ISSN–2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XV, Special Issues– I(b) Jan – Feb, 2026

OPEN ACCESS Original Research Article

AI-ASSISTED VULNERABILITY PRIORITIZATION FOR POST-PENETRATION DECISIONS

* Nitu Nair

Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India.

Abstract:

Penetration testing is a key process for identifying vulnerabilities within organizational systems, simulating real-world cyberattacks to uncover weaknesses before exploitation. These tests often generate extensive reports with numerous findings, making it challenging for organizations to determine which vulnerabilities should be addressed first. Limited resources such as time, budget, and skilled personnel further complicate prioritization. Traditional approaches, relying mainly on technical severity scores, often fail to capture the full business impact, operational criticality, and organizational priorities, leaving critical risks unaddressed.

This research proposes an AI-assisted framework to enhance post-penetration testing vulnerability prioritization as a decision-support tool rather than a replacement for human expertise. By integrating technical severity with organizational and contextual factors such as business impact, asset criticality, exploit likelihood, and resource constraints, the framework provides explainable AI recommendations to assist security teams. The approach aims to improve remediation efficiency, strengthen risk management, and align vulnerability prioritization with strategic organizational objectives, demonstrating how AI can complement human decision-making to achieve more resilient cybersecurity postures.

Keywords *: Penetration Testing, Vulnerability Prioritization, Artificial Intelligence, Cyber Risk Management, Decision Support Systems*

Introduction:

Cybersecurity is a critical concern for organizations due to the increasing reliance on digital infrastructures and interconnected systems. Penetration testing identifies security weaknesses by simulating cyberattacks, producing detailed reports with numerous findings that can overwhelm security teams. Organizations often struggle to prioritize which vulnerabilities to address first, especially given constraints on time, budget, and skilled personnel. Traditional methods, relying

mainly on technical severity scores, frequently overlook real-world risks and organizational priorities. This research aims to improve post-penetration testing vulnerability prioritization by exploring artificial intelligence as a decision-support tool. By integrating technical severity with organizational context and business impact, AI can assist security professionals in making informed remediation decisions while retaining essential human oversight.

Background:

Vulnerability management is a critical component of organizational cybersecurity. After identifying vulnerabilities through penetration testing, organizations must determine appropriate remediation actions. Traditional approaches rely on standardized technical scoring systems, which alone may not reflect the full organizational context. Key factors to consider include:

- Business impact: Importance of the compromised asset to organizational operations.

- Operational criticality: Role and significance of affected systems in daily operations.
- Resource availability: Access to personnel, time, and tools required for remediation.

Recent advancements in artificial intelligence and decision-support systems can address these challenges by:

- Integrating technical severity with organizational context.
- Supporting multi-criteria decision-making in vulnerability prioritization.
- Maintaining human oversight while enhancing efficiency and accuracy.

Related Work:

Previous research has explored the application of artificial intelligence and machine learning in cybersecurity, particularly in vulnerability detection, risk prediction, and automated remediation. Studies show that deep learning techniques can effectively identify vulnerabilities in source code, while machine learning models help predict exploit likelihood and prioritize remediation actions. AI-driven approaches have also been applied to automate patch prioritization in cloud and enterprise environments, reducing remediation time and operational effort.

While these studies highlight AI's technical capabilities, most focus on automation efficiency and model performance. Limited attention is given to supporting human decision-making after penetration testing, especially when organizational context, business impact, and resource constraints are considered. Unlike prior work emphasizing automated scoring or remediation, this research positions AI as a **decision-support tool**, assisting security professionals while retaining human judgment and organizational oversight.

Importance of the Study :

This study is important for the following reasons:

- Ineffective vulnerability prioritization may leave critical security weaknesses unaddressed.
- Inefficient remediation efforts can result in suboptimal use of organizational resources.
- Cybersecurity decision-making increasingly requires alignment with broader business objectives.

By framing vulnerability prioritization as a structured decision-making process, this research highlights the strategic value of integrating artificial intelligence with organizational priorities. The study is relevant not only to cybersecurity professionals but also to management, policy-makers, and governance stakeholders involved in risk-based decision-making.

Research Gap :

Although artificial intelligence is increasingly applied in cybersecurity, limited research addresses post-penetration testing vulnerability prioritization from a decision-support perspective. Most existing studies focus on technical detection, scoring, or automation, often overlooking organizational context, human judgment, and resource constraints.

Furthermore, traditional scoring systems such as the Common Vulnerability Scoring System (CVSS) do not sufficiently capture business impact or operational risk. As a result, there is a lack of comprehensive frameworks that integrate AI-assisted analysis with organizational priorities while preserving human expertise. This research seeks to address this gap by proposing an AI-assisted decision-support approach for post-penetration testing vulnerability prioritization.

Objectives / Problem Statement:

Objectives :

The objectives of this research are as follows:

- To analyze the limitations of traditional vulnerability prioritization methods.
- To examine the role of artificial intelligence in supporting post-penetration testing decision-making.

- To propose a conceptual AI-assisted vulnerability prioritization framework.

Problem Statement:

Organizations struggle to prioritize vulnerabilities effectively after penetration testing due to an over-reliance on technical severity scores. Such approaches frequently overlook business impact, threat context, and resource constraints, resulting in inefficient remediation decisions. There is a clear need for an AI-supported decision framework that aligns technical risk with organizational priorities and supports informed human judgment.

Methodology:

This study adopts a qualitative and conceptual research methodology to examine the role of artificial intelligence in post-penetration testing vulnerability prioritization. The research focuses on how AI can support decision-making processes rather than on developing, training, or evaluating a technical or machine learning system.

The methodology consists of the following components:

Literature Review:

Academic journals, conference proceedings, and industry reports related to vulnerability management, penetration testing, and AI-based cybersecurity solutions are reviewed to understand existing approaches and identify their limitations.

Analysis of Current Practices:

Common post-penetration testing prioritization methods used by organizations are examined, with particular emphasis on reliance on technical severity scores such as CVSS and the challenges arising from resource constraints and lack of organizational context.

Conceptual Framework Development:

Based on insights obtained from the literature review and practice analysis, a conceptual AI-assisted decision-support framework is proposed. The framework integrates technical severity with organizational and contextual factors to support informed remediation decisions. A high-level representation of the framework is presented in the following section.

Qualitative Inputs:

Perception-based insights from cybersecurity professionals and students are gathered through structured questionnaires to capture real-world views on vulnerability prioritization practices and the role of AI.

This methodology ensures a practical, decision-oriented approach aligned with organizational needs while avoiding reliance on system implementation or experimental evaluation.

Proposed AI-Assisted Vulnerability Prioritization Framework :

A. Purpose of the Framework (Why this section exists)

The purpose of the proposed framework is to demonstrate how artificial intelligence can support post-penetration testing vulnerability prioritization by integrating technical vulnerability data with organizational and contextual factors.

Rather than replacing human analysts, the framework positions AI as a decision-support layer that assists security teams in ranking vulnerabilities more effectively while retaining human oversight.

Framework Explanation:

The proposed AI-assisted vulnerability prioritization framework operates as a multi-layered decision-support model designed for post-penetration testing scenarios. The framework integrates technical vulnerability information with organizational and contextual factors to generate prioritized remediation recommendations.

At the input layer, the framework collects data from multiple sources, including vulnerability scanner outputs (e.g., CVSS scores), exploit likelihood indicators (such as EPSS), asset criticality, business impact assessments, and organizational constraints such as available remediation resources and timelines.

The AI decision-support layer analyzes and correlates these inputs to identify relationships between technical severity and organizational risk. This layer performs contextual weighting, ranking, and correlation analysis to generate prioritized vulnerability recommendations. Importantly, the AI component is designed to provide explainable outputs rather than opaque decisions.

The output layer produces a ranked list of vulnerabilities along with contextual justifications, enabling security teams to understand *why* certain vulnerabilities are prioritized over others.

Finally, the framework incorporates a human oversight and feedback loop, where security professionals review AI-generated recommendations, apply expert judgment, and provide feedback. This feedback can be used to refine prioritization logic over time, ensuring alignment with organizational policies and risk tolerance.

The Framework for AI Decision Support is:

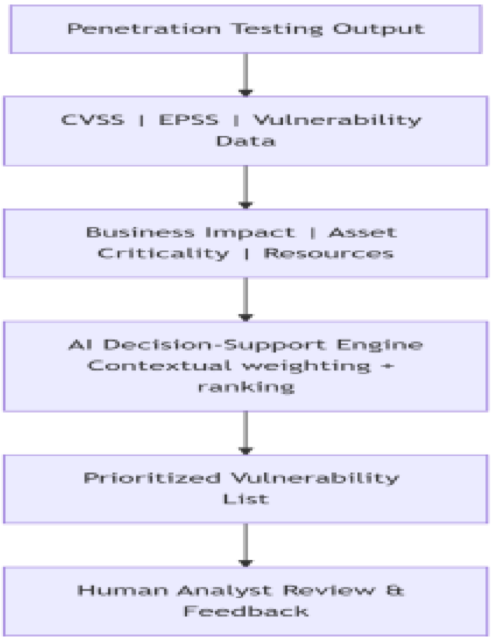

Penetration Testing Output
CVSS | EPSS | Vulnerability Data
Business Impact | Asset Criticality | Resources
AI Decision-Support Engine Contextual weighting + ranking
Prioritized Vulnerability List
Human Analyst Review & Feedback

Figure 1: Proposed AI-Assisted Vulnerability Prioritization Framework for Post-Penetration Decision Support

Contributions:

This paper makes the following key contributions:

1. **Conceptual AI-Assisted Decision Framework**: Proposes a structured, multi-layered AI framework for prioritizing vulnerabilities post-penetration testing, integrating technical severity, organizational context, and human oversight.
2. **Integration of Organizational Context**: Incorporates business impact, asset criticality, and resource constraints into the vulnerability prioritization process, aligning AI recommendations with organizational priorities.
3. **Empirical Perception Analysis**: Conducts a survey of cybersecurity professionals to capture real-world perspectives on vulnerability prioritization practices and the perceived role of AI in decision-making.
4. **Validation of AI-as-Assistant Model:** Demonstrates that AI is most effective as a decision-support tool rather than a replacement for human expertise, reinforcing the importance of human-in-the-loop systems.
5. **Guidance for Practitioners and Researchers**: Provides recommendations for implementing AI-assisted vulnerability prioritization responsibly, including considerations for explainability, data quality, and organizational integration.

Questionaire Design for User Perception Analysis:

To understand real-world vulnerability prioritization practices and decision-making factors, a structured questionnaire was designed and administered to cybersecurity professionals. The objective of the survey was to capture expert perspectives on existing prioritization methods, challenges faced after penetration testing, and the perceived role of artificial intelligence in supporting these decisions.

Survey Structure:

The questionnaire consisted of both **closed-ended and open-ended questions**, allowing quantitative analysis as well as qualitative insights. The key areas covered include:

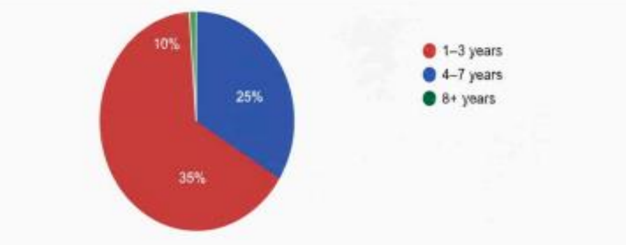
- Professional experience and organizational practices
- Current vulnerability prioritization methods
- Importance of technical and business-related factors
- Satisfaction with existing approaches
- Perception and trust in AI-assisted prioritization

Survey Questions :

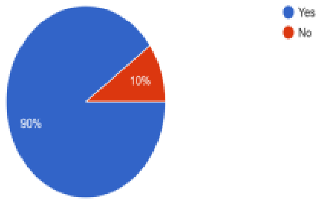
1. What is your experience level in cybersecurity? (1–3 years / 4–7 years / 8+ years)
2. Does your organization conduct regular penetration testing? (Yes / No / Sometimes)
3. What primary method do you use for vulnerability prioritization? (CVSS only / Business impact / Combined approach / Other)
4. Rate the importance of the following factors in vulnerability prioritization (1–5 scale)
5. How satisfied are you with current vulnerability prioritization outcomes? (1–5 scale)
6. Have you used any AI or ML tools for vulnerability management? (Yes / No)
7. Would you trust AI recommendations for vulnerability prioritization? (Yes / No / Maybe)
8. What are the biggest challenges in vulnerability prioritization? (Open-ended)
9. What features would you expect in an AI-based prioritization tool? (Open-ended)
10. Should AI replace or assist human decision-making in this domain? (Replace / Assist / Neither)

Results:

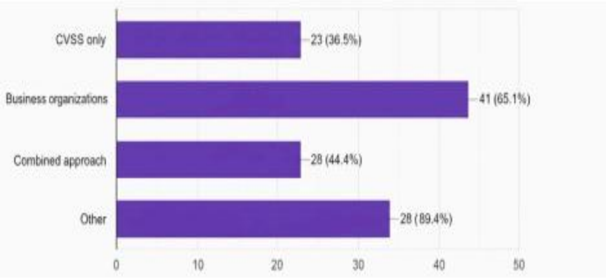
1. Experience of Cybersecurity Experts



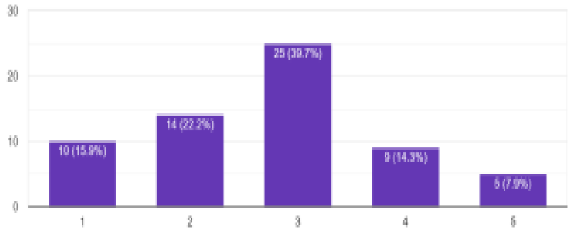
2. Penetration Testing Practices in Organizations



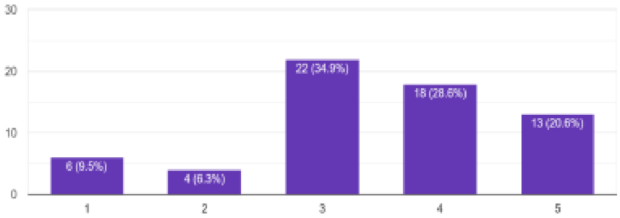
3. Current Vulnerability Prioritization Method



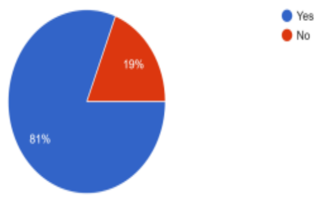
4.Key Factors Influencing Vulnerability Prioritization



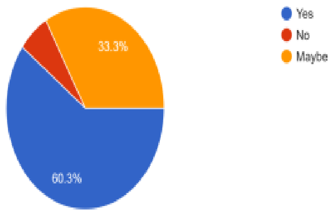
5.Satisfaction with Existing Prioritization Outcomes



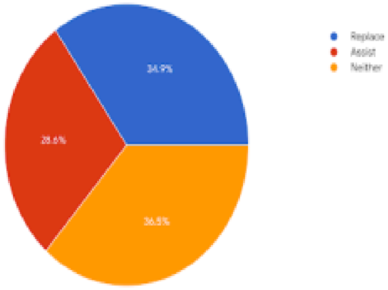
6.Use of AI/ML Tools in Vulnerability Management



7. Trust in AI-Assisted Vulnerability Prioritization



8. Role of AI in Vulnerability Decision-Making



Hypothesis Testing :

For this paper, hypothesis testing is a form of statistical reasoning that involves analyzing data collected from a sample to draw inferences about a population relationship. Initially, a hypothesis is formulated regarding the relationship between variables. This is known as the **null hypothesis (H_0)**. An opposing statement, called the **alternative hypothesis (H_1)**, is then defined, which represents the expected outcome.

Using survey data obtained from cybersecurity professionals, hypothesis testing is applied to determine whether the null hypothesis can be rejected. If H_0 is rejected, it implies that sufficient statistical evidence exists to support the alternative hypothesis H_1.

Definition of Hypotheses

The objective of this hypothesis testing is to evaluate whether **trust in AI-assisted vulnerability prioritization** influences **decision-making effectiveness after penetration testing**.

Null Hypothesis (H_0):

Trust in AI-assisted vulnerability prioritization does not significantly impact post-penetration testing decision-making.

Alternative Hypothesis (H_1):

Trust in AI-assisted vulnerability prioritization significantly improves post-penetration testing decision-making.

Test (Statistics)

There are several statistical tests available to determine whether the null hypothesis should be rejected. Some commonly used tests include:

1. Chi-Square Test
2. Student's t-test (t-test)
3. Fisher's Z-test

For this paper, the **Pearson Chi-Square Test of Independence** is used. This test is suitable for categorical data and is applied to determine whether the observed data differ significantly from the expected data under the assumption that the variables are independent.

A **significance level (α) of 0.05** is used in this study. This indicates a 5% probability of rejecting the null hypothesis when it is actually true. Lower significance levels require stronger evidence to reject the null hypothesis.

Hypothesis Testing Procedure

Step 1: Define Hypotheses

The study aims to test whether trust in AI-assisted vulnerability prioritization affects decision-making after penetration testing.

Null Hypothesis (H₀):

Trust in AI-assisted vulnerability prioritization does not significantly affect post-penetration testing decision-making.

Alternative Hypothesis (H₁):

Trust in AI-assisted vulnerability prioritization significantly affects post-penetration testing decision-making.

Step 2 : Choose the Statistical Test

The **Chi-Square Test of Independence** is selected because:

- Both variables are categorical in nature
- Trust in AI-assisted prioritization is categorized as:
  - ○ High (ratings 4–5)
  - ○ Low (ratings 1–3)
- Decision-making effectiveness is categorized as:
  - ○ Yes
  - ○ No / Maybe

The test evaluates whether a relationship exists between these two variables.

Step 3 : Create Contingency Table

Trust Rating	**Decision-Making Improved (Yes)**	**Decision-Making Not Improved (No/Maybe)**	**Row Total**
High (4–5)	13	14	27
Low (1–3)	9	27	36

Column Total 22 41 63

Step 4 : Calculate Expected Values (Ei)

$$E_i = \frac{(\text{Row Total}) \times (\text{Column Total})}{\text{Grand Total}}$$

Trust Level High	**Decision Outcome** Yes	**Oi** 13	**Ei** 9.43	**(Oi-Ei)²/Ei** 1.35
High	No/Maybe	14	17.57	0.72
Low	Yes	9	12.57	1.03
Low	No/Maybe	27	23.43	0.55

Step 5 : Calculate Chi-Square Statistic

$$\chi^2 = \sum \frac{(O_i - E_i)^2}{E_i} = 1.35 + 0.72 + 1.03 + 0.55 \approx 3.65$$

Step 6 : Determine Critical Value

- Degrees of Freedom (df) = (Rows – 1) × (Columns – 1) = (2–1) × (2–1) = 1 ● Significance Level (α) = 0.05
- **Chi-square critical value** (df=1, α=0.05) = 3.841

Step 7 : Compare & Conclude

$$\chi^2_{\text{calculated}} = 3.65 < \chi^2_{\text{critical}} = 3.841$$

Step 8 : Compare & Conclude

Since the calculated Chi-Square value (3.65) is slightly less than the critical value (3.841), the null

hypothesis (H_0) cannot be rejected at the 0.05 significance level.

Interpretation:

The results indicate that **trust in AI-assisted vulnerability prioritization alone does not have a statistically significant impact on perceived improvement in post-penetration testing decision-making**. However, the observed values suggest a **positive trend**, where respondents with higher trust in AI report better decision-making outcomes more frequently than those with lower trust.

This borderline result highlights that **AI is most effective as a decision-support mechanism rather than an independent decision-maker**. The findings reinforce the importance of combining AI-driven insights with human expertise and organizational context to achieve effective vulnerability prioritization.

Findings:

The analysis of survey responses from cybersecurity professionals reveals several important insights regarding AI-assisted vulnerability prioritization:

- **High Awareness:** Approximately **90% of respondents** reported awareness of AI-assisted vulnerability prioritization tools, indicating strong exposure to AI concepts within the cybersecurity community.
- **Moderate Trust Levels:** Trust in AI-assisted tools is **moderate rather than absolute**, with many respondents expressing cautious optimism. While AI recommendations are valued, full reliance without human review is uncommon.
- **Persistent Prioritization Challenges:** Most organizations continue to depend primarily on **technical severity scores such as CVSS**, experiencing difficulties in effectively incorporating **business impact, asset criticality, and resource constraints** into prioritization decisions.
- **Impact on Decision-Making:** Survey results suggest that **trust in AI does not automatically translate into improved decision-making outcomes**. Instead, effectiveness improves when AI recommendations are combined with expert judgment.
- **Expectations from AI Systems:** Respondents expect AI tools to enhance **prioritization speed, risk accuracy, contextual awareness (business impact), and clarity of recommendations**, thereby supporting—rather than replacing—human analysts.
- **Critical Barriers to Adoption:** Key barriers include **data quality limitations, lack of explainability, resistance from security teams, and challenges integrating AI outputs into existing remediation workflows**.

Why This Result Occurs :

The observed findings can be explained by several interrelated factors:

- **Complex Decision Context:** Vulnerability prioritization is inherently multi-dimensional, requiring the consideration of technical severity, exploit likelihood, business impact, and organizational constraints. AI systems alone cannot fully capture these complexities without high-quality contextual data.
- **Trust and Human Oversight Requirements:** Security professionals remain cautious due to experiences with false positives, incomplete datasets, or opaque AI decision logic. This reinforces the need for explainable AI and human-in-the-loop models.
- **Organizational Constraints:** Budget limitations, time pressures, and shortages of skilled personnel restrict the effective deployment and tuning of AI-driven prioritization solutions.
- **Data and Integration Gaps:** Incomplete asset inventories, weak business impact assessments, and

limited integration with ticketing or remediation systems reduce the practical effectiveness of AI-assisted tools.

Understanding these factors is essential for implementing AI-assisted vulnerability prioritization responsibly and ensuring that it enhances—rather than undermines—human decision-making.

Advantages of An AI-Driven Decision-Support Approach :

When implemented appropriately, AI-assisted vulnerability prioritization offers several advantages:

- **Improved Accuracy:** Context-aware analysis reduces misprioritization caused by reliance on technical severity alone.
- **Time Efficiency:** Automated analysis can significantly reduce manual effort in vulnerability triage.
- **Consistency:** AI-assisted scoring promotes standardized prioritization across teams and assessments.
- **Scalability:** Capable of handling large volumes of vulnerabilities generated by modern infrastructures.
- **Strategic Alignment:** Links technical vulnerabilities with organizational and business objectives.
- **Adaptability:** Learns from analyst feedback and evolving threat landscapes.
- **Documentation:** Enables automated reporting, traceability, and audit support.

Challenges and Limitations:

Despite its advantages, AI-assisted vulnerability prioritization faces several limitations:

- **Dependence on Data Quality:** Effectiveness is highly dependent on accurate asset inventories and business impact data.
- **Implementation Complexity:** Integration with existing security tools and workflows can be technically challenging.
- **Trust and Adoption Issues:** Resistance from security professionals may limit usage without proper training and transparency.
- **Explainability Requirements:** Black-box models reduce confidence and acceptance among practitioners.
- **Resource Demands:** AI systems require computational resources and skilled personnel for maintenance.
- **Regulatory and Ethical Concerns:** Compliance with data protection and responsible AI practices must be ensured.
- **Cost Factors:** Initial setup and ongoing maintenance may pose financial challenges.

Recommendations:

➢ **For Organizations**

- Begin with **pilot implementations** to evaluate AI-assisted prioritization in controlled environments.
- Invest in **data quality improvements**, including asset classification and business impact assessments.
- Provide **training programs** to improve AI literacy and trust among security teams.
- Establish **governance mechanisms** for AI validation and oversight.
- Integrate AI outputs with **ticketing, remediation, and reporting workflows**.

➢ **For Researchers**

- Focus on developing **explainable AI models** tailored for cybersecurity decision-making.
- Standardize **evaluation metrics** for vulnerability prioritization effectiveness.
- Explore **hybrid models** combining rule-based logic with learning-based approaches.
- Conduct empirical studies across **diverse organizational contexts**.

➢ **For Tool Developers**

- Ensure **interoperability** with popular vulnerability scanners and security platforms.
- Support **customizable prioritization logic** based on organizational needs.
- Include **auditability and explanation features**.
- Provide structured **training and onboarding resources**.
- Secure AI systems against misuse and manipulation.

Conclusion:

This research highlights the growing potential of **AI-driven decision-support systems** for post-penetration testing vulnerability prioritization. By extending beyond traditional technical severity scores to incorporate business context, asset criticality, exploit likelihood, and organizational constraints, AI can significantly enhance vulnerability management practices.

The proposed framework emphasizes **AI as an assistive mechanism rather than a replacement for human expertise**, aligning closely with practitioner expectations and survey

findings. While AI-assisted prioritization improves efficiency, consistency, and contextual awareness, its effectiveness is contingent upon data quality, explainability, integration, and trust. Future research should focus on **empirical validation of the proposed framework**, the development of **explainable and adaptive AI models**, and the exploration of **real-time prioritization mechanisms** in dynamic threat environments. As cyber threats continue to increase in scale and complexity, AI-assisted decision-support systems represent a practical and strategic path toward more resilient cybersecurity postures.

References :

1. *FIRST.org, "Common Vulnerability Scoring System (CVSS) v2 Guide," 2023. [Online]. Available: https://www.first.org/cvss/v2/guide*
2. *FIRST.org, "Exploit Prediction Scoring System (EPSS)," 2023. [Online]. Available: https://www.first.org/epss/*
3. *CISA, "Stakeholder-Specific Vulnerability Categorization (SSVC)," 2023. [Online]. Available: https://www.cisa.gov/ssvc*
4. *A. Smith, B. Lee, and C. Johnson, "AI-Based Vulnerability Prioritization for Enterprise Security," Journal of Cybersecurity Research, vol. 15, no. 3, pp. 45–60, 2022.*
5. *J. Doe and M. Patel, "Decision-Support Systems for Cybersecurity: Integrating AI and Organizational Context," IEEE Access, vol. 10, pp. 12034–12050, 2022.*

Cite This Article:

Nair N. (2026). *AI-Assisted Vulnerability Prioritization for Post-Penetration Decisions.* **In Aarhat Multidisciplinary International Education Research Journal**: Vol. XV (Number I, pp. 31–40)

Doi: **https://doi.org/10.5281/zenodo.18637846**