Malware Detection Web Application (Beluga) 🦾🛡️

Problem Statement 🔥

Malware is a growing concern, with **millions of individuals and organizations** suffering from security breaches every year due to downloading and executing malicious files. According to cybersecurity reports, over **560,000 new pieces of malware** are detected daily, leading to financial losses and privacy breaches. Traditional antivirus solutions struggle to keep up with evolving threats and are often difficult for non-technical users to operate.

The need for a **fast, accessible, and user-friendly malware detection tool** is more pressing than ever. Our solution aims to bridge this gap by offering a **web-based static malware analysis tool** that allows users to quickly upload a file and receive an immediate verdict on its safety.

Brief Solution ⚡

We propose a **web application** that performs **static analysis** on uploaded files (`.exe`, `.docx`, `.pdf`) to identify potential threats without executing the file. Our system will:

- Scan the file for suspicious patterns using **YARA rules** and **PE file analysis**.
- Provide a **clear and concise verdict** ("Malicious" or "Clean").
- Offer a **simple and intuitive user interface** for easy file uploads.
- Ensure **security and scalability**, allowing multiple concurrent users to scan files efficiently.

Additionally, we introduce:
✅ **File Hash Comparison** – Quickly identify known threats via SHA-256 hash matching.
✅ **Report Export & Sharing** – Generate downloadable reports for security teams.
✅ **Dark Mode & Accessibility** – Improve UI experience with a night-friendly theme.

Our Approach / Architecture 🛠️

1. **File Upload & Validation**: Users upload a suspicious file via an intuitive web interface.
2. **Static Analysis**: The backend performs signature-based analysis using:
   - **YARA Rules**: Identifying known malware patterns.
   - **PEFile Library**: Analyzing Windows executable structures.
   - **Entropy Calculation**: Detecting obfuscated or packed malware.
3. **Verdict Generation**: The system classifies the file as:
   - **Clean**: "No malicious indicators found."
   - **Malicious**: "High entropy and suspicious macro code detected."
4. **User Notification**: The results are displayed instantly on the UI with optional risk factor details.
5. **Security Measures**: Input validation, file size limits, and restricted file types to prevent exploitation.
6. **Additional Features**:
   - **File Hash Comparison** 🔍 – Identify threats instantly using known malware hash databases.
   - **Report Export & Sharing** 📄 – Generate downloadable reports for future reference.
   - **Dark Mode & Accessibility** 🌙 – User-friendly enhancements for all environments.

Team Information 👨‍💻👩‍💻

- **Arya P G** (Full Stack Developer) - Frontend & API Integration
- **Dyuthi Ramesh** (Security Engineer) - Malware Detection Logic
- **Syed Hashir Ahmed** (Backend Developer) - API Development & Database Integration
- **Mugdha Suresh** (UI/UX Designer) - User Experience & Interface

---

Tech Stack 🖥️🔧🛠️

Frontend

- React.js (for an interactive UI)
- Tailwind CSS (for styling)
- Axios (for API calls)

Backend

- Python (Flask/FastAPI for server-side processing)
- YARA (for pattern-based malware detection)
- PEFile (for analyzing Windows executables)
- SQLite/PostgreSQL (for storing scan logs - optional)

Security & Performance Enhancements

- **File Validation**: Restrict file types and sizes
- **Concurrency Handling**: Async processing for handling multiple requests
- **Scalability**: Deploying on AWS/GCP with load balancing

Conclusion 🎯

Our **Beluga Malware Scanner** is designed to provide **fast, accurate, and user-friendly malware detection**. With a robust backend powered by **static analysis tools**, a sleek frontend, and essential security measures, our system will help users make **informed decisions** about potentially harmful files. By integrating **modern web technologies**, we ensure **scalability and reliability**, making this an ideal solution for everyday users and security enthusiasts alike.