RIPHAH
INTERNATIONAL UNIVERSITY

Riphah International University

Semester Project

BSCY-2-1

Tayyab Pervez –24533

Information Security

Submitted To: Sir Yawar Abbas

November 02, 2025

Project Title

Web-Based Interface and Security Analysis Layer for RustScan

---

1. Introduction

With the rapid growth of network-based systems, understanding exposed network services is an essential part of information security. Port scanning is commonly used during the reconnaissance phase of security assessments to identify open and accessible services on a system. However, many existing tools are command-line based and difficult to use for beginners or non-technical users.

This project aims to design and develop a **web-based interface and analysis layer for RustScan**, an open-source, fast port scanning tool written in Rust. The proposed system will enhance usability, visualization, and security awareness while maintaining ethical and academic boundaries.

---

2. Problem Statement

Although **RustScan** is a powerful and efficient port scanning tool, it lacks a graphical or web-based interface and provides raw output that may be difficult to interpret. Users must manually analyze scan results to understand potential security risks. There is a need for a system that simplifies scan execution, presents results in a clear manner, and provides security-oriented insights.

---

3. Objectives

The main objectives of this project are:

- To develop a web-based interface using HTML and CSS for interacting with RustScan
- To create a Rust backend that securely executes RustScan commands
- To visualize port scanning results in a structured and user-friendly format
- To enhance scan results with basic security analysis and reporting features
- To ensure ethical usage through safety controls and rate limiting

---

4. Scope of the Project

This project focuses on **network exposure discovery and security awareness**. It does not perform exploitation, brute-force attacks, or unauthorized access. The tool is intended strictly for educational purposes and ethical security assessments in controlled environments.

---

5. Proposed System Architecture

The proposed system consists of three main components:

1. **Frontend Interface**
    - Developed using HTML and CSS
    - Allows users to input target information and select scan options
    - Displays scan results and reports
2. **Rust Backend Application**
    - Handles user requests from the frontend
    - Validates input and enforces safety rules
    - Executes RustScan using secure system calls
3. **RustScan Tool**
    - Performs fast port scanning
    - Outputs scan results to the backend for processing

---

6. Core Features

6.1 Web-Based User Interface

- Input fields for target IP address or domain name
- Option to select predefined scan profiles
- Button to initiate scanning process

6.2 Secure Rust Backend Integration

- Backend written in Rust
- Secure execution of RustScan commands
- Input validation to prevent command injection

6.3 Scan Result Visualization

- Display of open ports in tabular format
- Clear separation of port numbers and detected services

---

7. Selected Enhancements (Phase 2)

7.1 Risk-Based Port Classification

The tool will analyze detected open ports and classify them into risk categories such as low, medium, or high risk. This classification will be based on commonly known service exposure risks.

7.2 Exportable Security Report

The system will allow users to generate and export scan reports in structured formats such as:

- Text format
- JSON format

Reports will include:

- Target details
- Scan timestamp
- List of open ports
- Risk classification summary

7.3 Rate Limiting and Safe Mode

To ensure ethical and controlled usage, the tool will include:

- Scan rate limiting to prevent aggressive scanning
- Safe scan mode with predefined port ranges
- Restrictions on repeated scans within short intervals

This feature promotes responsible use of the tool in academic environments.

---

8. Tools and Technologies

- **Programming Language:** Rust
- **Frontend:** HTML, CSS
- **Backend Framework:** Rust-based HTTP server
- **Security Tool:** RustScan (Open Source)
- **Operating System:** Linux / Windows

9. Conclusion

This project combines practical cybersecurity concepts with modern system design using Rust and web technologies. By enhancing an existing open-source tool, the proposed system demonstrates real-world security assessment workflows while maintaining academic integrity. The project will strengthen understanding of network security, secure software design, and ethical security practices.