ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/rajalakshmi-thiruthuraipondi-natarajan/444

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 2 & Iss: 3

Research Article

AI & Machine Learning in Applications Security and Vulnerability

Rajalakshmi Thiruthuraipondi Natarajan*

Citation: Kashyap G. AI for Robustness and Fairness: Addressing Bias, Fairness and Robustness in Machine Learning Algorithms. *J Artif Intell Mach Learn & Data Sci 2024*, 2(3), 2020-2023. DOI: doi.org/10.51219/JAIMLD/rajalakshmi-thiruthuraipondi-natarajan/444

Received: 02 July, 2024; **Accepted:** 18 July, 2024; **Published:** 20 July, 2024

***Corresponding author:** Rajalakshmi Thiruthuraipondi Natarajan, USA, E-mail: rajalan11@gmail.com

ABSTRACT

Vulnerabilities are the cracks in IT landscape through which hackers and other malicious users gain unauthorized access to the underlying systems and perform nefarious activities. These attacks can cost dearly to the company leading to financial and legal impacts. With the attackers getting smarter and finding new ways to hack, it is a continuous and tedious job for the security division to wade away these attacks and protect their applications. Leveraging AI and machine learning the security team cat have a better understanding of their systems and be able to identify and plug any gaps found. Using machine learning the team can have a complete knowledge of their landscape to understand the functionalities and with AI they can identify the gaps in the system that might potentially be a target for hackers to creep into the system. With careful design considerations and definitions AI can be a boom to the security division for performing various security checks in various phases of the project and support to find problems with the system and take corrective remedial actions. It can also be used to scan through the Internet and other support centers to find similar situations and recommend patches and other practical solutions for the issues identified thereby directing the team to traverse in the right path. There are several steps and techniques that can be followed to accomplish this which will be seen in detail in the following document.

Keywords: AI, Application vulnerability scanning, Data security, Machine learning, Regression scanning, Application landscape monitoring, Application security, Iterative analysis, Automated security data gathering.

1. Introduction

By going digital every organization has moved their data and operations into a machine thereby automating their process and by providing access to anyone around the world with proper access. However, it comes with the cost where unauthorized users can creep through the gaps in the system causing damages to the company these damages can reach anywhere from stealing corporate data or to cripple the entire system with the intent of disrupting the operations or extortion. Hence every organization has a resolute team and systems working around the clock to monitor their service and other applications to see if there are any such attacks and take timely and decisive actions against it. However not every problem can be identified since as the landscape grew this attack surface increases proportionally leaving certain areas susceptible to such attacks. Hence there needs to be a systematic approach in dealing such problems and leveraging every technology and options available in the market to secure once data and other proprietary items from being stolen or corrupted. These vulnerabilities can be in any layer and manually scanning through them to find any problems is naturally impossible hence leveraging AI and machine learning to do these scanning on behalf of the security team is a blessing to quickly scan through and receive necessary guidance for remediating these problems.

2. Challenges with Vulnerability Scanning

With advent of globalization and open market systems, it has become an inherent need for every organization to expose their systems to the outside network. With divorce operating model where employees work from every corner of the world the ability to connect these systems and work around the clock for the growth of the organization has been very fruitful. However, this has introduced new challenges with respect to data security since the systems are exposed to the outside world and are secured by various algorithms and authentication methodologies. While these security measures have helped the organization to a great extent there are some technically savvy hackers who can bypass the security and gain access to their internal systems and with several layers of infrastructure and platforms a vulnerability in any one of the layers might compromise the whole architecture. Hence, its particularly important that these scans are done on every system frequently. But there are several factors both internal and external that pose challenges.

2.1. Size and complexity of IT landscape

The first hurdle is the IT landscape by itself. Most organizations do not use one single application for their entire operations, but a combination of various applications and solutions integrated by a middleware or a complex networking system. This system might how they run architecture and framework and scanning each application for vulnerabilities would mean a clear and deep understanding of these applications itself. To accomplish this organizations, depend upon vendor documentation and expert knowledge, but these details are accurate only to a certain extent and there could be several rouge codes and unexpected additions that would significantly deviate from what is recorded and documented. Hence it is impossible to have one generic scan solution for identifying all the cracks in the system.

The complexity of the architecture can also be a huge challenge. In a typical IT environment that usually is a server, database and an application that run to help run a business. There are different scans and different identification methodologies needed to find problems in each of these sections hence that needs to be different methods of scanning addressing a particular segment of the IT architecture.

2.2. Application Changes

With evolving technologies and organizations adapting to the more modern and advanced versions, The IT department constantly undergoes changes and it is extremely hard for scaling up these scans to meet with the modern technology. Also, the need for frequent scans means there is an exceedingly small window between the upgrade and the tuning of the scanning algorithms to be in line with the latest version which is practically impossible. Additionally, if the vulnerability is identified in sections of the out-of-the-box product kappa the organizations are forced to rely on the vendors to provide patches and security updates to address the gaps. This might take a while before such patches are developed, tested and released, leaving the systems exposed for attacks.

Even with custom coding, which the organizations have complete control over, there are challenges in scanning for any problems. An ineffective and open-ended coding might but create a crack in the system that can be exploited. However, to confirm if there is in fact a weakness, there needs to be a clear understanding of the requirement and the design. There could be a conflict between what is considered as a vulnerability and what is needed by the organization for its functioning thereby putting it in a stalemate unable to deduce if there is a problem or not. While security Trump's the functionality that was always a grey area where each of the teams need to compromise to move ahead, leaving the weaknesses dormant and ready to be exploited.

2.3. Scan Frequency

Security threat to the IT systems is a constant and a continuous one for every organization. Especially critical industries such as banks, defense and government institutions face hundreds of such attacks on a daily basis. It is important that these attacks are thwarted every time since even a single breach could be a costly one. To effectively do that the systems have to be scanned on a regular basis such that the gap between the introduction of a vulnerability and the time it is identified is kept as minimum as possible. However, this would mean that that needs to be high performing high capability processors running all the time and scanning systems taking up a significant amount of time and resources for performing this activity. These scans have to be specially triggered during and after a project goes live, not just the product that is going like but any application or systems surrounding it to find if there are any weaknesses introduced. While large, well-funded organizations can afford such scans small and medium scale industries cannot, but the threat is no less significant.

And there is also a factor of human error. There is always a chance that certain aspects will be overlooked or neglected by manual intervention which might prove to be a fatal flaw. As part of the regression testing that is always a chance that either the testing will be skipped or will run based upon certain assumptions which might no longer hold good causing some weaknesses gone undetected. Certain assumptions and reliance on other systems such as firewalls or VPN to take care of the security might leave the cracks in the applications unaddressed.

3. AI in Vulnerability Scans

By Using AI and watch most of the challenges mentioned above, if not all can be successfully addressed. The technology has advanced so much that the modern AI systems can read the entire it structures with minimal or no human intervention. This can be a powerful tool that can aid the security team to constantly monitor, scan, collect data and analyze them to identify and provide relevant suggestions to tackle the issues. Coupling this with bots, makes it at deadly and effective defense system that can protect from external threat and constantly check and fix the internal systems. To achieve this there are a few preparatory steps that need to be performed to make AI equipped to protect underlying systems.

3.1. Understand the Landscape

To check the quality of the system EA needs to first understand the system. It needs to and review the system to know the functionalities of the system individually and its relation to other applications both within the network and outside. This would help the AI system recognize what should and should not be exposed to the outer world. For instance, an application storing employee data, the system needs to know how this application operates and used both internally and externally. The service it provides determines what data exposed is considered a breach and what not. This forms the basis of the entire scan. Anything that violates these rules would be considered as invisibility and a red flag raised for the appropriate team to take an action. The ideal way would be to feed AI with proper documentation associated to the product, however, there are many instances where the documentation is vague or incomplete rendering it useless. Hence the AI and machine learning systems should be hooked to these applications to continuously read the system of its daily operations to have a comprehensive knowledge of the application and its related systems, therefore possessing the day-to-day knowledge of the system in question. This activity can also throw light on the on-ground functioning, which can be further reviewed by the operational committee for any operational gaps that can be remediated.

3.2. Define Security Laws and Priority

The next part is the definition of security rules and regulations that every application needs to adhere by. These last can be dictated either by the government or by industrial standards or within the organization to maintain their reputation and the standards in the market. These rules can be hardened fast that can never be broken or guidance which the development and maintenance teams need to keep in mind unless it does not seriously affect the business operations. These rules can also have various levels of adherence that is the rules can be relevant for the entire corporation or for a certain set of applications. There should be careful definition of this rules to ensure that they do not conflict with each other and in case they do there needs to be a certain amount of priority provided to clearly define which overrides. These rules serve as the guiding metrics for all the scans and the applications that they cannot needs to adhere to these rules necessary if not flags are raised depending upon the criticality of the vulnerability. Care should also be taken that these rules are neither too strict that it is practically impossible to sustain such a standard or too lenient that a lot of vulnerabilities do not get captured as part of the scanning process.

It is also important to know that not every system needs the same level of security. Certain applications do not hold such sensitive data nor Part of the core network that any breach into such system might Causeway a grave damage to the organization. While any and all threats need to be eliminated, the organizations need to take into consideration the cost factor while defining such rules. Having a uniform code of security might not always be the best course of action. Hence that needs to be detailed analysis of the current IT structure, the future scope and any other factors in deciding these rules.

3.3. Scope and Frequency

Whit the Systems analyzed and understood and rules defined, the next logical step is to design the scans themselves. Realistically this is an extremely complex process since the landscape can have diverse set of applications running with different operating systems in different capacities. While the rules to adhere might be the same the ability to identify vulnerabilities based upon these rules would mean different forms of scanning. For example, to identify an authentication vulnerability in a server the process would be completely different from the scan that will be done in Oracle applications or database. Similarly, each application might be quoted using different languages such as PLSQL, Java, python, etc. and scanning these codes would mean a knowledge of these languages and the API's that they usually use and their validation, for example, a piece of code could be using and depreciated API from a Java cool so this can be called out as a vulnerability only with the knowledge of the valid APIs in the Java version that is being used.

Earlier, the scans can either be a continuous one or a periodic one. For the most critical systems and applications it is recommended that these scans happen in the highest frequency, continuous if possible. Using bots coupled with the knowledge gained by AI can be an effective combination. Bots are tireless piece of software that is designed to do a specific set of activities. These come in handy in situations where application testing is needed in a much frequent scale. Continuously scanning through the applications and collecting data the security team would have a great wealth of data to perform the analytics and identify appropriate solutions. This comes in handy especially in situations where the vulnerabilities are identified as part of an out-of-the-box product where the company needs to rely on the vendor to provide a solution. Until then using the data gathered the company can take educated and timely decision to overlay the burden on other systems such as network and VPN to take care of security until the problem is addressed. Though might not be an ideal solution this might be a quick fix solution to avoid any unpleasant situations.

The abilities discussed above are merely a fraction of what AI can do for the security of an organization. With the machine learning evolving every day the capabilities have increased multiple folds enabling the system using these facilities to design a comprehensive and a robust solution. While it is true that the hackers are getting innovative by the day with careful planning and design and proper rules in place these attacks can be prevented or at minimum controlled that by avoiding any significant financial or legal issues. Several mundane and a repetitive task have been taken over by AI and bots where the margin of error is expected to be minimal or none. However, the effectiveness of these systems depends upon the rules and the landscape of the organization.

4. Conclusion

While it is true that not all cracks and weaknesses can be identified and addressed, with the help of AI and bots a sizable number of these problems can be identified and addressed. While AI and other latest technologies can assist in tackling these problems, it is extremely important that the underlying architecture be designed to have layers of security based on the criticality of each application. Also, every application owner needs to accept the fact the security is everybody's responsibility and not just rely on outer layers to secure them since the attack can originate internally too. In the current digital world, security is not stopping all the attacks, which is impossible by itself, but the ability to respond quickly by taking necessary counter measures and recover with the least impact and time. By leveraging the latest technologies and solutions in the market, these is no doubt that any organization can achieve this.

5. References

1. https://www.allstarsit.com/blog/automating-vulnerability-detection-in-networks-with-ai#:~:text=AI%20automates%20the%20tasks%20of,past%20encounters%20and%20emerging%20threats.
2. https://portswigger.net/burp/vulnerability-scanner/guide-to-vulnerability-scanning

3. https://www.helpnetsecurity.com/2024/06/10/ai-vulnerability-management-role/

4. https://www.deepseas.com/ai-risk-ai-becoming-unintended-vulnerability-scanner/

5. https://datadome.co/bot-management-protection/vulnerability-scanning-protection-for-websites-apps-apis/

6. https://www.cimcor.com/blog/5-ways-to-help-fix-security-vulnerabilities

7. https://brightsec.com/blog/vulnerability-testing-methods-tools-and-10-best-practices/