IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125116

A Vulnerability Assessment In Web Application

Abinesh R [1], Adithyan U[2], Gowtham K[3] and Mrs.J.Shakila[4]

DMI college of Engineering[1]

DMI college of Engineering[2]

DMI college of engineering[3]

Assistant professor, DMI college of Engineering[4]

Abstract: Nowadays, most of the business enterprises are running through web application. But the major drawback is that they fail to provide a secure environment. To overcome this security issue in web application, there are vulnerability detection tools are available at present. But these tools are not proactive and consistent as it unable to track vulnerabilities. Vulnerability assessment reports play a vital role in ensuring the security of an organization's application, computer systems and network infrastructure.it is a process of identifying, classifying and prioritizing security vulnerabilities in IT infrastructure. It is a systematic review of security weakness in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assign severity levels to those vulnerability and can help to identify problem area. A comprehensive vulnerability assessment evaluates whether an IT system is exposed to known vulnerability. Web application vulnerability scanners are automated tools that scan web application, normally from the outside, to look for security vulnerabilities such as cross-site scripting, SQL injection, command injection, path traversal and insecure server configuration. It is a software command-line vulnerability scanner that scans webservers for dangerous file/CGIs, outdated server software and other problems. It performs generic and specific type checks.

Keywords: Command-Line Interface(CLI), Graphical User Interface(GUI).

I. INTRODUCTION

A vulnerability is a flaw in code or design that creates a potential point of security compromise for an endpoint or network. Vulnerabilities create possible attack vector through which an intruder could run code or access a target system's memory. The means by which vulnerabilities are exploited and include code injection and buffer overruns; they may be conducted through hacking scripts, applications and free hand coding. A Vulnerability assessment is the process of identifying and evaluating security vulnerabilities in a web application. Web applications have been a significant target for security breaches. Web applications are targeted by attackers, making it crucial to identify and address vulnerabilities in order to prevent potential security breaches. A vulnerability assessment involves using a combination of automated tools and manual testing to identify potential security weaknesses in a web application. These vulnerabilities can include issues such as cross-site scripting (XSS), SQL injection, insecure user input handling, and many others. These vulnerabilities give attackers unauthorized access to sensitive information, such as credit card data, accounts, and medical information. Approaches for identifying vulnerabilities in web applications. The tool which uses dynamic testing for web application is known as web vulnerability scanners. Once vulnerabilities are identified, they can be prioritized based on their severity and likelihood of exploitation. This allows developers and security teams to focus on addressing the most critical issues first, in order to reduce the risk of a successful attack. Overall, a vulnerability assessment is a critical part of the web application security lifecycle, and should be conducted regularly to ensure the ongoing security of a web application. An automated risk assessment approach is explored in this work. from the conference website.

II. LITURATURE SURVEY

[1] Due to the increasing number of network security vulnerabilities, vulnerability risk assessment must be performed to prioritize the repair of high-risk vulnerabilities. Traditional vulnerability risk assessment is based primarily on the Common Vulnerability Scoring Systems (CVSS) and attack graphs. Nevertheless, the CVSS metrics ignore the impact of the vulnerability on the specific network, which accounts that the identical vulnerability exists in different network environments is assigned repeated values. Additionally, the attack graphs still suffer from scalability and readability issues. To solve the above problems, a ranking method based on the heterogeneous information network is innovatively proposed to assess the vulnerability risk in a specific network. It considers the exploitability of a vulnerability, the impact of a vulnerability on the network components, and the importance of the vulnerable components. First, a heterogeneous information network containing vulnerability and host and the relationships between host and host is constructed to compute the risk score for each vulnerability and implement the ranking process. Second, a model extension method is proposed to adapt to situations in which additional factors related to vulnerability risk assessment need to be considered.

DOI: 10.17148/IJARCCE.2023.125116

Finally, we explore two case studies to compare the proposed method with CVSS and attack graph-based methods. The simulation results show that the proposed method can accurately assess the risk of vulnerabilities in a specific network environment and that it has a lower computational complexity than other methods.

[2] Deep neural network (DNN) has been recently applied to many safety-critical environments. Unfortunately, recent research has proven that DNN can be vulnerable to well-designed examples, called adversarial examples. Adversarial examples can easily fool a well-performed deep learning model with little perturbations imperceptible to humans. In this paper, to tackle the DNN security issue, we propose a Model Adversarial Score (MAS) index to evaluate the vulnerability of a deep neural network, and introduce a deep learning vulnerability assessment system (SecureAS) using adversarial samples to assess the vulnerability and risk of a trained DNN in a blackbox way. We also present two adversary algorithms (FGNM and PINM) that provide better adversary images with the similar attack effect compared to existing approaches like FGSM and BIM. Our experimental results confirm the effectiveness of MAS algorithm, SecureAS, FGNM and PINM. Take the self-driving system as an example. The vehicles are normally empowered by deep learning models in their image recognition system to detect and identify all kinds of traffic signs and signal signs. During the model training, a malicious attacker can construct adversarial examples by injecting adversarial perturbation to the original traffic sign image. Though the adversarial examples look very similar to the original image by human eyes, it can lead to a wrong classification. This becomes dangerous while deploying the deep learning model in the self-driving vehicles for image recognition. Once the attacker slightly modifies the actual traffic sign on the road using the same perturbation as the adversarial examples, the vehicles will miss-classify the traffic sign into the wrong classification and incur serious traffic accidents. This attack does not need to change the deep learning model itself but only the samples to mislead the deep neural network classifier. Additionally, the same attack samples are effective for many different deep neural networks, which makes the problem more critical. we make the first attempt to address the question: how to evaluate the vulnerability of a deployed neural network without knowing its inner structure? Currently, there is no systematic and intuitionistic index to reflect the vulnerability of DNNs, and no standard system to evaluate the vulnerability of DNN remotely in a blackbox way. To address this issue, we propose an index, named Model Adversarial Score (MAS) to evaluate and quantify the vulnerability of DNNs. The output of the MAS index is a score which measures the vulnerability of a model, and can also be used to evaluate the attack effect of an adversarial examples generation algorithm. Furthermore, to evaluate the vulnerability of a deep learning model thoroughly, we present a deep learning security assessment system SecureAS, which evaluates the security of a deep neural network for image classification through adversarial examples, in a blackbox way. Using this system, users can quickly generate the adversarial examples of local sample images, use them to test the target model, and analyze the security level of the target model.

[3] With the increase of extreme natural disasters and the frequent occurrence of man-made attacks, resilience studies of power grids have attracted much attention, among which resilience assessment reflects the resistance and resilience of power systems to cope with extreme disasters. To improve the resilience of distribution grids under extreme weather conditions, this paper proposes a resilience assessment framework for distribution grids under typhoon disasters. First, a probabilistic generation model of typhoon is established. Second, a spatiotemporal vulnerability model of the distribution grid lines to quantify the spatiotemporal impacts of typhoon. Third, a breadth-first search algorithm is used to island the distribution grid, and the amount of load shedding of the islanded microgrid is calculated. Meanwhile, the resilience of the distribution grid was quantitatively assessed according to the proposed new resilience index.

Finally, the feasibility of the proposed resilience assessment method is verified in the IEEE 33-bus test system, and the results show that the proposed method can accurately account for the impact of typhoon on the distribution grid and provides a quantitative reference basis for later power system planning and scheduling. The impact of extreme weather on power grids has received widespread attention, such as the snowstorm in China in 2008 and Hurricane Sandy in the United States in 2012, which cause to grid lines damage and tower toppling, widespread power outages and huge economic losses. In extreme weather conditions, multiple failures often occur in the distribution grid, and the N-1 safety criterion of the distribution grid alone is not sufficient to guarantee the safe operation of the distribution grid. Resilience is defined as the ability of the grid to withstand and recover from small probability of extreme events. Besides, as the distribution grid has the closest relationship with the user's production and life, the resilience of the distribution grid is mainly manifested by the support and recovery ability of the critical load in the distribution grid under extreme weather events. The resilience assessment of the distribution grid is of great significance for the safe operation and planning of the distribution grid. one of the most common extreme disasters, have an impact on the failure rate of the lines of the power grid, which in turn may cause to system load shedding and economic losses. This study focused on the impact of typhoons on distribution grids. Therefore, it is necessary to establish the model of the wind fields of typhoons. Several studies have also studied the model of typhoons.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125116

The Ref. [3] proposed a stochastic method to simulate typhoon trajectories based on historical data, which is seriously dependent on historical data. Thereafter, the Batts wind field model was proposed in [4], which is a more mature wind field model. [5] proposed the Georgiou typhoon wind field model, which can more accurately forecast the wind speed of typhoon when the typhoon is moving on the sea surface. [6] proposed a method for simulating a typhoon wind field based on SPARK for high-performance computing.

[4] Nowadays, vulnerability attacks occur frequently. Due to the information asymmetry between attackers and defenders, vulnerabilities can be divided into known and unknown. Existing researches mainly focus on the risk assessment of known vulnerabilities. However, unknown vulnerabilities are more threatening and harder to detect. Therefore, unknown vulnerability risk assessment deserves the widespread attention. To model the exploit process, directed graph models are applied to vulnerability risk assessment. And security metrics are used to quantify the exploitability of vulnerabilities. In this paper, according to the data source of nodes, related works of unknown vulnerability risk assessment based on directed graph models are divided into two types. One is based on network-level data, the other is based on system-level data. The former is to visualize the network status, while the latter is to reflect the running process of the system. The concept and purpose of these directed graph models are given at first. Then, these models are analyzed from three aspects, including advantages, flaws and solutions. After that, challenges and solutions of unknown vulnerability risk assessment based on directed graph models are given.

Meantime, security metrics for unknown vulnerability risk assessment based on directed graph models are summarized and classified. Finally, future work directions of unknown vulnerability risk assessment are discussed from the perspective of techniques and application trends. Consequently, this paper can fill in the lack of current survey on unknown vulnerability risk assessment based on directed graph models. Vulnerability risk assessment based on directed graph models needs to accomplish both qualitative and quantitative tasks. For Known Vulnerability Risk Assessment (KVRA), vulnerability information can be obtained by vulnerability scanners, such as Nessus, Nmap, etc. Directed graphs can be generated automatically by existing tools. Meantime, standards such as Common Vulnerability Scoring System (CVSS) [3] can be directly used to quantify the exploitability of each known vulnerability. However, KVRA does not consider the situation that defenders may have less or no prior knowledge on vulnerabilities. To solve this problem, the technology of Unknown Vulnerability Risk Assessment (UVRA) is proposed and should be given more attention because unknown (zero-day) vulnerabilities are harder to detect. Moreover, the threat and loss caused by this kind of attack are far more serious than known vulnerabilities. For UVRA, current researches often set a time point to divide known vulnerabilities into known and unknown vulnerabilities because the latter is difficult to obtain in reality

[5] An automated risk assessment approach is explored in this work. The focus is to optimize the conventional threat modeling approach to explore software system vulnerabilities. Data produced in the software development processes are better leveraged using Machine Learning approaches. A large amount of industry knowledge around security vulnerabilities can be leveraged to enhance current threat modeling approaches. Work done here is in the ecosystem of software development processes that use Agile methodology. Insurance business domain data are explored as a target for this study. The focus is to enhance the traditional threat modeling approach with a better quantitative approach and reduce the biases introduced by the people who are part of software development processes.

This effort will help bridge multiple data sources prevalent across the software development ecosystem. Bringing these various data sources together will assist in understanding patterns associated with security aspects of the software systems. This perspective further helps to understand and devise better controls. Approaches explored so far have considered individual areas of software development and their influence on improving security. There is a need to build an integrated approach for a total security solution for the software systems. A wide variety of machine learning approaches and ensemble approaches will be explored. The insurance business domain is considered for the research here. CWE (Common Weaknesses Enumeration) mapping from industry knowledge are leveraged to validate the security needs from the industry perspective. This combination of industry and company data will help get a holistic picture of the software system's security. Combining the industry and company data helps lay down the path for an integrated security management system in software development. The risk management framework with the quantitative threat modeling process is the work's uniqueness. This work contributes toward making the software systems secure and robust with time. Threat modeling and its constructs are described. Exploration of risk assessment methodology for threat modeling is conducted. Data collection and modeling for threat prediction are covered. Paper wraps up with the recommendations and future work. The focus of the work is automating the security vulnerability risk assessment approach and threat modeling approach with the machine learning approach. Both exercises are optimally combined for better outcomes. Machine learning classification approaches are leveraged to get visibility into possible security vulnerabilities.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

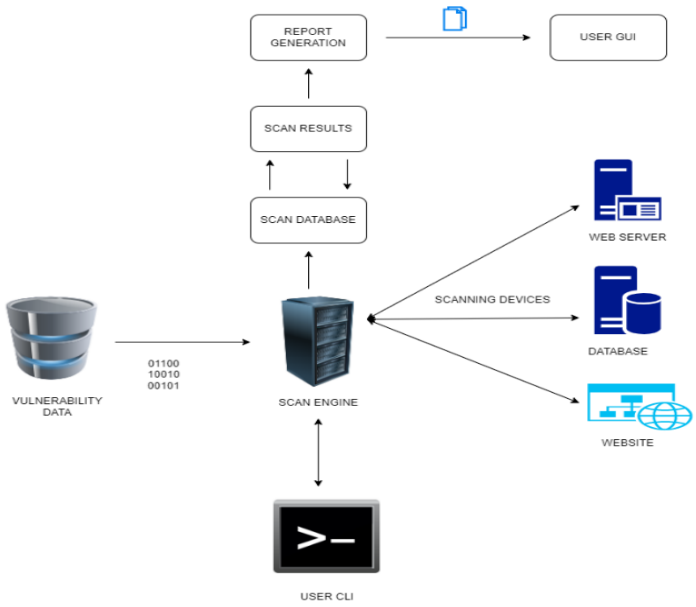
International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125116

III. PROPOSED SYSTEM

Vulnerability assessments are automated processes performed by scanners.It is a command-line tool to detect vulnerabilities. It is capable of scanning for over 6700 items to detect misconfiguration, risky files, etc. and some of the features include. You can save the report in HTML, XML, and CSV. It supports SSL Scan multiple ports on the server Find subdomain. Apache user enumeration. In our project we used to every command-line tools together to scan a web server for the vulnerability that can be exploited and can compromise the server. It can also check for outdated version details of 1200 servers and can detect problems with specific version details of over 200 servers. It can also fingerprint the server using favicon.ico files present in the server. It is not designed to be a particularly stealth tool rather than it is designed to be fast and time-efficient to achieve the task in very little time. Because of this, a web admin can easily detect that its server is being scanned by looking into the log files.



1. Web Application Scanning Server:
The Web Application Scanning Server is responsible for coordinating and managing the vulnerability assessment process. It acts as the central control point and performs the following tasks:
- Vulnerability scanning: Utilizes specialized vulnerability scanning tools or frameworks to scan the web application for known vulnerabilities. This can include tools like OWASP ZAP, Burp Suite, or commercial vulnerability scanners.
- Workflow management: Orchestrates the scanning process, including configuring the scanning parameters, scheduling scans, and managing the scanning workflow.
- Report generation: Collects the scan results from the database scanning servers and generates comprehensive vulnerability assessment reports.
- Integration: Interfaces with other systems or tools for enhanced vulnerability assessment capabilities, such as integrating with a ticketing system to track and manage vulnerabilities.

2. Database Scanning Servers:
The Database Scanning Servers focus on scanning the three target databases for potential vulnerabilities. Each database scanning server is responsible for the following tasks:
- Database scanning tool: Utilizes a specialized database vulnerability scanning tool to identify vulnerabilities specific to the database technology being used. Examples include AppScan, Acunetix, or SQLMap.
- Connection and authentication: Establishes connections with the target databases using appropriate credentials and authentication mechanisms.
- Vulnerability identification: Scans the databases for known vulnerabilities, including configuration issues, weak access controls, injection vulnerabilities, and other database-specific weaknesses.
- Logging and reporting: Captures scan results and logs any identified vulnerabilities or suspicious activities for further analysis and reporting.

DOI: 10.17148/IJARCCE.2023.125116

3. Network Infrastructure:
The network infrastructure provides the necessary connectivity and security for the vulnerability assessment process. It includes:

- Network segmentation: Segments the network to isolate the web application and database servers from other systems and networks to minimize the attack surface.
- Firewalls and security measures: Implements network firewalls, intrusion detection/prevention systems, and other security measures to protect the scanning infrastructure and prevent unintended impacts on the target systems.
- Secure communication: Ensures secure communication channels between the scanning servers and the target systems, using protocols like SSH or VPNs to protect sensitive information and credentials.

4. Reporting and Analysis:
The vulnerability assessment architecture should include a reporting and analysis component that consolidates the findings from the web application and database scanning servers. This component:
- Collects and aggregates vulnerability assessment results from the scanning servers.
- Performs analysis to prioritize and categorize vulnerabilities based on their severity and potential impact.
- Generates comprehensive reports that provide detailed information about the identified vulnerabilities, their potential risks, and recommended remediation steps.
- Supports integration with vulnerability management or ticketing systems to facilitate vulnerability tracking and resolution.

IV. CONCLUSION

In conclusion, vulnerability assessments are essential for organizations to proactively identify and address vulnerabilities in their systems, networks, and infrastructure. These assessments provide valuable insights into potential weaknesses, enable prioritization of remediation efforts, and enhance overall security posture. By conducting vulnerability assessments regularly, organizations can mitigate risks, comply with regulations, protect sensitive information, improve incident response preparedness, and continuously enhance their security measures. Investing in vulnerability assessments is a crucial step towards safeguarding against cyber threats and maintaining a robust and resilient security posture.

Server-Side Request Forgery (SSRF) Mitigations: SSRF is a vulnerability that allows an attacker to make requests from the web server to internal resources. Developing techniques to detect and prevent SSRF vulnerabilities in web servers would be valuable.Web Application Firewall (WAF) Improvements: WAFs are designed to protect web applications from various attacks. Enhancing the capabilities of WAFs by developing more advanced rule sets and detection mechanisms could help mitigate both known and emerging vulnerabilities.

Serverless Architecture Security: With the rise of serverless computing, new security challenges have emerged. Investigating and addressing vulnerabilities specific to serverless architectures and functions as a service (FaaS) would be beneficial. As web applications increasingly rely on APIs to communicate with each other, securing API endpoints becomes crucial. Exploring vulnerabilities like insecure API authentication, authorization issues, and API abuse scenarios could be an area of focus. Zero-day Vulnerability Discovery: Zero-day vulnerabilities are unknown vulnerabilities that can be exploited before the vendor is aware of them. Developing innovative techniques for vulnerability discovery, including fuzzing, static analysis, and machine learning-based approaches, could be valuable in proactively identifying and patching vulnerabilities.Containerization Security: Containerization technologies like Docker and Kubernetes have gained significant popularity. Identifying and addressing vulnerabilities related to container escape, container runtime security, and securing container orchestration platforms would be important for ensuring robust web server deployments.Security Automation and DevSecOps: Integrating security into the development and deployment pipeline is essential. Developing tools and frameworks that facilitate secure coding practices, automated security testing, and vulnerability remediation in the context of DevSecOps would be highly valuable.

REFERENCES

[1] S. N. Chari, T. A. Habeck, I. Molloy, Y. Park, J. R. Rao, and W. Teiken, ‘‘A platform and analytics for usage and entitlement analytics,’’ IBM J. Res. Develop., vol. 60, no. 4, pp. 1–12, Jul. 2016.
[2] T. Marschall, I. Herms, H.-M. Kaltenbach, and S. Rahmann, ‘‘Probabilistic arithmetic automata and their applications,’’ IEEE/ACM Trans. Comput. Biol. Bioinf., vol. 9, no. 6, pp. 1737–1750, Nov. 2012.
[3] R. Padmanaban, M. Thirumaran, V. Sanjana, and A. Moshika, ‘‘Security analytics for heterogeneous Web,’’ in Proc. IEEE Int. Conf. Syst., Comput., Autom. Netw. (ICSCAN), Pondicherry, India, Mar. 2019, pp. 1–6, doi: 10. 1109/ICSCAN.2019.8878832.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125116

[4] W. Wang, F. Shi, M. Zhang, C. Xu, and J. Zheng, "A vulnerability risk assessment method based on heterogeneous information network," IEEE Access, vol. 8, pp. 148315–148330, 2020, doi: 10.1109/access.2020.3015551.
[5] B. D. Priyaa and M. I. Devi, "Hybrid SQL injection detection system," in Proc. 3rd Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), Jan. 2016, pp. 22–23.
[6] A. Petukhov and D. Kozlov, "Detecting security vulnerabilities in Web applications using dynamic analysis with penetration testing," in Proc. Appl. Secur. Conf., Ghent, Belgium, May 2008, pp. 1–6. [7] V. Prokhorenko, K.-K.-R. Choo, and H. Ashman, "Context-oriented Web application protection model," Appl. Math. Comput., vol. 285, pp. 59–78, Jul. 2016.
[8] L. K. Shar, L. C. Briand, and H. B. K. Tan, "Web application vulnerability prediction using hybrid program analysis and machine learning," IEEE Trans. Dependable Secure Comput., vol. 12, no. 6, pp. 688–707, Nov. 2015.
[9] J. Thome, "A scalable and accurate hybrid vulnerability analysis framework," in Proc. IEEE Int. Symp. Softw. Rel. Eng. Workshops (ISSREW), Nov. 2015, pp. 2–5.
[10] J. Fonseca, M. Vieira, and H. Madeira, "Evaluation of Web security mechanisms using vulnerability & attack injection," IEEE Trans. Dependable Secure Comput., vol. 11, no. 5, pp. 440–453, Sep. 2014.
[11] L. K. Shar and H. B. K. Tan, "Automated removal of cross site scripting vulnerabilities in Web applications," Inf. Softw. Technol., vol. 54, no. 5, pp. 467–478, May 2012.
[12] F. Valeur, D. Mutz, and G. Vigna, "A learning-based approach to the detection of SQL attacks," in Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment. Berlin, Germany: Springer, 2005, pp. 123–140.