# Cyber Security

## Project Report


**SUBMITTED BY**

**HASSAN ALI**

**AHSAN NASEER**

**SYED ALEEM**

***Software Engineering 22 (Blue)***

**SUBMITTED TO**

**Mr. Luqman Shehzad**

**DEPARTMENT OF IT & COMPUTER SCIENCE**

**PAK-AUSTRIA FACHHOCHSCHULE INSTITUTE OF APPLIED SCIENCES AND TECHNOLOGY**

## 1. Introduction

**Repo Scanner-X** is an automated security scanning tool designed to analyze GitHub repositories for vulnerabilities, misconfigurations, and exposed secrets. It combines **Trivy** (a powerful vulnerability scanner) with **AI-powered analysis** (using Groq's LLaMA3-70B model) to provide actionable security recommendations.

**Key Features:**

- ✅**GitHub Repository Scanning** – Detects vulnerabilities in code and dependencies.
- ✅**AI-Powered Analysis** – Provides remediation steps and attack insights.
- ✅**User-Friendly Interface** – Built with Gradio for easy interaction.
- ✅**Report Generation** – Exports findings in text and markdown formats.

## Source Code Github Repo link:

**https://github.com/hassanali167/SecureDeploy**

---

## 2. Team Members & Contributions

| Team Member | Role | Key Responsibilities |
|---|---|---|
| **Hassan Ali** | **Backend & AI Integration** | Implemented Trivy scanning, GitHub API interactions, and AI recommendation system. |
| **Ahsan Naseer** | **UI/UX & Frontend** | Designed the Gradio interface, improved user experience, and implemented CSS styling. |
| **Syed Aleem** | **Testing & Documentation** | Conducted testing, wrote documentation, and ensured smooth deployment. |

---

## 3. Project Breakdown

### 3.1 Hassan Ali – Backend & AI Integration

**Tasks Completed:**

- **GitHub API Integration:**

- Implemented repository verification and metadata extraction.
- Handled OAuth token authentication for private repos.

- **Trivy Scanner Integration:**
  - Automated vulnerability scanning (`vuln, secret, config, license`).
  - Processed scan results for AI analysis.
- **AI-Powered Recommendations:**
  - Integrated **Groq's LLaMA3-70B** model for security insights.
  - Designed structured prompts for accurate AI responses.

**Challenges Faced:**

- **API Rate Limits:** Had to optimize GitHub API calls.
- **Trivy Output Parsing:** Implemented regex to extract vulnerable files.

---

**3.2 Ahsan Naseer – UI/UX & Frontend**

**Tasks Completed:**

- **Gradio Interface:**
  - Developed an interactive UI with input fields, buttons, and output displays.
  - Added **downloadable report** functionality.
- **Styling & Theming:**
  - Customized CSS for a professional look (`gr-themes.Soft()`).
  - Improved readability with **markdown formatting**.
- **User Experience:**
  - Added **status indicators** (✅/❌) for better feedback.
  - Ensured smooth navigation between scan results.

**Challenges Faced:**

- **Real-time Output Handling:** Managed dynamic text updates in Gradio.
- **Mobile Responsiveness:** Adjusted layout for different screen sizes.

---

### 3.3 Syed Aleem – Testing & Documentation

**Tasks Completed:**

- **Testing:**
    - Verified **Trivy scans** on multiple repositories.
    - Tested **AI responses** for accuracy.
    - Checked edge cases (invalid URLs, token failures).
- **Documentation:**
    - Wrote **user documentation** (installation, usage, customization).
    - Prepared **project report** (this document).
- **Deployment:**
    - Ensured smooth execution in different environments.

**Challenges Faced:**

- **AI Hallucinations:** Some AI responses needed manual validation.
- **Cross-Platform Issues:** Fixed dependency conflicts.

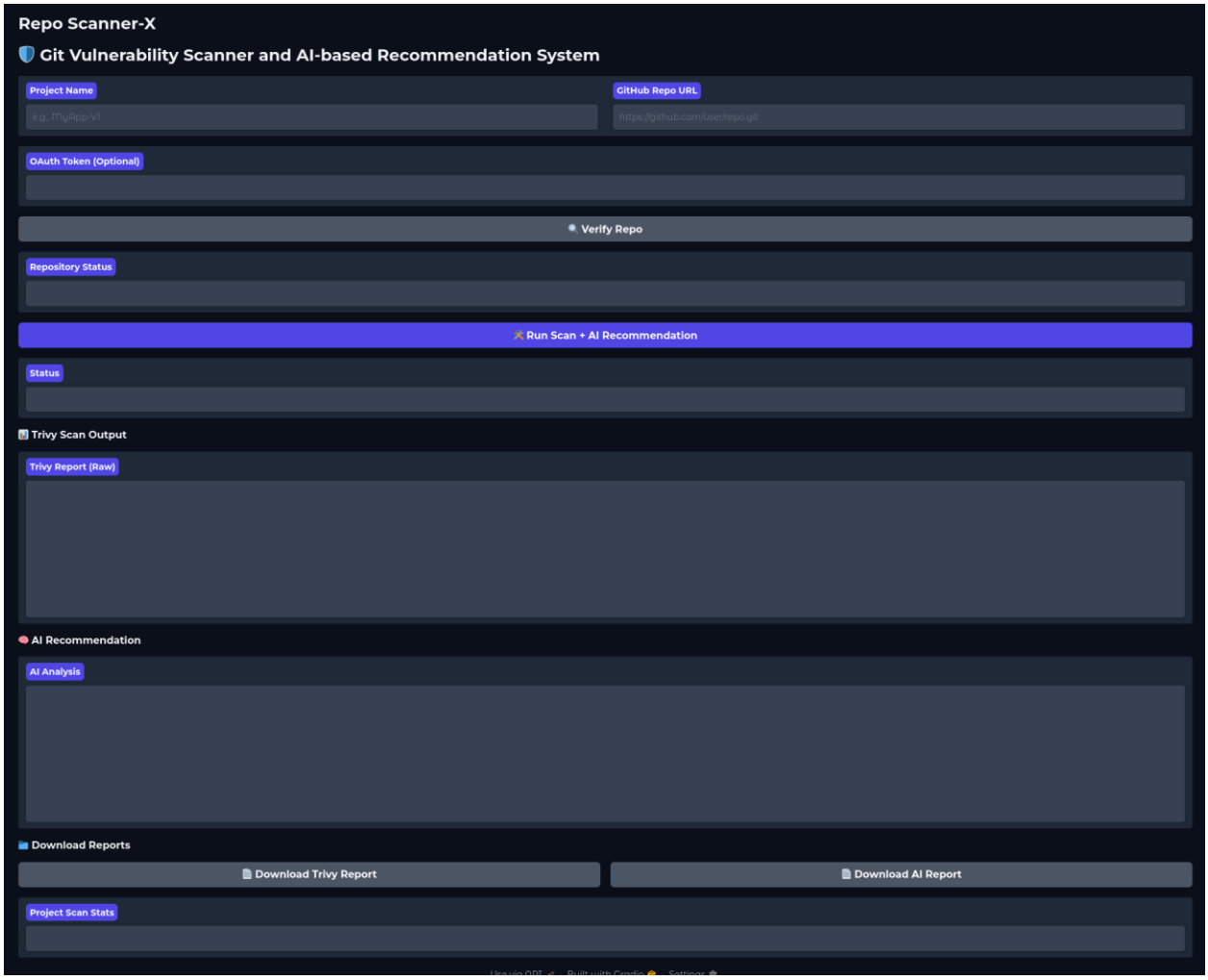
---

## 4. Results & Outcomes

- ✅**Successfully implemented** a working security scanner with AI recommendations.
- ✅**User-friendly interface** with clear vulnerability reports.
- ✅**Tested on multiple repositories** (public & private).

**Future Improvements:**

- Add **PDF report generation**.
- Support **more scanning tools** (Bandit, Semgrep).
- Implement **scheduled scans**.




## 5. Conclusion

Repo Scanner-X provides an **automated, AI-enhanced** approach to GitHub repository security scanning. The project was successfully completed with contributions from all team members, covering **backend, frontend, testing, and documentation**.

This tool helps developers **identify security risks early**, reducing potential vulnerabilities in production.