VOIS for Tech University Engagement Program

Innovation Marathon 2025-2026

Team No.-

Project Title –Centralized Vulnerability Detection and Intelligent Query Interf

Problem statement-

- Today, security teams use many separate tools to check for weaknesses in websites and servers. That makes it hard to see the full picture — results are scattered, confusing, and take time to understand.
- Teams need an easy way to run checks, collect the results in one place, and quickly understand how serious each problem is and which systems are affected.
- It is also hard for non-technical people (managers, decision makers) to understand raw scan outputs. Teams need clear reports and a simple way to ask questions about the findings in plain language.
- Finally, defenders want help understanding possible ways an attacker could use the found weaknesses together (a chain of problems leading to a major breach) so they can prioritize fixes

Proposed solution (in detail)-

- Build a single web application that lets users start security checks for websites and systems they own. The app will run automated checks and collect results in one place.
- The system will turn raw scan outputs into easy-to-read reports that show each problem, how serious it is, where it is, and suggested fixes. Reports will be short and clear so both engineers and managers can act fast.
- The app will create a simple visual map showing how different weaknesses could be combined by an attacker to move through the network — like a “roadmap” of possible attack steps (presented as a high-level diagram, not a how-to guide).

- A chat-style assistant will let users ask questions in normal language (for example: “Which servers need urgent fixes?” or “How do we fix the high-risk issues?”). The assistant will answer using the collected scan results and trusted reference sources, and it will refuse to provide any instructions that would help someone attack a system.
- The system will include safety rules: it will only be used on systems the team owns or has permission to test, it will log all actions, and the assistant will focus on remediation and explanation rather than exploit steps.

Technology to be used –

- **Web Interface (Frontend):**
    - This is the main dashboard that users see when they open the system in their web browser.
    - It allows users to enter a website or system address, start scans, and track progress in real time.
    - The interface displays scan results in a simple, colorful, and organized way — showing which issues are critical, which are minor, and where they are located.
    - It also includes search and filtering options so users can quickly find information they need.
    - The design is fully responsive, meaning it works smoothly on desktops, laptops, and tablets.

- **Automated Scanning Tools (Backend):**
    - These are security analysis tools that automatically check for weaknesses in authorized websites or systems.
    - The system integrates multiple popular scanners — such as **Nmap** (for network discovery), **Nuclei** (for vulnerability testing), **OpenVAS** or **Nessus** (for in-depth vulnerability analysis).
    - Each scanner runs independently and reports its findings back to the main system.

- The platform collects and organizes all these results into a single, unified format so users don't need to open multiple reports.
- This automation reduces manual work and ensures that every scan is consistent and accurate.

- **Database & Storage:**
  - All scan results, reports, and system details are stored safely in a central database.
  - The database organizes information into structured records — such as target name, detected vulnerabilities, risk levels, and timestamps.
  - This allows quick searching, filtering, and exporting of reports when needed.
  - In addition, raw scan files and large reports are stored in secure cloud-based storage (or a local file server) so that data remains backed up and protected.
  - Access to stored data is restricted only to authorized users, ensuring privacy and security.

- **AI Assistant (Query Interface):**
  - The platform includes an intelligent assistant that users can chat with in normal, everyday language.
  - Instead of reading through lengthy reports, users can simply ask questions like "Which systems are at high risk?" or "How do I fix the top vulnerability?"
  - The assistant looks up the answers from the stored reports and verified cybersecurity databases (like CVE, NVD, and ExploitDB).
  - It then explains the issue, its severity, and safe ways to fix it — in simple terms.
  - The assistant also helps prioritize what should be fixed first based on risk level and impact.
  - It strictly avoids giving harmful or exploit-based instructions and focuses only on safety and prevention.

- **Visualization Module (Attack Path Map):**
    - This feature creates an easy-to-understand diagram or “map” that shows how different vulnerabilities might be connected.
    - For example, it can show how an attacker might move from one weak point in the network to another.
    - The map helps users see which vulnerabilities are isolated and which could lead to a larger breach if combined.
    - Each node or line on the map represents a system, service, or connection, giving a visual overview of the network’s security posture.
    - This helps in making better decisions and prioritizing patches more effectively.

- **Security & Safety Layer:**
    - The system follows strict security and ethical rules.
    - Scans can only be performed on authorized systems that the user owns or has permission to test.
    - Every scan, user action, and result is logged automatically for accountability and auditing.
    - User accounts have roles and permissions — for example, some users can start scans, while others can only view reports.
    - Data is encrypted during storage and transmission to prevent leaks or tampering.
    - The assistant is programmed to refuse unsafe queries and focus on responsible cybersecurity practices only.
    - Together, these controls ensure that the system remains secure, legal, and trustworthy.