

A large, stylized white shield icon is positioned on the left side of the slide. The shield contains a central padlock icon surrounded by a hexagonal border. To the left of the shield is a vertical stack of blue horizontal bars, resembling a bar chart or a digital interface. The background of the slide features a dark blue gradient with faint, glowing blue circuit board patterns and a grid.

# Cyber Diagnostics Lab: A Digital Health Checkup

GROUP 09

PG-DCSF | Centre for Development of Advanced Computing (C-DAC), Thiruvananthapuram | 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 applications 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



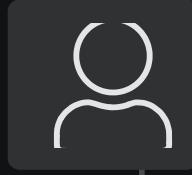
# Literature Survey Insights

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

The image displays a series of screenshots from a web-based security diagnostic application named "Cyber Diagnostics Lab".

**1. Login Screen:** Shows a dark-themed login form with fields for Email Address (containing a placeholder email) and Password, and a blue "Login" button.

**2. Report Generation Screen:** A form titled "Enter details to generate a report" with fields for Name (containing "test") and Target IP / Domain (containing "testphp.vulnweb.com"). It includes a note: "Please enter your Name and Target to proceed." and a "Next" button.

**3. Configuration Screen:** A sidebar titled "Select Rules to Include in Report" listing categories: Identity & Infrastructure Analysis, Security Configuration Analysis, Threat Intelligence & Abuse Checks, Web Application Risk Analysis, and Behavioral Analysis. Under Behavioral Analysis, there is a note: "Note: Covers OWASP Top 10 - A04:2021-Insecure Design, A06:2021-Software and Data Integrity Failures". A list of checked items includes: Auto-download triggers (drive-by downloads), Excessive pop-ups, fake alerts, tech support scams, Redirect chains to malicious domains, and Browser exploitation behavior.

**4. User Management Screen:** A table titled "User Management" showing user details: abc (Personal, Verified, Supervisor, Joined 2026-01-26), abcd (Personal, Verified, Admin, Joined 2026-01-29), Sam (Personal, Verified, Admin, Joined 2026-01-29), and another entry for Sam (Standard User, Joined 2026-02-02). Actions columns include "Revoke" and "Promote".

**5. Security Scan Report Preview:** A summary for target "testphp.vulnweb.com" showing a total of 32 findings: 0 Critical, 4 High, 2 Medium, 9 Low, 12 Info, and 5 Pass. It includes a "Detailed Findings Summary" with links for Identity Infra, Security Config, Threat Intel, Web App Risk, and Behavioral.

**6. Progress Overlay:** A white box with a circular progress bar indicating "Scanning in Progress..." at 23%, with the message "Analyzing: Security Config: Checking HTTPS Availability..." below it.

# 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

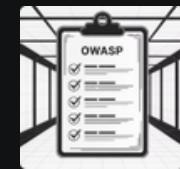
## Risk Classification

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

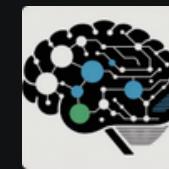
Each finding includes detailed technical descriptions and actionable remediation guidance.

# Future Roadmap & Conclusion



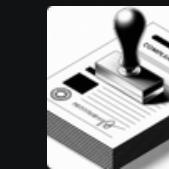
## Full OWASP Coverage

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



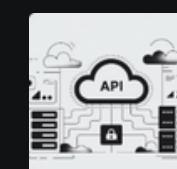
## AI-Powered Detection

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...