2. **Scanning and Analysis:** The AI scans the web application, analyzing code structure, configuration, and functionality.
3. **Vulnerability Detection:** The AI leverages its knowledge base and analysis to identify potential vulnerabilities.
4. **Exploitation Attempts:** The AI attempts to exploit identified vulnerabilities, simulating real-world attack scenarios.
5. **Prioritization and Reporting:** AI prioritizes vulnerabilities based on severity and potential impact, generating a comprehensive report for developers and security professionals.

## VII. CONTINUOUSLY UPDATING TEST CASES WITH AI

One of the significant advantages of AI-powered WAPT lies in its ability to continuously update test cases. This dynamic approach ensures that security assessments remain relevant and effective in the face of the ever-evolving threat landscape. Here are several ways AI can achieve this:

- ***Machine Learning (ML):*** AI models can be trained on historical testing data, including successful and unsuccessful exploit attempts, vulnerability databases, and code patterns associated with vulnerabilities. By analyzing these vast datasets, the AI can learn to identify patterns and trends that might indicate new vulnerabilities or variations of existing ones. This knowledge can then be used to automatically generate new test cases or refine existing ones to target these emerging threats.
- ***Community-driven Updates:*** AI systems can be designed to leverage the collective knowledge of a security community. This can be achieved by integrating with platforms where security professionals share information about newly discovered vulnerabilities and their associated exploit methods. By analyzing this shared data, the AI can update its test case library to incorporate these new findings, ensuring that even the latest threats are covered during WAPT.
- ***Real-time Learning:*** Advanced AI systems can be designed to learn from the results of ongoing WAPT scans. If a new vulnerability is identified during a scan, the AI can analyze the exploit method and the application code involved. Based on this analysis, the AI can automatically create new test cases specifically designed to detect similar vulnerabilities in other parts of the application or even across different applications developed by the same organization.
- ***Integration with Vulnerability Databases:*** AI-powered WAPT tools can be integrated with real-time vulnerability databases. As new vulnerabilities are discovered and reported, the database is updated. The AI system can then access these updates and automatically incorporate them into its test case

library, ensuring that newly discovered vulnerabilities are promptly addressed during subsequent WAPT scans.

## VIII. PENETRATION TESTING ARTIFICIAL INTELLIGENCE: -

by Simon Tjoa (St. Pölten UAS, Austria), Christina Buttinger (Austrian Armed Forces), Katharina Holzinger (Austrian Armed Forces) and Peter Kieseberg (St. Pölten UAS, Austria) Securing complex systems is an important challenge, especially in critical systems. Artificial intelligence (AI), which is increasingly used in critical domains such as medical diagnosis, requires special treatment owing to the difficulties associated with explaining AI decisions. Currently, to perform an intensive security evaluation of systems that rely on AI, testers need to resort to blackbox (penetration) testing. In recent years, artificial intelligence (AI) has significantly changed the way we do business and research. Applications that previously seemed possible only in science fiction (e.g. personal assistants like Siri and Alexa) are now a reality. AI components are also becoming increasingly important in the automated decision-making routines behind many systems that are used in areas such as cancer research, open-source intelligence (OSINT) and intrusion detection. However, there is one huge drawback that limits the use of this technology. Often it remains unclear what exactly deep neural networks or similar approaches have learned and whether the software can be trusted. For some applications, either substantial research is conducted to gain a deeper understanding of their inner workings, or a human is involved in the process to ensure valid operation (i.e. 'human-in-the-loop'). While this approach is feasible in many cases, e.g. the doctor-in-the-loop, many applications, especially those that concern decision-making in critical infrastructures, do not scale with a human in the loop, often due to their time-critical nature. Furthermore, many of these decision-making processes need to be based on large amounts of inference datasets, thus making manual analysis practically impossible. This greatly reduces the trust in the results derived from such systems. In addition, in some applications, such as self-driving vehicles, it is not possible to use explainable AI or human intervention. Therefore, it is crucial to use an attacker's mindset to test the robustness and trustworthiness of the artificial system – especially considering the large attack surface posed by these systems and the massive developments in adversarial machine learning [1]. Combined with the inability to explain results, a lot of damage could be caused by attackers manipulating intelligent systems for their own gain. We propose a high-level concept of a systematic process to test AI systems within the data science lifecycle. This is mainly done by combining techniques from risk management (i.e. assessing the business risk, existing controls and the business case for an attacker), adversarial machine learning (i.e. evaluating the trustworthiness and robustness of the algorithm and trained abilities) and traditional penetration testing (i.e. evaluating the security of the implemented system, e.g. manipulation of sensor data). Figure 1 gives an overview of the generic approach, focussing on the AI components. While standard penetration testing of the underlying platform is required to mitigate threats and security gaps on this level (the greyed-out part labelled 'platform in Figure 1), this method extends the standard approaches to achieve certain tasks required for the AI components. The main problem with AI components is explainability; it is usually not possible to gain a detailed understanding of why a certain decision was made [2]. Thus, testers resort to black-

box security testing, trying to generate unwanted results either by using completely random (fuzzied) input material or by using nearby or extreme values. When using algorithms that learn from past decisions, it is vitally important to attack the underlying knowledge. We must assume that an attacker might be in possession of parts of the underlying (training) data or even have a (black-box) environment running the algorithms in question. The latter would enable the attacker to run many executions using arbitrary data or fuzzied information, trying differential attacks and feeding specially structured information into the system. This is very similar to the cryptanalytic counterparts of partially known and chosen plaintext attacks. Furthermore, depending on the algorithms in use, specific attacks might exist that need to be considered during the penetration test. While penetration testing is extremely valuable to evaluate such systems, proper risk analyses are often overlooked. These are important to: (i) carve out the attack surface, and (ii) help determine mitigation strategies and possible attack scenarios. Further research into possible attack scenarios is particularly important as the potential damage caused by manipulation of intelligent systems is often not clear even for the system's designers. Possible outcomes range from the introduction of broad bias into decision-making processes through to an attacker being able to launch fine-tuned attacks. Thus, together with identifying the (information) assets, the security analyst will also need to determine possible attack and damage scenarios in order to develop a feasible mitigation strategy. The proposed workflow is at first draft stage and requires additional methods to tailor it to specific systems and the technologies. Nevertheless, it can be used as a template to provide a basic level of security in AI-based systems. Importantly, penetration testing can never give a security guarantee; at best, the testers will find all bugs that could have been found by attackers, but as history has shown, even very prominent software stacks can be susceptible to newfound or newly introduced errors [3]. We are investigating these issues in two academic projects, the COIN-project "Big-Data Analytics" [L1] and the FORTE-project "exploreAI" [L2]. In these projects we are conducting indepth research into efficient penetration testing against intelligent systems and future implications for critical infrastructuresecurity.

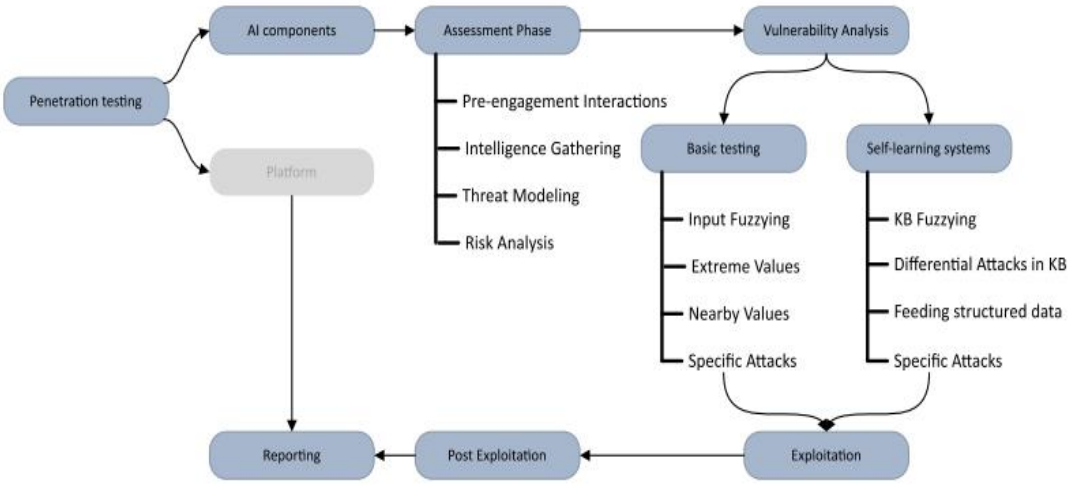


Figure 1 : A high-level approach to penetration testing AI system

- **BENEFITS OF CONTINUOUSLY UPDATED TEST CASES:**

➢ **Enhanced Security:** By continuously updating test cases, AI-powered WAPT tools can identify a wider range of vulnerabilities, including both known and emerging threats.

➢ **Reduced False Positives:** Traditional WAPT approaches might generate false positives due to outdated test cases. Continuously updated test cases based on real-world data can minimize false positives, improving the efficiency of security assessments.

➢ **Improved Efficiency:** Automating test case updates through AI can significantly reduce the manual workload associated with maintaining a comprehensive test suite. This frees up security professionals to focus on more complex tasks requiring human judgment and expertise.

- **CHALLENGES AND CONSIDERATIONS:**

  - **Data Quality:** The effectiveness of AI-powered test case updates relies heavily on the quality and comprehensiveness of the training data. It is crucial to ensure that the AI is trained on reliable and up-to-date data sources.
  - **Explainability:** As AI models become more complex, their decision-making processes can become less transparent. It is essential to develop mechanisms that explain the rationale behind AI-generated test cases, allowing security professionals to understand and potentially refine them if necessary.
  - **Human oversight:** While AI can automate test case updates, human oversight remains crucial. Security professionals need to review and validate AI-generated test cases to ensure their effectiveness and relevance to the specific application being tested.

## IX. CURRENT AI-POWERED WAPT TOOLS AND VALUATIONS:

The AI-powered WAPT market is experiencing rapid growth, with several established players and emerging startups offering innovative solutions. Here's a glimpse into some prominent tools and their estimated valuations (figures based on publicly available information and may not be fully accurate):

- **Apigee API Test (by Google Cloud):** Part of the Apigee API Management platform, Apigee API Test offers comprehensive AI-powered testing features.

It leverages machine learning for test case generation and prioritization, with valuations for the entire Apigee platform exceeding **USD 15 billion**.

- **Contrast Security:** This leading application security platform offers an AI-powered WAPT solution with features like intelligent scanning, self-learning vulnerability detection, and automated exploit analysis. Contrast Security's valuation is estimated to be around **USD 5 billion**.
- **Sqreen:** This cloud-based WAPT platform utilizes AI for automated vulnerability detection, prioritization, and real-time threat monitoring. While private, Sqreen has secured significant funding rounds, indicating a high potential valuation.
- **Detectify:** This European company offers an AI-driven WAPT platform that focuses on continuous security posture management and automated vulnerability detection. Detectify's valuation is estimated to be in the range of **USD 100 million to USD 500 million**.

**REFERENCES: -**

*1. A. Chakraborty et al.: "Adversarial attacks and defences: A survey", arXiv preprint arXiv:1810.00069, 2018.*

*2. K. Holzinger et al.: "Can we trust machine learning results? artificial intelligence in safety-critical decision support", ERCIM NEWS, (112), pp.42-43, 2018.*

*3. Z. Durumeric et al.: "The matter of heartbleed", in proc. of the 2014 conference on internet measurement (pp. 475-488), 2014.*

*4. Artificial intelligence in mental health research, World Health Organisation(WHO), (https://www.who.int/europe/news/item/06-02-2023-artificial-intelligence-in-mentalhealth-research--new-who-study-on-applications-and-challenges)*

*5. Galderisi S, Heinz A, Kastrup M, Beezhold J, Sartorius N. Toward a new definition of mental health. World Psychiatry. 2015;14(2):231-233. DOI:10.1002/wps.20231, (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4471980/)*

*6. Mental Health, Medically reviewed by Marney A. White, PhD, MS, Psychology by Adam Felman and Rachel Ann Tee-Melegrito, (https://www.medicalnewstoday.com/articles/154543)*

*7. Davenport, Thomas, and Ravi Kalakota. "The potential for artificial intelligence in healthcare." Future healthcare journal vol. 6,2 (2019): 94-98. doi:10.7861/futurehosp.6-2- 94, (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6616181/)*

*8. Minerva, F., & Giubilini, A. (2023). Is AI the Future of Mental Healthcare?. Topoi : an international review of philosophy, 42(3), 1–9. Advance online publication. (https://doi.org/10.1007/s11245-023-09932-3)*

*9. Artificial Intelligence for Mental Health and Mental Illnesses: an Overview, Sarah Graham, Colin Depp,Ellen E. Lee, Camille Nebeker, Xin Tu & Ho-Cheol Kim, Dilip V. Jeste, (https://doi.org/10.1007/s11920-019-1094-0) (https://escholarship.org/content/qt9gx593b0/qt9gx593b0_noSplash_d814b6b41c76cb874 050695d2bf30ced.pdf)*

*10. Detecting individuals with severe mental illness using artificial intelligence applied to magnetic resonance imaging, Wenjing Zhang, Chengmin Yang, Zehong, March 28, 2023, DOI:(https://doi.org/10.1016/j.ebiom.2023.104541) (https://www.thelancet.com/journals/ebiom/article/PIIS2352-3964(23)00106-8/fulltext)*

*11. Detecting individuals with severe mental illness using artificial intelligence applied to magnetic resonance imaging, Wenjing Zhang, Chengmin Yang, Zehong, March 28, 2023, DOI:(https://doi.org/10.1016/j.ebiom.2023.104541) (https://www.thelancet.com/journals/ebiom/article/PIIS2352-3964(23)00106-8/fulltext)*

*12. H. C. van Cuylenburg and T. N. D. S. Ginige, "Emotion Guru: A Smart Emotion Tracking Application with AI Conversational Agent for Exploring and Preventing Depression," 2021 International Conference on UK-China Emerging Technologies (UCET), Chengdu, China, 2021, pp. 1-6, doi: 10.1109/UCET54125.2021.9674993. (https://ieeexplore.ieee.org/document/9674993)*

*13. Virtual Reality Therapy: Everything You Need To Know, Emily Laurence, Forbes Health (https://www.forbes.com/health/mind/virtual-reality-therapy/)*

*14. The big promise AI holds for mental health, By Yelena Lavrentyeva, Emerging Tech Analyst, Published on December 13, 2022, (https://itrexgroup.com/blog/ai-mental-healthexamples-trends/)*

*15. Huang, Jessica A et al. "Telemedicine and artificial intelligence to support self-isolation of COVID-19 patients: Recent updates and challenges." Digital health vol. 8 20552076221100634. 15 May. 2022, doi:10.1177/20552076221100634 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9118431/)*

16. Fiske A, Henningsen P, Ethical Implications of Embodied Artificial Intelligence in Psychiatry, Psychology, and Psychotherapy, J Med Internet Res 2019;21(5):e13216: DOI: 10.2196/13216 (https://www.jmir.org/2019/5/e13216)

17. Farhud DD, Zokaei S. Ethical Issues of Artificial Intelligence in Medicine and Healthcare. Iran J Public Health. 2021 Nov;50(11):i-v. doi: 10.18502/ijph.v50i11.7600. PMID: 35223619; PMCID: PMC8826344.

18. Graham S, Depp C, Lee EE, et al. Artificial Intelligence for Mental Health and Mental Illnesses: an Overview. Curr Psychiatry Rep. 2019;21(11):116. Published 2019 Nov 7. doi:10.1007/s11920-019-1094-0

19. . Minerva F, Giubilini A. Is AI the Future of Mental Healthcare? [published online ahead of print, 2023 May 31]. Topoi (Dordr). 2023;42(3):1-9. doi:10.1007/s11245-023-09932-3 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10230127/)

20. Rakesh Margam. "Importance of Cybersecurity in Electronic Health Records." Volume. 8 Issue. 7, July - 2023 International Journal of Innovative Science and Research Technology (IJISRT), www.ijisrt.com. ISSN - 2456-2165, PP :-24-28. https://doi.org/10.5281/zenodo.8142290