OPEN ACCESS

Kashf Journal of Multidisciplinary Research
Vol: 03 - Issue 03 (2026)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

RISKVISTA: A COMPREHENSIVE STUDY OF SECURITY TOOL INTEGRATION, CYBER RISK SCORING, AND DASHBOARD-BASED DECISION SUPPORT IN ENTERPRISE ENVIRONMENTS

[1]Muhammad Usama khan, [2*]Muhammad Zamin Ali Khan, [3]Syed Talib Zaheer Zaidi,[4] Amad Asif, [5]Khalid Bin Muhammad,[6]Faigha Karim, [7]Ammad Mallick

[1]UHF Solutions Pvt Ltd, Karachi, Pakistan

[2]Department of Computer Science, Iqra University, Karachi, Pakistan

[3]HBL, Karachi, Pakistan

[4]Graphica Pro Artistry (Australia, Broadmeadows, Victoria)

[5]COCSE, Ziauddin University, Karachi, Pakistan

[6]Department of Computer Science, Iqra University, Karachi, Pakistan

[7]Department of Computer Science, Cardiff Metropolitan University, London, UK

[*]Corresponding Author: (muhammad.zamin@iqra.edu.pk)

DOI:(*https://doi.org/10.71146/kjmr878*)

Article Info

Abstract

Organizations utilize several security solutions (vulnerability scanners, static code analyzers, network discovery tools) for continuous cyber posture monitoring. Despite the high information value provided by such tools, it is difficult to unify, correlate, and interpret the outputs generated due to the disparate nature of the data. This significantly hinders the visibility and prioritization efforts of an organization. In this paper, I propose RiskVista, an open-source cyber risk assessment and integration prototype which gathers vulnerability data and asset information from various security tools using RESTful APIs or file imports, normalizes these data into a canonical form ACS (asset-centric schema) and calculates normalized risk scores for assets and business capabilities. RiskVista implements an understandable composite risk scoring system based on severity i.e CVSS, exposure, exploitability, and impact to the business. Scores range from 0 to 100 with corresponding letter grades to provide more intuitive understanding of the problem and allow triage. The solution features a web providing access to several dashboards including tool onboarding, vulnerabilities overview, most vulnerable assets, and business capability level risks. An evaluation methodology will be designed for future implementation of RiskVista.

Keywords: *Cybersecurity, Cyber Risk Assessment, Vulnerability Management, Risk Scoring*

1. INTRODUCTION

Cybersecurity has matured from a mere technical practice into an operational and strategic activity that impacts the availability of service, trust of customer, liability and continuity of business operations. With increased adoption of cloud services, micro services architecture, APIs and remote working, there has been an increase in managed assets and hence attack occurs. To mitigate cyber risks, enterprises utilize specific security toolkits such as vulnerability management (VM), static application security testing (SAST) tools and network scanners. Although these tools offer important detection capabilities, they present integration problems due to duplicated findings, varied severity scoring, different asset inventories, and fragmented reporting. An identified problem is the gap in transforming technical cybersecurity findings into relevant business risks. VM tools provide vulnerability data in form of CVSS scores, SAST provides technical findings based on repositories/components while the network scanning tools offer exposure data such as open ports and services. Managers of the business risk. RiskVista as depicted in **Figure 1** solves this problem through integration, normalization and calculation of a comparable business risk score which is then visualized using dashboards. This paper is based on three findings from previous literature: **(i)** Risk is multi-dimensional, including severity and business impact. **(ii)** Prioritization of vulnerabilities is better when severity is incorporated with other parameters such as asset criticality and remediation environment. **(iii)** situational awareness dashboards enhance decision-making capabilities.

1.1 PROBLEM STATEMENT

It is common practice for companies to run more than one security tool Example: Qualys for VM, Sonar Qube for SAST, and nmap for exposure discovery. These tools have their own output formats, data models and scoring systems. Leaving each tool's findings locked in its own separate report. Without normalization and correlation, it is difficult to develop a consistent asset inventory, compare risk across business functions and prioritize remediation in a transparent manner.

1.2 CONTRIBUTIONS

This paper provides the following contributions: **(i)** a system design for multi-tool ingestion and normalization into canonical asset-centric entities **(ii)** a transparent composite risk scoring model combining severity, exposure, exploitability, and business impact **(iii)** a prototype dashboard as shown in **Figure 5** design demonstrating executive roll-ups and technical drill-downs and **(iv)** an evaluation methodology for validating integration completeness, scoring behavior and usability in a follow-on implementation.

2. BACKGROUND AND PRELIMINARIES

RiskVista aligns with established risk management guidance that emphasizes structured assessment of likelihood, impact, and control context. Reflecting NIST risk assessment practices, the system separates evidence collection (tool outputs) from risk analysis and communication. RiskVista also supports the risk management framing in ISO/IEC 27005, where risk treatment decisions require traceable inputs and repeatable scoring. A key technical input in many organizations is the Common Vulnerability Scoring System (CVSS), which provides standardized severity scores for vulnerabilities. CVSS is widely used in VM tools and can be used as a baseline severity measure. Nevertheless, CVSS is not enough for prioritizing vulnerabilities since it does not measure asset criticality, exposure or exploitability. RiskVista considers other metrics to generate a combined rating that is better suited for organizational prioritization **[11], [12], [13].**

3. RELATED WORK

This chapter integrates previous research on five topics. Each pertinent to the RiskVista project: Risk assessment variables and models, prioritizing vulnerabilities based on contextual factors, situational awareness via dashboards, managing risks within complex systems and data limitations.

3.1 RISK ASSESSMENT VARIABLES AND QUANTITATIVE MODELS

The framework put forward by Amin et al. categorize cyber risk assessment parameters into a hierarchical taxonomy. Whereas in the asset, vulnerability, threat, probability and impact variables are considered discrete input factors to the risk assessment process. It is in line with the design rationale behind RiskVista, where multiple context factors, along with severity are stored. Sánchez-García et al. offer an extensive review on cybersecurity risk assessment models and tools and stress the importance of defining explicit variables in quantifiable risk assessment models **[1],[2].**

3.2 CONTEXT-AWARE VULNERABILITY MANAGEMENT AND PRIORITIZATION

Walkowski et al. examine models for vulnerability management that include the use of CVSS in conjunction with asset information and find that factoring in the asset provides increased prioritization efficiency. Allodi et al. note inconsistencies that may occur during vulnerability assessment due to the assessor's subjective judgment when using CVSS scoring. This is remedied by RiskVista through its use of standardized scoring rules **[3],[9].**

3.3 DASHBOARDS AND SITUATIONAL AWARENESS FOR DECISION SUPPORT

The work of Chandra et al. outlines how situational awareness models and visualization techniques enhance risk assessment processes and decisions regarding corrective actions.

Kaufhold et al. design and test an interactive dashboard for cybersecurity incidents during emergencies that highlights design considerations such as modularity in data aggregation, filtering and exporting. RiskVista incorporates similar design considerations to provide executive summaries and technical details **[4], [6].**

3.4 INTEGRATED RISK MANAGEMENT AND COMPLEX SYSTEMS

As shown in **Figure 3**, an integrated framework of cybersecurity risk management in real time emphasizes lifecycle management and dependencies. Kure et al. suggest an integrated risk management model for cyber-physical systems which focuses on cascading impacts as well as stakeholder involvement. Ouaissa et al. provide an integration of threat modeling and risk scoring in a heterogeneous environment. This illustrates the significance of using domain-specific weights in this process. Although RiskVista is developed to meet the demands of enterprises in general, the studies discussed above can inspire future improvements **[7], [8], [10].**

3.5 DATA AVAILABILITY AND PRACTICAL CONSTRAINTS

The authors state that a lack of standardized data is a structural constraint in cyber risk studies and the validation process of models. In reality, organizations encounter issues such as non-standardized tool output, non-uniform identifiers and differences in updating frequency. RiskVista resolves these constraints by employing a canonical structure, correlation and metadata for ingestion **[5].**

4. RISKVISTA SYSTEM OVERVIEW

RiskVista is an online cyber risk assessment and management platform that integrates multiple security tools by gathering their evidence data, calculating risk scores and presenting its findings using dashboards and reports. As mentioned in **Table 1** below, there are a number of high-level requirements for RiskVista's functionality.

Table 1 HIGH-LEVEL FUNCTIONAL REQUIREMENTS

ID	DESCRIPTION
FR1	Tool onboarding via API or CSV import; store connector metadata and authentication parameters.
FR2	Normalize tool outputs into a unified schema (assets, vulnerabilities/issues, findings, scans, tool sources).
FR3	Compute asset risk scores and categorical grades (Low/Medium/High/Critical).

FR4	Dashboards: vulnerability breakdown, most vulnerable assets, risk roll-up by business capability.
FR5	Search, filtering, and sorting across assets and findings (severity, status, patch availability).
FR6	User management and role-based access control (Admin, Analyst, Management).
FR7	Exportable reports (CSV/PDF planned) for technical and executive stakeholders.

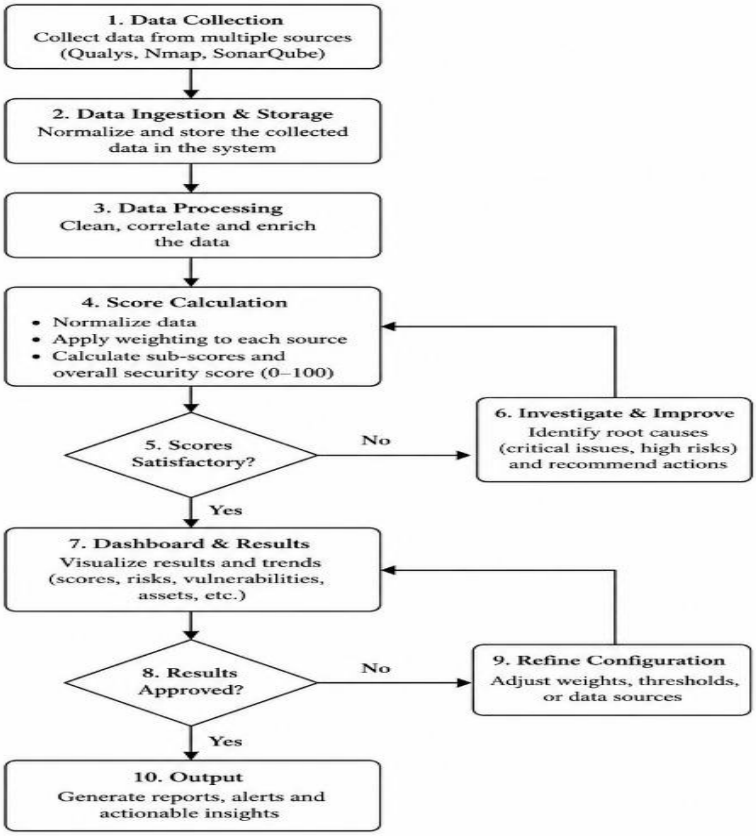

Figure 1 FLOW CHART OF THE RISKVISTA SYSTEM

5. DATA INTEGRATION AND NORMALIZATION

The RiskVista solution applies an ETL process adapted to work with data from security tools. In the extraction phase, findings are acquired using REST APIs where possible or alternatively using file imports (CSV, XML, JSON) in case there is no access to APIs. The transformation

phase includes normalization of identifiers, timestamps, scales of severity and other tool-specific fields.

5.1 TARGET TOOLS AND OUTPUT CHARACTERISTICS

RiskVista highlights three selected tools that deal with the vulnerability of the infrastructure, the problems in application code and network vulnerability: Qualys (VM), SonarQube (SAST) and Nmap (network scan). All the tools used in the system, their means of data provision and functionality are thoroughly discussed in **Table 2 [19], [20].**

Table 2 TARGET TOOLS AND INGESTION MODES

TOOL	CATEGORY	PRIMARY EVIDENCE	INGESTION MODE
Qualys	Vulnerability Management	Host vulnerabilities (CVE/CVSS), patch status	API (JSON) or CSV/XML
SonarQube	SAST	Code vulnerabilities/issues, project and component metadata	API (JSON) or XML
Nmap	Network Scanning	Host reachability, open ports, service versions, OS guess	XML/CSV or parsed text

5.2 CANONICAL DATA MODEL

This model is comprised of three components: Asset, Vulnerability/issue and Finding. The term Asset refers to hosts, applications or devices. The term Vulnerability/Issue refers to weaknesses' identifiers like CVEs, CWEs or tool rules. For more information, see **Table 3** which shows key fields and notes of assest, vulnerability and finding. Finding means that a certain vulnerability or issue is present on an asset at a certain point in time **[18].**

Table 3 CANONICAL ENTITIES (LOGICAL SCHEMA SUMMARY)

ENTITY	KEY FIELDS (ILLUSTRATIVE)	NOTES
Asset	asset_key, ip, hostname, type, owner, business_capability	Supports infrastructure assets and application assets.
Vulnerability/Issue	weakness_id (CVE/CWE/rule), title, description, published_date	De-duplicated across tools when possible.
Finding	finding_id, asset_key, weakness_id, tool_id, severity, status, first_seen, last_seen	Links tools to canonical assets and weaknesses.

6. COMPOSITE RISK SCORING MODEL

This engine transforms the results to an equivalent measure used for ranking and prioritizing. RiskVista uses an open and weighted composite methodology based on four parameters, namely: severity, exposure, exploitability and business impact.

6.1 FACTORS AND DEFINITIONS

Severity is obtained from CVSS (see

Figure 6) if present (as in Qualys) or

mapped severity categories (as in SonarQube). Exposure considers external accessibility or attack surface indicators like open ports and internet facing condition. Business impact accounts for asset criticality and business capability importance **[14],[15],[16], [21],[22],[23], [24] [25].**

6.2 SCORE FORMULA AND WEIGHTING

RiskScore_raw = (0.4 x Severity) + (0.2 x Exposure) + (0.2 x Exploitability) + (0.2 x BusinessImpact).

Final score is in between 0 to 100 for reporting and categorizing.

7. SYSTEM ARCHITECTURE AND IMPLEMENTATION

RiskVista has a web application structure that is based on a modular architecture design. These layers include presentation, application, analysis and data layers. Details of each individual layer are described in **Table 4** below. Connectors pull information from outside applications and put the data into the normalization process. The scoring engine analyzes and scores assets and roll-ups, which will be displayed using dashboards.

Table 4 LOGICAL COMPONENTS AND RESPONSIBILITIES

COMPONENT	RESPONSIBILITIES
Web UI	Login as shown in **Figure 2**, tool setup, dashboards, reports, search and filtering.
Backend Services	Auth and RBAC, tool management, ingestion orchestration, dashboard query API.
Connectors	API pulls or file imports; schema validation; metadata capture.
Normalization and Correlation	Field mapping, de-duplication, asset matching, canonical entity creation.
Risk Scoring Engine	Factor derivation, composite scoring, categorization, roll-up aggregation.
Database	Persistent storage for assets, findings, scores, tool metadata, logs.

8. PROTOTYPE USER INTERFACE DEMONSTRATION

This chapter presents the prototype interface using screenshots. This interface showcases the entire process flow including login, managing connectors, configurations as shown in **Figure 4**, ingestion views, and dashboards for reporting and visualization.

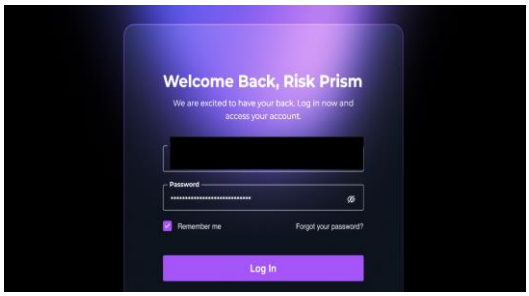

Figure 2 PROTOTYPE LOGIN INTERFACE (USER IDENTIFIER REDACTED)

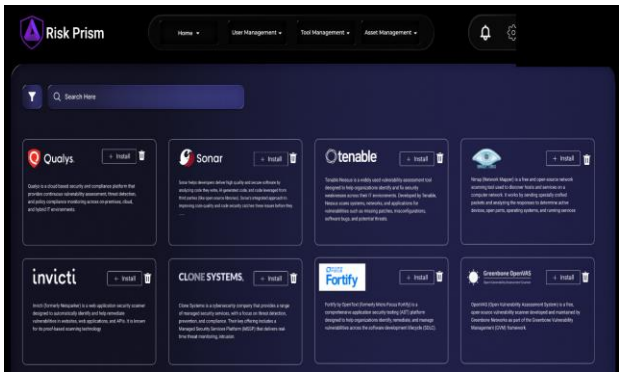

Figure 3 TOOL MANAGEMENT SCREEN SHOWING INSTALLABLE CONNECTORS

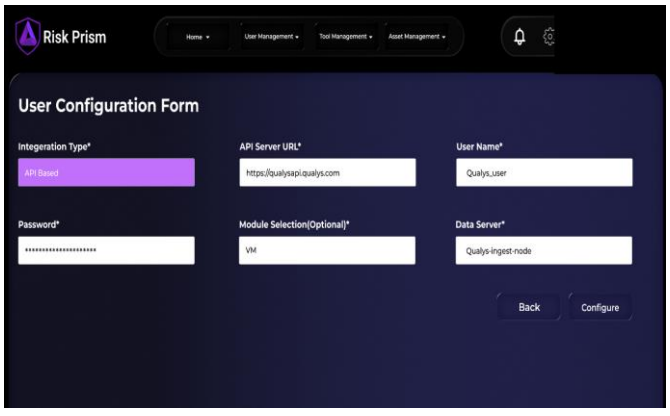

Figure 4 EXAMPLE TOOL CONFIGURATION FORM FOR AN API-BASED CONNECTOR

(USER DETAILS REDACTED)

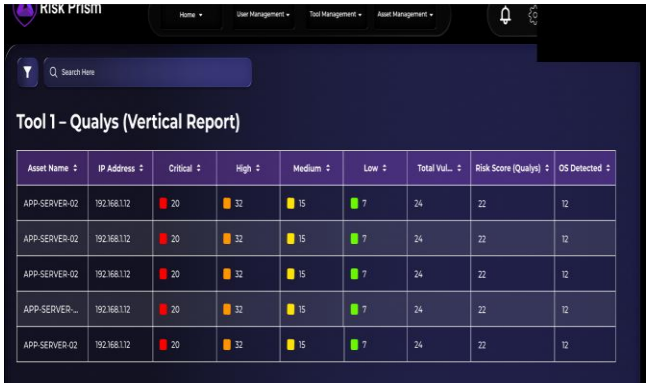

Figure 5 TOOL-SPECIFIC VERTICAL REPORT (QUALYS EXAMPLE) SHOWING ASSET VULNERABILITY SUMMARY

Figure 6 VULNERABILITY BREAKDOWN VIEW WITH CVSS, STATUS, AND PATCH AVAILABILITY

9. CONCLUSION AND FUTURE WORK

RiskVista was first introduced in this paper, which is a cyber risk assessment and integration solution that aggregates evidence from multiple tools, normalizes the evidence to canonical representations, calculates explicit composite risk scores and reports back through dashboards. This idea is based on literature related to the subject areas like factors influencing cyber risks, vulnerability scoring and prioritization schemes and use of dashboards for situational awareness. The future work involves implementation of resilient connectors, making canonical schema and the scoring engine operational, and validating solution per the outlined methodology in this paper. Furthermore, the plan is to implement additional features like enriching evidence with exploit intelligence using EPSS/KEV score and/or computing dependency-aware risk score and conducting attack path analysis as an option for assets connected heavily. Plans for the future work involve: Developing and securing connectors for ingestion of the data from the target tools i.e Qualys, SonarQube, Nmap with resilience, error handling, retry and scheduling capabilities. Implementing canonical database schema including integrity constraints and indexing. Operationalizing the scoring engine with storing factors contribution for explainability within the

UI. Adding advanced correlation logic such as host to application mappings, and deduplication for cross scanner detected CVEs. Implementation of report generation capabilities for generating CSV and PDF files.

REFERENCES

Z. M. Amin, N. Anwar, M. S. Mohd Shoid, N. R. Ahmad, and S. Samuri, "Discovering the Variables of Cyber Risk Assessment Through a Systematic Literature Review," Journal of Information and Knowledge Management, vol. 15, Special Issue 2, pp. 55-65, Aug. 2025, doi: 10.24191/jikm.v15iSI2.7241.

I. D. Sanchez-Garcia, J. Mejia, and T. San Feliu Gilabert, "Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation," Applied Sciences, vol. 13, no. 1, Art. no. 395, 2023, doi: 10.3390/app13010395.

M. Walkowski, J. Oko, and S. Sujecki, "Vulnerability Management Models Using a Common Vulnerability Scoring System," Applied Sciences, vol. 11, no. 18, Art. no. 8735, 2021, doi: 10.3390/app11188735.

N. A. Chandra, K. Ramli, A. A. P. Ratna, and T. S. Gunawan, "Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools," Risks, vol. 10, no. 8, Art. no. 165, 2022, doi: 10.3390/risks10080165.

F. Cremer, B. Sheehan, M. Fortmann, A. N. Kia, M. Mullins, F. Murphy, and S. Materne, "Cyber Risk and Cybersecurity: A Systematic Review of Data Availability," The Geneva Papers on Risk and Insurance - Issues and Practice, vol. 47, pp. 698-736, 2022, doi: 10.1057/s41288-022-00266-6.

F. A. Kaufhold, M. Rohen, and C. Reuter, "Cyber Threat Observatory: Design and Evaluation of an Interactive Dashboard for Computer Emergency Response Teams," in Proc. European Conf. on Information Systems (ECIS), Timisoara, Romania, 2022.

H. I. Kure, S. Islam, and M. A. Razzaque, "An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System," Applied Sciences, vol. 8, no. 6, Art. no. 898, 2018, doi: 10.3390/app8060898.

M. Ouaissa, M. Ouaissa, Z. Nadifi, S. El Himer, Y. Al Masmoudi, and A. Kartit, "A Framework for Cyber Threat Modeling and Risk Assessment in Smart City Environments," Frontiers in Computer Science, vol. 7, Art. no. 1647179, 2025, doi: 10.3389/fcomp.2025.1647179.

L. Allodi, M. Cremonini, F. Massacci, and W. Shim, "Measuring the Accuracy of Software Vulnerability Assessments: Experiments with Students and Professionals," Empirical Software Engineering, vol. 25, no. 2, pp. 1063-1094, 2020, doi: 10.1007/s10664-019-09797-4.

R. C. Poonia, K. Upreti, B. P. Alapatt, and S. Jafri, "Real-Time Cyber-Physical Risk Management Leveraging Advanced Security Technologies," in Proc. 9th Int. Congress on Information and Communication Technology (ICICT 2024), Lecture Notes in Networks and Systems, vol. 1011, Springer, Singapore, pp. 339-350, 2024, doi: 10.1007/978-981-97-4581-4_25.

National Institute of Standards and Technology (NIST), "Guide for Conducting Risk Assessments," NIST Special Publication 800-30 Rev. 1, Sep. 2012, doi: 10.6028/NIST.SP.800-30r1.

National Institute of Standards and Technology (NIST), "Managing Information Security Risk: Organization, Mission, and Information System View," NIST Special Publication 800-39, Mar. 2011, doi: 10.6028/NIST.SP.800-39.

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), Information Security, Cybersecurity and Privacy Protection - Information Security Risk Management, ISO/IEC 27005:2022, 2022.

FIRST.Org, Inc., "Common Vulnerability Scoring System Version 3.1: Specification Document (Revision 1)," 2019. [Online]. Available: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

J. Jacobs, S. Romanosky, B. Edwards, I. Adjerid, and M. Roytman, "Exploit Prediction Scoring System (EPSS)," Digital Threats: Research and Practice, vol. 2, no. 3, pp. 1-17, 2021, doi: 10.1145/3436242.

Cybersecurity and Infrastructure Security Agency (CISA), "Known Exploited Vulnerabilities (KEV) Catalog." [Online]. Available: https://www.cisa.gov/known-exploited-vulnerabilities-catalog. Accessed: Jan. 18, 2026.

National Institute of Standards and Technology (NIST), "National Vulnerability Database (NVD)." [Online]. Available: https://nvd.nist.gov/.

The CVE Program, "Overview - About the CVE Program." [Online]. Available: https://www.cve.org/about/overview. Accessed: Jan. 18, 2026.

Qualys, Inc., Qualys API (VM, PA/PC) User Guide, ver. 10.37, Jan. 5, 2026. [Online]. https://cdn2.qualys.com/docs/qualys-api-vmpc-user-guide.pdf. Accessed: Jan. 18, 2026.

SonarSource Sarl, "Web API | SonarQube Server (Documentation)." [Online]. Available: https://docs.sonarsource.com/sonarqube-server/extension-guide/web-api/. Accessed: Jan. 18, 2026.

Hussain Saleem, M Zamin Ali Khan, et al “Towards Identification and Recognition of Trace Associations in Software Requirements Traceability” Vol 9, Issue 5, pp 257-263 Sep, 2012.

Hussain Saleem, M Zamin Ali Khan, et al “Mobile Agents: An Intelligent Multi-Agent System for Mobile Phones” Vol 6 Issue 2, pp 26-34, Oct 2012

Saim Masood Shaikh, Muhammad Zamin Ali Khan et al “NAVIGATING CONTEMPORARY CHALLENGES OF SOFTWARE QUALITY ASSURANCE IN SOFTWARE TESTING” Vol 3 Issue 9, PP 45-71, April 2025.

Humera Azam, M.Zamin Ali Khan et al, “Quality Assurance in the Digital Age: Exploring Contemporary Challenges in Software Testing” Vol 5 , Issue 2, PP 9-26, 2025

Muhammad Zulqarnain Siddiqui , Muhammad Zamin Ali Khan et al, “ANALYSIS OF THE EFFECTIVENESS OF GENERATIVE AI MODELS FOR TEXT-TO-SQL TASKS IN BUSINESS INTELLIGENCE SYSTEMS” Vol3 Issue 12, PP 1777-1794 Dec 2025