Cyber Diagnostics Lab: A Digital Health Checkup

GROUP 09

PG-DCSF | Centre for Development of Advanced Computing (C-DAC), Thiruvanathapuram | August 2025

Project Team

Expert Guidance & Development

Under the Guidance of:

- Mr. Jayaram – Centre Coordinator
- Dr. Priya P. Sajan – Project Guide

Development Team: Dhananjay Shivarkar, Shubham Joshi, Khilesh Mahajan, Rasika Mahajan, Sagar Chaudhari, Uday Sambare

Project Overview

Web-Based Platform

Automated cybersecurity diagnostic system performing comprehensive security health checks of web applications and infrastructure

Intelligent Scanning

Domain and IP address vulnerability assessment with real-time progress tracking and detailed reporting capabilities

Admin Control

Comprehensive admin panel for user monitoring, activity tracking, and centralized security management

Centralized Security Assessment

Enables centralized security assessment by integrating scanning, reporting, and monitoring within a single platform.

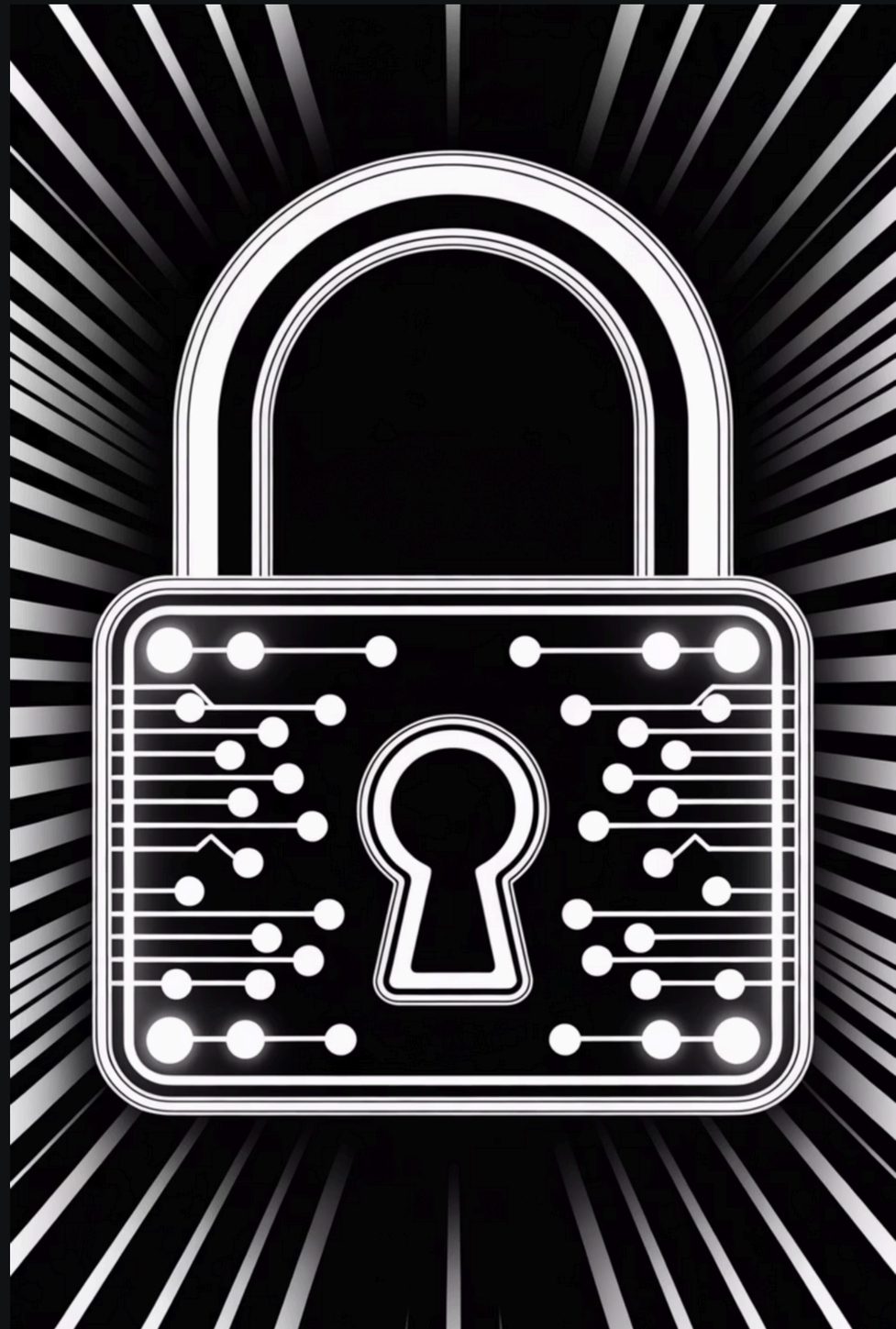
The Cybersecurity Challenge

Modern web application handle critical and sensitive data.

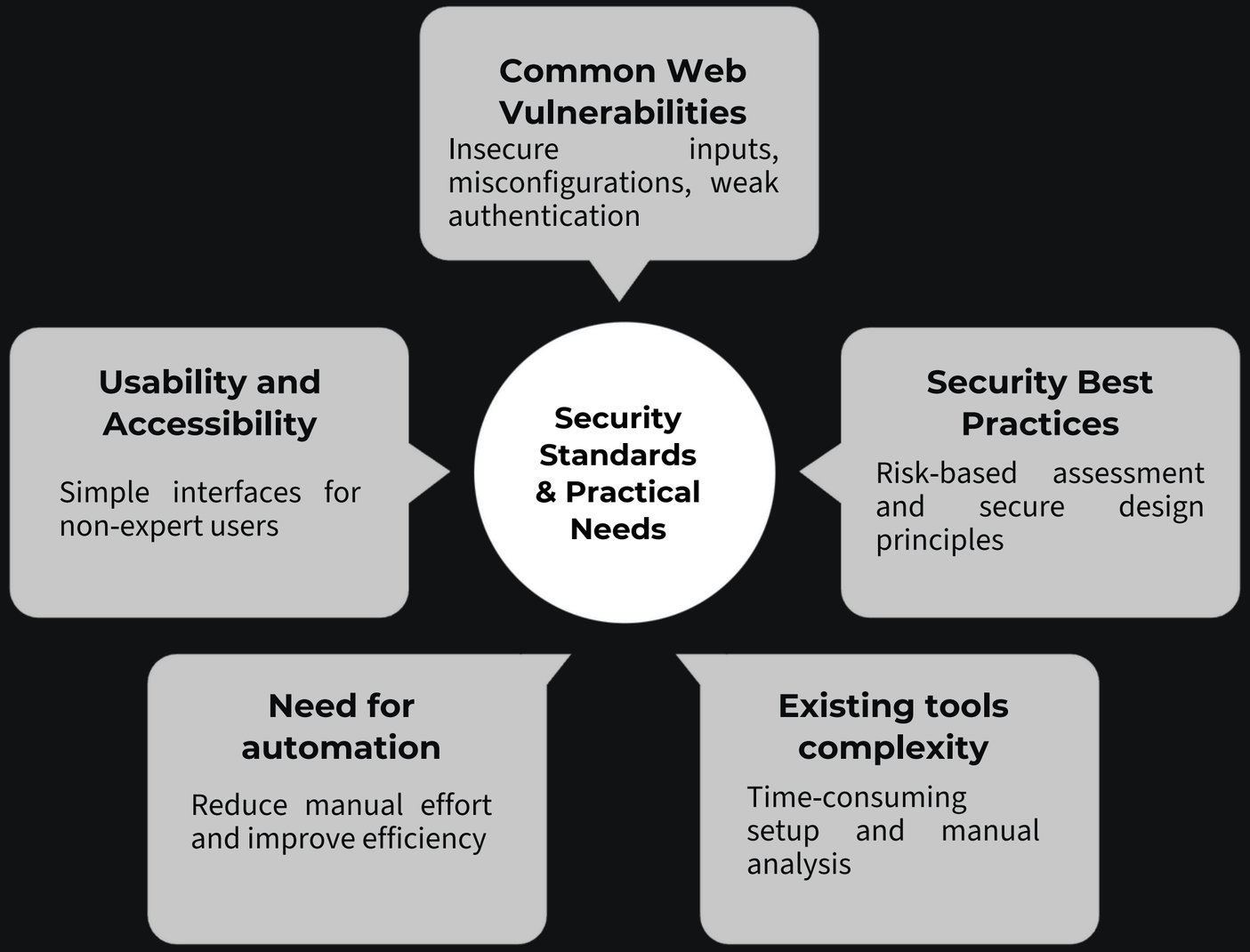
Cyber threats are increasing due to insecure coding and misconfigurations.

Many organizations lack continuous security assessment mechanisms. Manual security testing is time-consuming and expertise-dependent.

Our Solution: Cyber Diagnostics Lab provides an automated, structured and role-based security assessment solution for web applications



Project Foundation



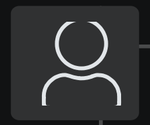
Literature Survey Insights

Focused on existing cybersecurity standards, commonly observed web application risks, and the practical limitations of current security assessment tools.

Industry guidelines emphasize regular vulnerability assessment; however, existing tools often involve complex configurations and time-consuming manual processes. This makes them difficult to use in academic environments and small organizations.

The key insight from the survey is the need for an **automated, centralized, and user-friendly security assessment system** that simplifies scanning, reporting, and monitoring. These insights directly influenced the design of the Cyber Diagnostics Lab.

System Architecture & Workflow



Secure Access & Role Management

Role-based authentication system separating user and admin privileges, ensuring secure sessions and controlled access to system features.

Scan Submission & Request Handling

Users submit domain or IP addresses through a validated interface; requests are managed and forwarded to the centralized scanning engine.

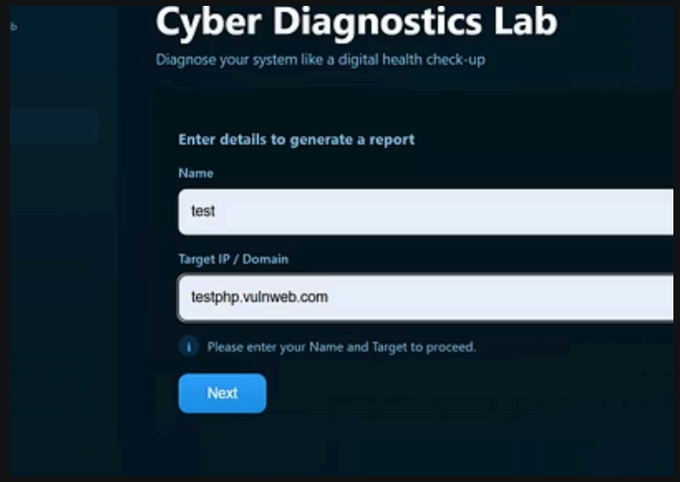
Automated Security Analysis

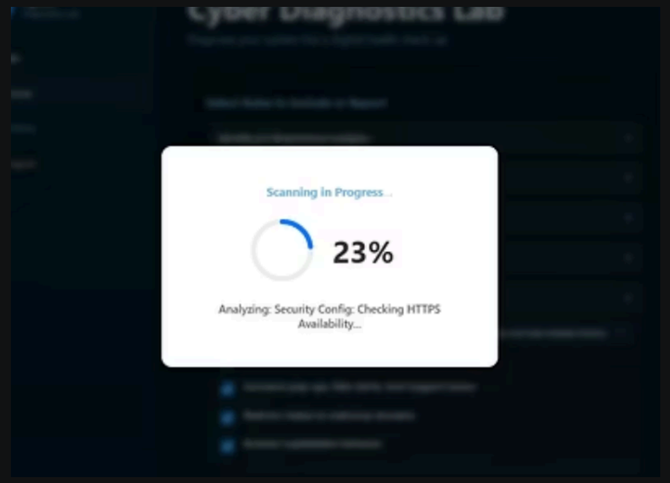
Backend security modules perform infrastructure, configuration, threat intelligence, web application, and behavioral analysis with live progress tracking.

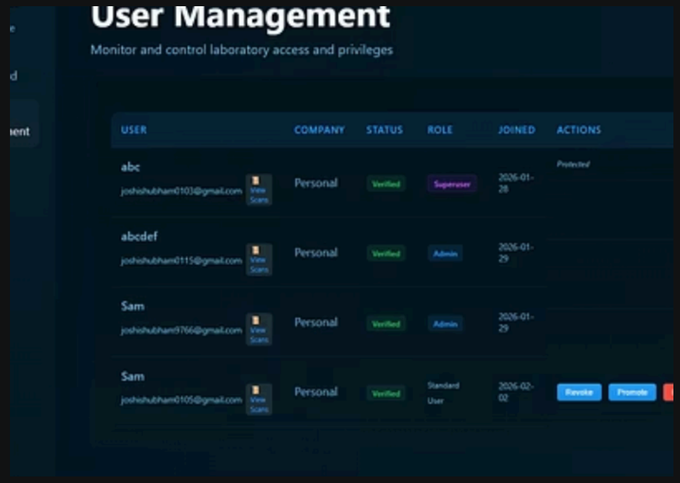
Reporting, Scanning & Administration

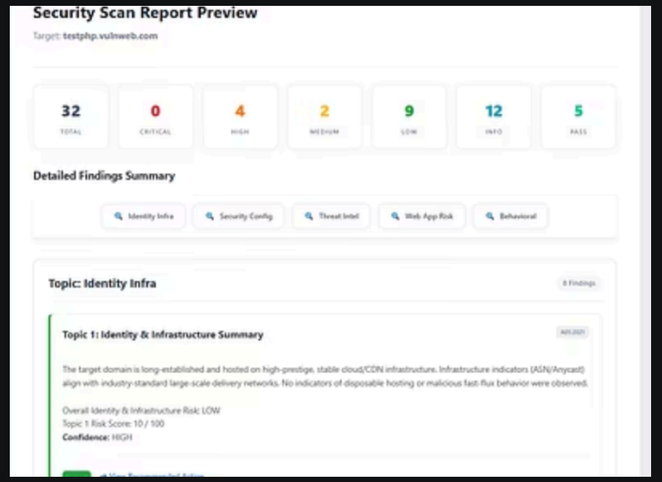
Scan results are processed, stored in the database, and presented as detailed reports; the admin panel enables user management, monitoring, and audit control.

Web Application Walkthrough









Security Analysis Framework

01

Infrastructure & Asset Identification

Comprehensive discovery of digital assets, network topology, and exposed services

02

Security Configuration Analysis

Deep inspection of server configurations, SSL/TLS settings, and security headers

03

Threat Intelligence & Abuse Checks

Cross-reference against known threat databases and blacklists for malicious activity indicators

04

Web Application Risk Analysis

Automated testing for injection flaws, authentication weaknesses, and data exposure vulnerabilities

05

Behavioral Risk Analysis

Pattern recognition for suspicious activities and anomalous application behavior

Risk Classification

Findings categorized into seven severity levels for prioritized remediation:

- Critical – Immediate action required
- High – Urgent remediation needed
- Medium – Schedule for resolution
- Low – Address when possible
- Informational – Awareness notices
- Passed – Security controls validated

Each finding includes detailed technical descriptions and actionable remediation guidance.

Future Roadmap & Conclusion

Full OWASP Coverage

Complete automation of OWASP Top 10 vulnerability detection with advanced testing modules

AI-Powered Detection

Machine learning algorithms for intelligent anomaly detection and predictive threat analysis

Compliance Reporting

Automated PDF generation and regulatory compliance report formatting for audit requirements

Cloud & API Security

Extended assessment capabilities for cloud infrastructure and API endpoint vulnerability testing

---

> **Project Achievement:** Successfully developed an automated cybersecurity diagnostic platform that demonstrates real-world security practices while providing accessible vulnerability assessment capabilities for academic and practical applications.

References: OWASP Foundation-Web Application Security Guidelines | Flask Official Documentation | SQLAlchemy ORM Documentation | NIST Cybersecurity Framework (NIST CSF) | Python Security Best Practices (OWASP & Python Docs)

Thankyou...