CONVERGING VULNERABILITY INSIGHTS: UNIFYING VULNERABILITY INTELLIGENCE FOR ENHANCED APPLICATION SECURITY WITH COLLABORATION

Aparna, Khare[1]

[1]National Informatics Centre

ABSTRACT

The cyber threat landscape is ever evolving, and as technologies advance and grow, so do the vulnerabilities in software technologies, programming languages and software development frameworks. There is an imperative need to be able to preemptively counter emerging threats in software and applications, standalone or otherwise. There are several vulnerability intelligence tools and services available in the market, however they suffer from a single common drawback. The vulnerability intelligence they present depends on selective and even proprietary feeds of information. With software technology that is largely driven by community efforts, a much better solution is to present the vulnerability intelligence from the community driven vulnerability databases itself. Furthermore, vulnerability intelligence can also be utilized in the field of cyber forensics. Forensic investigators require a sound foundational knowledge of vulnerability insights and attack vectors to understand how an attack or an incident might have occurred. This paper presents a web-based vulnerability intelligence platform that can effectively leverage the OSV database, NVD, CAPEC and CWE to present a more comprehensive, community driven vulnerability intelligence that can not only help organizations in their vulnerability management efforts but also help cyber forensic analysts in getting relevant information about known attack methods in real time.

Keywords –Cyber Security, Open-Source Vulnerability Databases, Software Vulnerability Intelligence, Vulnerability Data Aggregation, Vulnerability Database Standardization, Vulnerability Intelligence Collaboration, Vulnerability Intelligence Platform, Vulnerability Prioritization

1. INTRODUCTION

A vulnerability database, sometimes also referred to as a vulnerability database repository, is a structured collection of information about newly discovered and known vulnerabilities present within system software, application software, and other computing systems. Vulnerability databases enable organizations and security professionals to identify, prioritize, and address vulnerabilities efficiently so that appropriate measures can be taken against cyber security threats. They are foundational in providing the necessary intelligence to organizations for proactive vulnerability management, which is of critical importance in the realm of cyber security. This is because the vulnerabilities within software and systems, if they are left unaddressed, can expose the organizations and online services to a plethora of risks such as data breaches and service disruptions that can severely impact the confidentiality, integrity, and availability of the assets involved [1].

While several organizations maintain their own proprietary vulnerability repositories for intelligence, when required to be availed by other organizations, they may impose a financial burden in terms of licenses and may also very well be inaccurate in terms of delay in updation with respect to continually discovered vulnerabilities. Community driven open-source vulnerability databases that are backed by organizations/communities solely focused on maintaining the database, are often regularly updated depending on the ecosystem of contributors. These continuously updated databases, if they can be converged under a common standardized format and a common access platform, can prove to be extremely fruitful when considering the holistic picture for enhancing security. Further, active options of collaborations would ensure that the converged system stays updated and of use to the community.

2. KEY TERMS

The key terms used in this paper are described as below:

2.1 Vulnerability

In the context of cyber security, a vulnerability, also referred to as a security vulnerability, is a flaw or weakness present in an information system, security procedures, internal controls, or implementation which can be exploited or triggered by a potential threat source [2].

2.2 Vulnerability intelligence

Vulnerability intelligence involves the systematic acquisition and comprehension of potential weaknesses in computer systems and software.

2.3 Vulnerability management

Vulnerability management is the process of identifying, classifying, prioritizing, addressing, and alleviating security vulnerabilities [3] within an organization's systems, software, and infrastructure.

2.4 Vulnerability intelligence dashboard

A vulnerability intelligence dashboard is a centralized user interface component that provides insights and data related to security vulnerabilities in a visually coherent format.

2.5 Web-based vulnerability intelligence platform

A platform, is a comprehensive software solution that supports and provides a wide range of specific functions and services. It includes multiple components that enable data storage, processing, analysis, and other application functionality. A web-based vulnerability intelligence platform, in the current context, refers to comprehensive software solution that provides the functionality to aggregate, process and distill vulnerability information into a concrete vulnerability intelligence, that can be accessed through a web browser over the Internet [4].

3. PROBLEM STATEMENT

There are inherent challenges when attempting to gain vulnerability intelligence from open-source vulnerability databases. First, the current vulnerability databases are fragmented when considering the entire landscape of tools, languages and frameworks used for developing software. They use diverse structure, formats, and taxonomies. This fragmentation makes it difficult for organizations to comprehensively track them and have a unified view of the vulnerabilities. Second, vulnerability databases themselves provide a sheer overload of information that can be extremely overwhelming. This requires the monumental task of sifting through large quantities of information that identify the pertinent vulnerabilities specific to each environment. Both these problems cause inefficiencies in vulnerability management and increase the security risks by increasing the likelihood of critical vulnerabilities being overlooked.

In view of the above challenges, the need for a vulnerability intelligence platform arises that can aggregate information about pertinent vulnerabilities from multiple vulnerability databases, converge the vulnerability insights and allow them to be distilled, specific to each development ecosystem. This need leads to the following two research questions –

- First, how can organizations efficiently aggregate and standardize data from the diverse vulnerability databases available?
- And second, how can organizations extract/distill relevant and actionable vulnerability information without getting overwhelmed by the information overload?

Additionally, the field of cyber forensics dealing with analysis of evidence linked with software, can gain significantly from vulnerability intelligence. A comprehensive foundational knowledge of vulnerability insights and attack vectors is required in crimes and cases where software is involved for performing an unintended or unauthorized activity for a malicious purpose, so that an attack or an incident methodology may be understood. The current fragmented databases and repositories pose a challenge for the cyber forensic analyst and require considerable time and effort to collect all information that may help in the analysis. This need leads to the following third research question:

- How can the fragmented information present in open-source vulnerability databases and separately maintained attack pattern CAPEC repository be efficiently linked and intuitively presented to save time and effort in forensic analysis when attempting to search known attack methods that use known vulnerabilities?

4. BACKGROUND, CONTEMPORARY APPROACHES AND RELATED WORKS

4.1 Vulnerability databases

Vulnerability databases are a foundational component within vulnerability management, as they play a key role in the identification, tracking, and management of vulnerabilities in software and hardware. They store known vulnerabilities in various technological systems, software applications, and hardware components along with their characteristics such as technical details, severity and affected versions in their own standardized taxonomies and often have scoring systems that prioritize them accordingly. Regularly managed and updated vulnerability databases are extremely valuable to organizations and the cyber security community, as they guide towards developing effective and proactive defense strategies.

In order to provide a solution for the posed research questions, two well-maintained and community driven vulnerability databases, along with some related repositories were identified that are discussed next.

4.2 The Open-Source Vulnerability (OSV) Database

The OSV database is a distributed vulnerability database that essentially aggregates and indexes vulnerability data from databases that record vulnerabilities of open-source software [5] and use the schema defined by OSV. It is an ongoing effort and its current data sources include GitHub Advisory Database, PyPI Advisory Database, Go Vulnerability Database, Rust Advisory Database, Global Security Database, OSS-Fuzz, Rocky Linux (BSD), AlmaLinux (MIT), Haskell Security Advisories, RConsortium Advisory Database (Apache 2.0) and Python Software Foundation Database [5].

4.3 The National Vulnerability Database (NVD)

The NVD is the official United States government repository of standardized vulnerability management data. The NVD repository consists of references to security checklists, documented software vulnerabilities, misconfiguration information, nomenclature for products and metrics assessing the impact of these vulnerabilities [6]. Originally created in 1999 [7], it is a product of the NIST Computer Security Division.

The Common Vulnerabilities and Exposures (CVE) comprises vulnerabilities identified within specific codebases and software applications, each uniquely identified by a CVE ID. While the CVE is maintained by the MITRE corporation, the NVD analyzes each CVE, post getting published in the CVE list and adds reference tags, CVSS scores, CWE and CPE applicability statements [6]. The NVD is fully synchronized with the CVE list ensuring that any changes or additions to CVE are near instantly reflected in the NVD. In general, CVEs are available within an hour of their initial publication in the NVD. NVD builds upon the CVE List and enhances each CVE record by adding information that include severity scores and impact ratings, additional search parameters such as searching by the name of the operating system's vendor, product, and/or version number, as well as the type of vulnerability.

4.4 Common Weakness Enumeration (CWE)

The Common Weakness Enumeration is a list of software and hardware weakness types created and maintained by a collaborative community effort [8]. CWE describes and categorizes vulnerabilities in software and hardware, helping in identification of these weaknesses in systems and is also maintained by MITRE.

4.5 Common Attack Pattern Enumeration and Classification (CAPEC)

An attack pattern describes typical characteristics and approaches/techniques employed by adversaries to exploit known weaknesses to compromise a software or hardware system's security. MITRE's CAPEC is a catalogue of categorized attack patterns targeting vulnerabilities in both software and hardware. An attack pattern can help understand how adversaries attempt to exploit vulnerabilities and can not only benefit organizations trying to protect against those vulnerabilities but can also help analysts understand how an attack might have happened in case of an incident [9]. This repository is an asset for the foundational understanding when performing forensic analysis of software systems.

Most CAPEC entries contain an execution flow which lists down the step-by-step instructions for an adversary to examine potential targets, understand and experiment with their assets and defensive mechanisms, if in place, and then to exploit the weakness by carrying out the exploit. This can be very helpful in the process of identification and analysis of digital evidence in software systems as it can enumerate the methods and steps an adversary may adopt to perform an activity. However, the information in CAPEC is extensive and it helps to extend it by mapping it to a CWE that it features the exploit for. This way the CWE can be correlated with the CVE ID and largely enhance the vulnerability intelligence. By definitions and purpose, the three repositories, namely, CVE, CWE and CAPEC are closely related. A CAPEC attack pattern typically shows in steps how a weakness in CWE can be leveraged to perform an attack. CVEs are specific instances of the CWEs, whose exploitation can be demonstrated.

4.6 Role of Vulnerability Intelligence in Maintaining Security Posture for Organizations

With increasing complexity and persistence in cyber threats today, vulnerability intelligence ensures that organizations have the crucial foundational information to take actionable decisions when it comes to known vulnerabilities in their digital infrastructure, including both software and hardware. Effective cyber security defense measures require the knowledge and insights of vulnerability information inherent in the digital infrastructure, to act upon, before malicious actors can exploit them and threaten critical assets. Vulnerability intelligence is foundational in enhancing the resilience of organizations in their efforts to safeguard their critical assets mitigate security risks.

4.7 Role of Vulnerability Intelligence in Forensic Analysis

Cyber forensics in general refers to the process of identification, preservation, examination, and analysis of digital evidence in computer crime investigations [10]. In cyber forensics, the crucial part of the analysis process is to be able to understand how an incident might have occurred and what evidence trails may be left behind for analysis. Vulnerability intelligence plays a subtle but vital role in this regard. Software vulnerability intelligence can efficiently point an analyst to the techniques and methods that may have been employed to exploit a software or application to manifest an unauthorized or unintended activity. This can play a vital role in cases where the trail of evidence is not directly evident. Attack patterns alongside vulnerability intelligence from known vulnerabilities can aid the process in forensic analysis by pointing to the attack vectors that may have been used by the adversaries.

4.8 Research Motivation

The vulnerability databases such as NVD and OSV are valuable and knowledge rich resources, however, they are often each presenting either segregated or overlapping information. The software development domain consists of multiple ecosystems of technologies, each with their own supported technology stack. In such a scenario, there is a need to integrate these valuable knowledge resources offered through various sources so that, not only semantic connections can be established within the existing

knowledge, but also provide the capability to infer and deduce new insights from the knowledge set. This need for convergence forms the primary motivation to work upon a solution that can comprehensively present vulnerability intelligence in a consistent format. However, the information overload and the eventual data explosion from multiple vulnerability databases poses challenges for organizations to when attempting to make informed decisions. Any manual effort in aggregation or categorization only delays and introduces errors in presentation of pertinent information. This presents the need for a solution that can distill and prioritize them specific to individual development ecosystem Furthermore, as mentioned earlier, the field of forensic analysis can gain significant advantages from a vulnerability intelligence platform that can aid in the analysis of attack scenarios. It is yet another crucial motivation to develop a platform that is advantageous in a multi-disciplinary fashion.

4.9 Contemporary Approaches for Vulnerability Intelligence

Traditionally, vulnerability intelligence platforms may aggregate data from many sources without adding any context to the information. Such extensive information without any added context or distillation may prove extremely overwhelming and burdensome when attempting vulnerability analysis or gathering vulnerability intelligence. Often in such scenarios, threat intelligence platforms often configure their intelligence from only the most rated vulnerabilities [11] and while this approach is more focused if the aggregation context is in alignment with the needs of the organization, this strategy may eventually cause loss of valuable vulnerability information for a different context than what is presumed. Furthermore, while initially, monitoring selective feeds individually may appear to address the issue of information overload, this method ultimately falls short in providing a comprehensive view and can potentially result in the inefficient expenditure of both effort and time.

The current approaches for fetching vulnerability intelligence are in lines with one of the following three methodologies:

- Building an Application Programming Interface (API) to serve relevant vulnerability lists. APIs provide real time access to the data and the search parameters provide significant flexibility to retrieve pertinent data. The search parameters can range from date ranges and specific keywords to a specific vulnerability identifier. The results are in the form of the individual standardized schemas as supported by the repository chosen and vary from source to source. The information overload is still predominant here as the formats may be too complex for parsing them easily via scripts. APIs, when provided free of cost, often have a rate limit or access limit associated with their use. However, they serve as the common data feeds for most vulnerability intelligence products since they are more flexible and usually offer a rich dataset. Examples include the NVD APIs.
- Providing a complete downloadable repository of the compiled data in a suitable format. These formats are often in CSV, HTML, JSON or XML format and they ensure that the entire data is directly accessible for processing as per one's requirements and does not depend on constant network connections. However, this also requires constantly ensuring that the downloaded version is up to date and requires preprocessing every time a new downloadable version of the repository is available. Examples include the MITRE's CVE list.
- Providing vulnerability data feeds for consumption at regular intervals. This mode requires regular connection with the data feeds and periodically updating the vulnerability data mirrored from the main repository through available options. However, the cyber security practitioner community has often deemed that APIs are a significantly better option over data feeds when web-based automation is in consideration [12]. Examples include the Kaspersky open-source software threats data feed and several data feeds provided by NVD.

4.10 Related Works

Vulnerability scanners work in close relation with vulnerability databases for vulnerability management and hence, often become synonymous. Tools like Greenbone Networks' OpenVAS and Tenable's Nessus work with customized CVEs [13], many of which are indexed from NVD. However, these vulnerability databases stay as a proprietary feed for the tools themselves and cannot be aggregated with other sources. NVD and OSV are the two prominent databases that allow for open-source collaboration through their feeds and data buckets. However, both work with different schemas to represent information.

4.11 Limitations

While all approaches available for building vulnerability intelligence involve preprocessing of data aggregated in order to derive pertinent insights, the mode of collecting and persisting the vulnerability data plays an important role in efficiency of the vulnerability intelligence product. Most contemporary products in the vendor market build their vulnerability intelligence from one or more common vulnerability repositories, processing them according to their design and updating it over the network from time to time. This processing is often kept proprietary and apart from a mention of the names of vulnerability databases used, mostly CVE, everything is opaque to the user. On the other hand, the open-source products or tools are often very simplistic and pre-customized with much less flexibility. They define their own limitations, depending on the resources available with them and may not suffice for organizations which intend to build a comprehensive vulnerability intelligence. Even official vulnerability scanners such as the OSV scanner, which build upon the OSV database itself [5], produces output in simple text format that requires further codebase processing and development to produce visual dashboard level insights. This extra effort is provided with proprietary solutions mostly and has the added financial cost of licenses.

5. PROPOSED SOLUTION

A solution to the above-mentioned research questions is presented that addresses to the limitations discussed. This solution that has been developed as a web-based software application, can present insights in the form of vulnerability intelligence from known vulnerability information targeting software applications built using either open-source technology stacks or proprietary software. This vulnerability information has been aggregated from two open-source vulnerability databases, namely OSV database and NVD. The software application has also integrated the attack pattern repository from MITRE CAPEC (Common Attack Patterns Enumeration and Classification) and utilized data from the MITRE CWE list to map them with the corresponding entries in the aggregated vulnerability database. The web-based vulnerability intelligence platform, alternatively referred to as *WebVIP* or "system" from henceforth, aims to function as a vulnerability intelligence platform with the following key features –

- It has defined a *Unified Schema* for the vulnerability information into which the data from the integrated vulnerability databases has been transformed and persisted in a local database for consistency. This will bring about convergence of the vulnerability information from multiple sources into a single, standardized format.
- It has built in components that can periodically collect data from the OSV and NVD databases and process it in order to persist the data in the defined unified schema.
- It has the functionality to collect and persist data from the CAPEC repository and the CWE list locally and use them to link the data to the aggregated vulnerability information.
- It processes the aggregated data to generate vulnerability intelligence and link insights about attack patterns that can be used for vulnerability management and forensic analysis.

The users can interact with the vulnerability intelligence platform through two modes. First, a web-based software application that will primarily present a vulnerability intelligence dashboard through its user interface, and second, a set of well-defined APIs that will be used for collaboration with external systems.

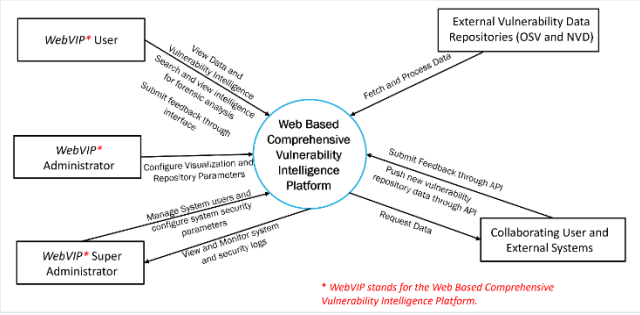

Figure 1 – Context diagram for the system

The system identifies five actors/external entities that can interact with it, namely, the user, the administrator, the super administrator, the external vulnerability data repositories, and the collaborating user/external systems (Figure 1). The user actor is the system user who will have access to the configured vulnerability intelligence dashboard and related user interfaces. The administrator actor is the system user authorized with privileges to configure the visualization and repository parameters for the system. The super administrator actor has the highest privileges to manage the role and access assignment of the remaining users in the system. This user also processes requests for registering collaborating users or external systems that wish to access the system's APIs. The external vulnerability data repositories actor represents other external open-source databases being used to aggregate vulnerability data and derive intelligence from. Lastly, the collaborating user/external systems actor represent the users who wish to access the aggregated data and intelligence data through an API and not through the user interface. They represent the external systems who wish to use, analyse, or build upon the data. They can also submit feedback through an API.

5.1 Core Modules of WebVIP

The architecture has been illustrated in Figure 2.

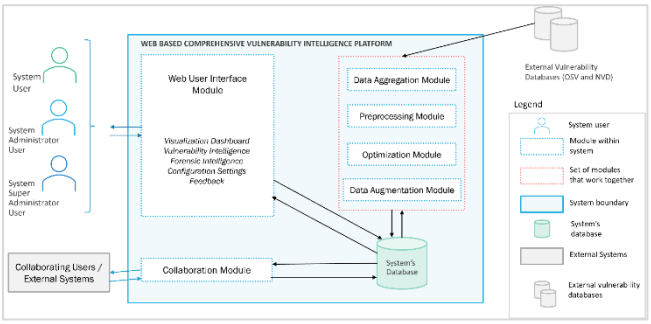

Figure 2 – System architecture diagram

The core modules developed for the vulnerability intelligence platform WebVIP are listed below:

- Data aggregation module
- Preprocessing module
- Optimization module
- Data augmentation module
- Web User Interface module
- Collaboration module

The data aggregation module is the module that periodically collects vulnerability data for the system. This periodicity is scheduled as per the external system constraints (For example, if the external repository updates their database every night, the periodicity can be set for every morning). Once an iteration from the data aggregation module is completed, the preprocessing module is scheduled to perform the task of transforming the data into the consistent format as defined for the system. After an iteration from the

preprocessing module is completed, further optimizations and categorizations are performed by the optimization module. This task is necessary to bring the data into a state optimal for generating vulnerability intelligence and includes data categorization, data organization, and parameter optimization. While the data augmentation module is responsible to collect data from the CAPEC repository and extend it using CWE list so that it can be linked with the aggregated vulnerability repository, the web user interface module is responsible for providing the means of interaction between the system users and system itself. Finally, the collaboration module provides the interoperability features for the external systems that wish to work with the data aggregated and/or the vulnerability intelligence generated by the system without using the web user interface module. This delivers the flexibility to enhance the data being requested without requesting changes in the system itself.

5.2 Interoperability Aspects

The developed vulnerability intelligence platform has two chief capabilities that allow the solution to interoperate with external systems. First, it has a standardized data format to consume the vulnerability data for future integrations, called the unified schema. Second, it exposes well- defined RESTful APIs (APIs that following the *Representational State Transfer* architectural style for exchanging data over the Internet) for external software systems to consume the aggregated vulnerability repository. Further, the main point of access to the platform is through a web user interface which has been built in compliance with the latest web standards ensuring cross browser interoperability.

5.3 Collaboration Aspects

The system supports collaboration with the users, both who directly use the vulnerability intelligence user interface and those who wish to interact with the data consumed by the external software systems. Additionally, it provides a feature to add feedback for integrations with external software systems, so that the vulnerability intelligence can be accordingly re-organized to show restructured priority for the specific usage.

5.4 Configurability Aspects

The developed system provides the ability to configure or modify several parameters through its user interface. The default ecosystem for which vulnerability intelligence is to be generated can be customized for each user. The aggregated vulnerability repository can be enhanced from another data source by configuring API information that can be consumed periodically to append the information to the overall system. Further, the collaboration with external software systems can also be managed through a configuration user interface.

5.5 Data Aggregation and Augmentation Strategies

For collecting data from OSV, it was found feasible to periodically download the complete zipped JSON files archive from the data dumps provided through their GCS bucket and process it (GCS bucket maintained by OSV at gs://osv-vulnerabilities [15]). This can be done timely through a scheduled application process over an encrypted web channel. For integration with NVD, the API mode of integration [15] best suited the mirroring the data, once completely and then incrementally.

To enhance the aggregated vulnerability data to suit the needs for being able to aid in forensic analysis process for software systems, the CAPEC repository, has been utilized for data augmentation. Given the CAPEC repository and CWE list are available for download in csv (comma separated values) format, their latest versions were both imported directly into the local database and further processed according to the needs for mapping and linking.

5.6 The Unified Schema for Seamless Integration

The OSV database transforms and stores the data from the multiple open-source databases into a custom schema, that grew from the vulnerability interchange schema, having gone several iterations of change [5]. Similarly, the NVD database maintains a standard format to keep the vulnerability records. These two records are different in several aspects and in order to integrate the data from these two sources to present the converged vulnerability insights, the schemas needed to be unified. This new unified schema developed for the system, not only provides relevant information without any data loss from either source, but also reduces the noise from unnecessary data fields, or data fields that may not be needed for current context.

Under the unified schema, all records are aggregated together under a unique identifier for every vulnerability record, called VIP ID (represented by *vip_id* in the format). This unified schema forms the crux of the convergence of vulnerability insights from multiple sources. It has been structured in JSON format and is composed of the fields as summarized in Table 1.

Table 1 – The Unified Schema Format

Field Name	Requirement	Field Value Type
vip_id	mandatory	string
source_name	mandatory	string
source_vuln_id	mandatory	string
ecosystem	optional	string
vulnerability_description	mandatory	object
source_published	mandatory	string
response_version	mandatory	string
response_timestamp	mandatory	string

affected_detail	optional	array of objects
references	optional	array of objects
metrics	optional	object
linked_weaknesses	optional	array of string
linked_capec	optional	array of string
vip_severity	mandatory	String
source_db_additional_info	optional	array of objects

5.7 User Interfaces of the Developed Platform

The user interfaces presented by the Web User Interface module present the results of the endeavor. While the complete functioning of the solution is out of scope for this paper, the screenshots of some of the primary user interfaces are shown below.

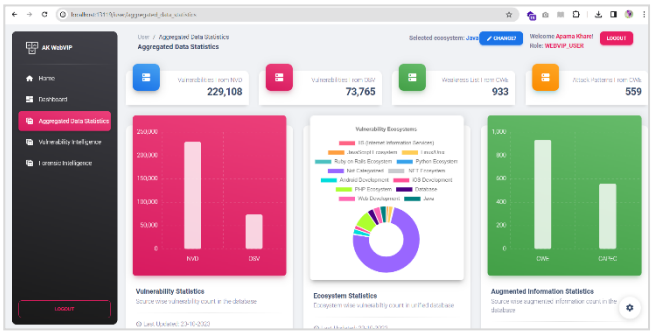

Figure 3 – Vulnerability Statistics Dashboard

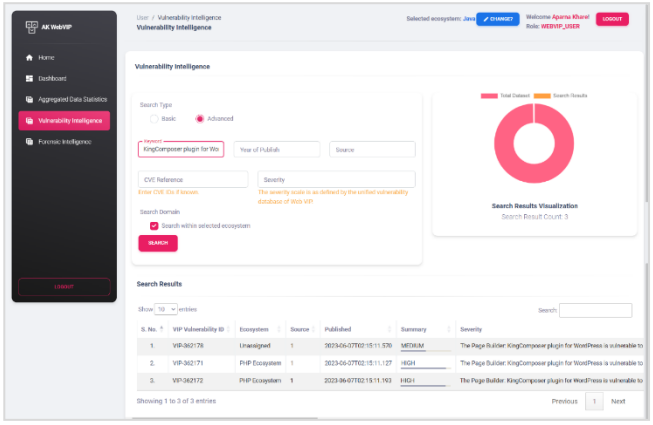

Figure 4 – Vulnerability Intelligence Search and Results

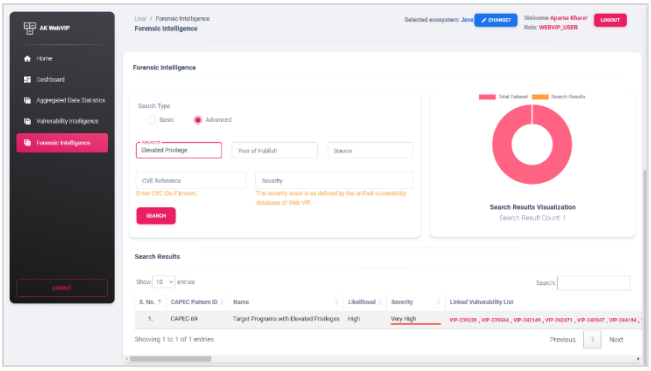

Figure 5 – Forensic Intelligence Search and Results

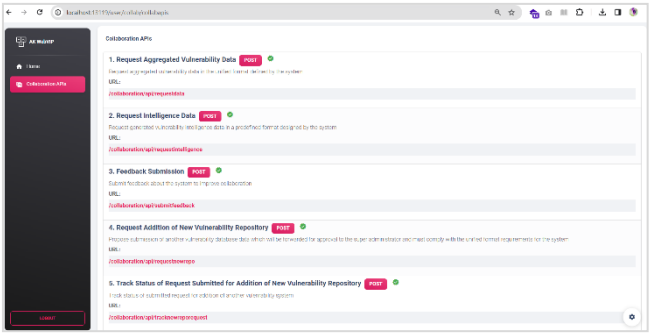

Figure 6 – Listing of Collaboration APIs for Collaborating User

5.8 Chosen Technology Stack for Development

The system has been developed using Java Spring Boot, a Java development framework that streamlines the development process for building robust and scalable web applications, Spring Web MVC, a part of the Spring framework of Java that provides clean separation of concerns through its Model-View-Controller architecture, and PostgreSQL, a community-driven open-source relational database management system.

6. RESULTS AND BENEFITS BROUGHT BY THE DEVELOPED SOLUTION

The developed vulnerability intelligence platform, WebVIP, defines an efficient automation of integration process from standardized vulnerability information databases, namely NVD and OSV database and augments only relevant information from the linked CWE list and CAPEC repository. The vulnerability information can be distilled through the user interfaces without getting overwhelmed by the information overload. The ecosystem configurability options aid in the process of distilling the information. This solution brings forth the following results –

- It enhances usability by presenting an intuitive dashboard with visualization and most relevant vulnerabilities at the first glance, making interpretation much easier and effective.

- It reduces information overload by providing filtering capabilities to only view relevant intelligence linked with a specific software ecosystem.
- It aggregates data from two comprehensive and standard community driven databases in a unified format and augmenting only relevant information aiding in quality with understandability.
- It opens the platform for integration for any future vulnerability databases through data interchange in the unified schema format.
- It brings about options for collaborations by sharing the vulnerability intelligence generated through REST APIs.

7. DIRECTIONS FOR FUTURE WORK

The developed system has strong potential to be further enhanced by efforts in several avenues. To ensure a richer body of knowledge to work upon, more reliable vulnerability databases may be aggregated. The existing vulnerability information can be enhanced by remapping to more concrete categorizations for ecosystems. Additionally, user feedback can be used to improve and update the severity and relevance of existing information. Another avenue for future work for enhancing the capabilities can be the exploration of incorporation of machine learning algorithms which can improve the system's capacity to anticipate and prioritize potential vulnerabilities by analyzing existing data and patterns.

8. CONCLUSION

The developed solution brings about enhanced usability by bringing the vastly fragmented vulnerability information together and converging them into valuable vulnerability insights. Its integration with NVD and OSV for centralized aggregation of vulnerability data and collaboration options through REST APIs, aligns with broader standardizations efforts for vulnerability information. It aims to bring all the available data under one single point of access to make handling of vulnerability information more efficient and fruitful. The key benefit of facilitating informed decision making in vulnerability management and minimizing information overload by only focusing on relevant and prioritized insights through visual interfaces greatly aids in the process of improving the security posture of the organization. In addition to that, the collaboration avenue that this solution opens can greatly enhance the value and ensure the solution stays relevant and beneficial to the community.

REFERENCES

[1] Q. &. S. D. &. F. M. &. S. K. Covert, "Towards a Triad for Data Privacy," in Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020.

[2] "NIST Computer Security Resource Centre," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/vulnerability. [Accessed 09 2023].

[3] P. Foreman, Vulnerability Management, CRC Press, 2019.

[4] "WHAT IS A WEB APPLICATION?" Stackpath, [Online]. Available: https://www.stackpath.com/edge-academy/what-is-a-web-application/. [Accessed 09 2023].

[5] "Google Security Blog," Google, [Online]. Available: https://security.googleblog.com/2021/06/announcing-unified-vulnerability-schema.html. [Accessed 09 2023].

[6] NIST, "NIST National Vulnerability Database," [Online]. Available: https://nvd.nist.gov/. [Accessed 09 2023].

[7] "NIST National Vulnerability Database: General Information," [Online]. Available: https://nvd.nist.gov/general. [Accessed 09 2023].

[8] "CWE - Common Weakness Enumeration," MITRE, [Online]. Available: https://cwe.mitre.org/. [Accessed 09 2023].

[9] "About CAPEC," MITRE, [Online]. Available: https://capec.mitre.org/about/index.html. [Accessed 09 2023].

[10] J. D. M. Albert J. Marcella, Cyber Forensics, CRC Press, Taylor & Francis Group, 2010.

[11] "CISA Launches Known Exploited Vulnerabilities (KEV) Catalog," [Online]. Available: https://www.securin.io/articles/cisa-launches-known-exploited-vulnerabilities-catalog/. [Accessed 09 2023].

[12] "What is the difference between a Feed and an API as export channel?," [Online]. Available: https://helpcenter.channable.com/hc/en-us/articles/360011205739-What-is-the-difference-between-a-Feed-and-an-API-as-export-channel. [Accessed 09 2023].

[13] "CVEs Tenable," Tenable, [Online]. Available: https://www.tenable.com/cve. [Accessed 07 2024].

[14] "Bucket Details: osv-vulnerabilities," [Online]. Available: https://console.cloud.google.com/storage/browser/osv-vulnerabilities. [Accessed 09 2023].

[15] "NVD Full Listing," NIST, [Online]. Available: https://nvd.nist.gov/vuln/full-listing. [Accessed 09 2023].