Vulnerability Management in IT Infrastructure

Raghav Taori[1], Jali Rohan[2], Raghavendra Prasad SG[3], Dr. K.B. Ramesh[4], Suryanarayana Vijay[5]

[1,3] Department of Information Science and Engineering, R V College of Engineering, Bangalore, India
[2,4] Department of Electronics and Instrumentation Engineering, R V College of Engineering, Bangalore, India
[5]Hewlett Packard Enterprise

---***---

Abstract – In today's world, cyber security is a major concern, and its risks can have far-reaching effects for organizations. The newspaper headlines are dominated by stories about data breaches, for instance. The company suffers from lowered trust levels, and its revenue suffers as a result. Therefore, it is important to comply with security policies. At present, security management processes are manual and need some intelligence and automation. A vulnerability report can be generated in several formats, such as XML, Excel, or CSV. We aim to make the critical infrastructure of the organization cyber-secure and automate the manual process of identifying mission critical assets, threat surfaces, vulnerabilities, and remediation procedures. Our solution was to create a web portal that allows asset owners to log in and see all their assets with vulnerabilities, which can then be remedied according to the solutions provided by the security lead. A web portal was developed using MONGO DB, NODE JS, EXPRESS JS, and REACT JS, so that the user could access the reports from the NOSQL database in an organized way. Besides data analytics, mail escalation, and false positive detection, other features have been implemented as well. Data centers, research labs, and other locations are included in the scope of this project. Assets such as crash & burn and other assets that are not mission-critical are not included in the product.

***Key Words*: Cybersecurity, Security Management, Vulnerability assessment, cyber-security compliant, Mission critical assets, React JS, Node JS, MongoDB, Web Application, MERN Stack**

1. INTRODUCTION

A vulnerability is a weakness in a system that allows threats to compromise assets. It is inevitable that all systems will have vulnerabilities. Vulnerability assessments help identify vulnerabilities using vulnerability scans. Performing a vulnerability assessment on a system is a systematic way of identifying its vulnerabilities and weaknesses ahead of time. Identifying loopholes ahead of time through vulnerability assessments allows any organization to safeguard itself against cyberattacks. We can obtain vulnerability alert reports from tools such as Tenable, Qualys, etc. In order to remedy these vulnerabilities, these reports are currently being analyzed manually, and emails are being sent to the asset owners. The security lead has a tough time determining whether the vulnerabilities have been remedied or not, and whether a false-positive will occur next time around. We came up with a solution to make the task of remediating these vulnerabilities to closure more effective, efficient, and transparent for Security Admins, Infra Admins, and Asset Owners. Vulnerability reports will mainly contain the following information:

- Vulnerability name
- IP address
- CVSS or Severity
- Scan date

It is possible to generate vulnerability reports in a variety of formats, such as XML, Excel, or CSV. Our primary objective is to make mission-critical assets cyber-security compliant and automate the manual tasks of identifying mission-critical assets, threat surfaces, and resolving vulnerabilities.

1.1 LITERATURE SURVEY

Comparative study of some applications made in the Vue.js and React.js frameworks [1]. There has been a significant increase in demand for these technologies stacks due to the growing desire for faster systems that are better than the traditional systems. Several JavaScript frameworks are available that have features such as popularity, ease of use, and integration with different technologies. ReactJS and VueJS are compared clearly in terms of the above-mentioned features as well as others.

Performance comparison and evaluation of Node.js and traditional web server (IIS) [2]. An analysis of discrete choice models' estimation process has been presented by the author. In the publication, Maximum Likelihood Estimation is described. Due to this, users can estimate many models, including multinomial logit, hybrid models, and others. Moreover, by employing a high number of iterations, the approach aims to eliminate any biases or inclinations that may exist in the model and produces equal weighted answers.

Research and Application of Node.js Core Technology [3]. Early on in the development of a network, various technologies were employed for front-end and back-end development. With the debut of node.js, the development of the website has undergone enormous changes. A server-side programming platform called node.js was created based on the Chrome V8 engine JavaScript runtime environment, in contrast with single-threaded PHP and multi-threaded Java. By utilizing its own built-in and defined properties, Node.js compensates for the limitations of the background development language. A server-side JavaScript interpreter is used to build rapid and easy-to-use web applications. There are several functions that Node.js can perform that Core JavaScript cannot, such as file systems, modules, packages, and operating system APIs, In this study, we compare the performance of MongoDB to MySQL by examining insertion and retrieval operations using a web/android application to explore sharding and its benefits in MongoDB [4]. Information gathered from multiple input and output sources can be used to build certain infrastructures, but if not handled properly, it can also be prone to damage, which could result in data loss. In order to overcome such loss, the NoSQL MongoDB is one example of a parallel strategy being used. The auto-sharding feature of Mongo DB makes it a differentiating cross-platform, document-oriented database that ensures optimal data management and excellent performance. As the database is sharded over several servers, capacity and scalability are increased.

Challenges faced today by computer security practitioners [5]. The report stated that computer security practitioners still have difficulty convincing management that these issues are important, as well as educating management and users, getting other security professionals' cooperation, and using the available security technology.

Safe Client/Server Web Development with Haskell [6]. A robust and comprehensive web development framework based on Reflex-Dom and Servant, two Haskell libraries, is shown to make use of type checking to ensure various security and correctness features. We can guide them by using types to ensure our API gets the right data.

Data Integrity: Recovering from Ransomware and Other Destructive Events [7]. To assist businesses in ensuring the integrity of their data, The National Cybersecurity Center of Excellence (NCCoE) works in partnership with businesses and the information technology community (IT). Several breaches of data integrity have exposed company data, including emails, personnel files, financial information, and consumer data.

Cyber Security Based on Artificial Intelligence for Cyber-Physical Systems [8]. Analyzed how systems have become more complex, intelligent, and autonomous as they have grown more sophisticated and complicated. A variety of cyber and physical components interact with each other in extremely complex ways. As a result of their extreme complexity, they are susceptible to significant perturbations.

2. METHODOLOGY

By developing a web portal where users can login and view Vulnerability reports and take the necessary actions, we can overcome the manual process of analyzing Vulnerability reports. As a result, the entire life cycle of Risk Treatment could be made more efficient and faster. The process of identifying false positives and raising exceptions becomes simpler and more efficient.

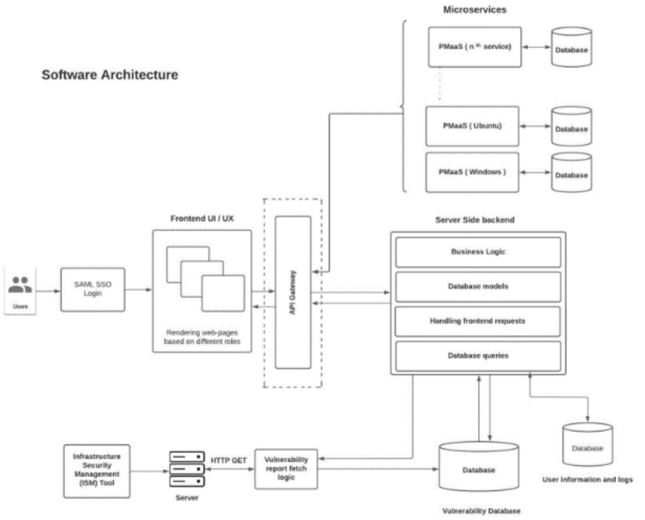


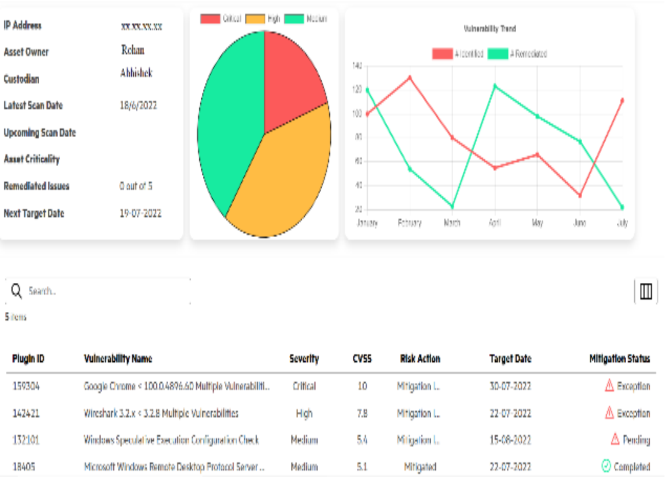
Fig 1. Proposed Software Architecture

3. RESULTS AND DISCUSSIONS

With the help of a portal, we have built a process for automating the process of cyber-security management and displaying vulnerability scan reports in a more structured way. We developed different user interfaces for different personas. Personae are mainly divided into two types:

1. Security Lead
2. Asset Owner

Our scanning tool produces a report which we store into a MongoDB collection once we receive its results. It mainly contains all the vulnerabilities associated with a specific infrastructure. Each vulnerability is then enhanced with some additional fields. There are a number of important fields, including Risk Treatment, Mitigation Status, and Remediation Target Date. Vulnerability Risk Treatments are initially not set for particular vulnerabilities. All vulnerabilities will be visible to the Security Lead once he/she logs in. Depending on the security lead's decision, Risk Treatment can either be mitigated or accepted. In the case of a Mitigate Risk Treatment, the Security Lead must specify a Remediation Target Date. When the Asset Owner logs in, he/she can view all assets belonging to their Infrastructure that have been assigned a Risk Treatment of Mitigate by the Security Lead. It is the asset owner's responsibility to remediate his/her assets before the remediation deadline. In order to remediate their assets, the Asset owner could follow the remediation steps provided by the Security Lead. As soon as the Asset Owner remediates the assets, the mitigation status must be updated from Pending to Completed. A status update made by an Asset owner is reflected in Security Lead's UI as well.



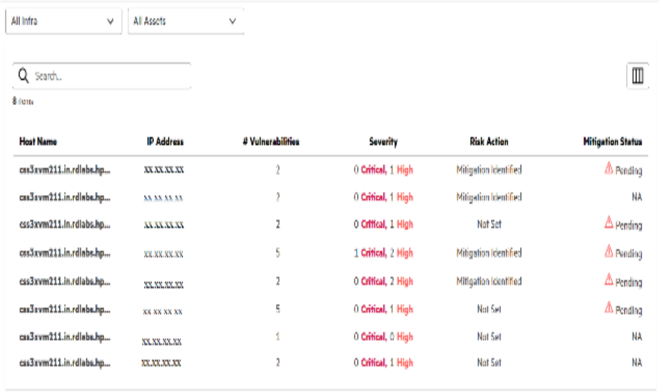
IP Address	xx.xx.xx.xx
Asset Owner	Rehan
Custodian	Abhishek
Latest Scan Date	18/6/2022
Upcoming Scan Date	
Asset Criticality	
Remediated Issues	0 out of 5
Next Target Date	19-07-2022

5 items

Plugin ID	Vulnerability Name	Severity	CVSS	Risk Action	Target Date	Mitigation Status
159304	Google Chrome < 100.0.4896.60 Multiple Vulnerabili...	Critical	10	Mitigation I...	30-07-2022	⚠ Exception
142421	Wireshark 3.2.x < 3.2.8 Multiple Vulnerabilities	High	7.8	Mitigation I...	22-07-2022	⚠ Exception
132101	Windows Speculative Execution Configuration Check	Medium	5.4	Mitigation I...	15-08-2022	⚠ Pending
18405	Microsoft Windows Remote Desktop Protocol Server ...	Medium	5.1	Mitigated	22-07-2022	✓ Completed

Fig 2. Security lead & Asset owner View

In the event that the owner is unable to resolve the issue by the target date, an email will be sent to his/her manager. Asset owners can also request an exception for extending the remediation target date by providing valid business justifications. This exception will be notified to the Security lead. As long as the Security lead accepts the exception, the Remediation target date will be updated as requested by the Asset owner.



8 items

Host Name	IP Address	# Vulnerabilities	Severity	Risk Action	Mitigation Status
css3xvm211.in.rdlabs.hp...	xx.xx.xx.xx	2	0 Critical, 1 High	Mitigation Identified	⚠ Pending
css3xvm211.in.rdlabs.hp...	xx.xx.xx.xx	2	0 Critical, 1 High	Mitigation Identified	NA
css3xvm211.in.rdlabs.hp...	xx.xx.xx.xx	2	0 Critical, 1 High	Not Set	⚠ Pending
css3xvm211.in.rdlabs.hp...	xx.xx.xx.xx	5	1 Critical, 2 High	Mitigation Identified	⚠ Pending
css3xvm211.in.rdlabs.hp...	xx.xx.xx.xx	2	0 Critical, 2 High	Mitigation Identified	⚠ Pending
css3xvm211.in.rdlabs.hp...	xx.xx.xx.xx	5	0 Critical, 1 High	Not Set	⚠ Pending
css3xvm211.in.rdlabs.hp...	xx.xx.xx.xx	1	0 Critical, 0 High	Not Set	NA
css3xvm211.in.rdlabs.hp...	xx.xx.xx.xx	2	0 Critical, 1 High	Not Set	NA

Fig 3. Security lead & Asset owner View

Time frame for remediation, escalation matrix and SLAs are determined by criticality of vulnerability and criticality of asset. In the UI, there are two types of views - Unique Vulnerabilities and All Assets. Using the Unique Vulnerabilities view, we are able to view all the assets that are affected by a particular vulnerability. Additionally, when we click on an asset in the assets-based view, we will be able to see all the vulnerabilities associated with that asset. Detection of false positives has also been implemented.

4. CONCLUSION

Unlike crash-and-burn projects, this project focuses on protecting mission-critical assets only. It is possible to migrate the project to a cloud platform such as AWS. In order to detect vulnerabilities more effectively, more databases could be used for vulnerability checks.

REFERENCES

[1] C. M. Novac, O. C. Novac, R. M. Sferle, M. I. Gordan, G. BUJDOSó and C. M. Dindelegan, "Comparative study of some applications made in the Vue.js and React.js frameworks," 2021 16th International Conference on Engineering of Modern Electric Systems (EMES), 2021, pp. 1-4, doi: 10.1109/EMES52337.2021.9484149.

[2] L. P. Chitra and R. Satapathy, "Performance comparison and evaluation of Node.js and traditional web server (IIS)," 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), 2017, pp. 1-4, doi: 10.1109/ICAMMAET.2017.8186633.

[3] X. Huang, "Research and Application of Node.js Core Technology," 2020 International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI), 2020, pp. 1-4, doi: 10.1109/ICHCI51889.2020.00008.

[4] L. F. Reese, "Challenges faced today by computer security practitioners," [1989 Proceedings] Fifth Annual Computer Security Applications Conference, 1989, pp. 143-, doi: 10.1109/CSAC.1989.81044.

[5] R. A. Kemmerer, "Cybersecurity," 25th International Conference on Software Engineering, 2003. Proceedings., 2003, pp. 705-715, doi: 10.1109/ICSE.2003.1201257

[6]H. Sedjelmaci, F. Guenab, S. -M. Senouci, H. Moustafa, J. Liu and S. Han, "Cyber Security Based on Artificial Intelligence for Cyber-Physical Systems," in IEEE Network, vol. 34, no. 3, pp. 6-7, May/June 2020, doi: 10.1109/MNET.2020.9105926

[7] T. McBride, A. Townsend, M. Ekstrom, L. Lusty and J. Sexton, "Data Integrity: Recovering from Ransomware and Other Destructive Events," 2018 IEEE Cybersecurity Development (SecDev), 2018, pp. 140-140, doi: 10.1109/SecDev.2018.00036

[8]M. Mazumder and T. Braje, "Safe Client/Server Web Development with Haskell," 2019 IEEE Cybersecurity Development (SecDev), 2019, pp. 150-150, doi: 10.1109/SecDev.2019.040.

[9] Y. Hong and X. Shao, " Analysis of CyberSecurity Product Reviews Based on Machine Learning", *2021 3rd International Conference on Applied Machine Learning (ICAML)*, pp. 398-401, 2021.