Advanced Log Analysis Tool

A powerful, web-based log file analysis platform that provides comprehensive insights through machine learning-powered clustering, anomaly detection, and predictive forecasting. Built with Flask, this tool transforms raw log data into actionable intelligence with an intuitive web interface.

🚀 Features

📈 Advanced Analytics

- **Real-time Log Processing:** Parse multiple log formats (Apache Common, Extended, Custom)
- **Machine Learning Clustering:** K-Means and DBSCAN algorithms for user behavior analysis
- **Anomaly Detection:** Multi-algorithm approach using Isolation Forest, Statistical Z-score, and Moving Average
- **48-Hour Forecasting:** Prophet-based predictive modeling with confidence intervals
- **Performance Monitoring:** Response time analysis and bottleneck identification

🛡️ Security Intelligence

- **Threat Detection:** Automatic identification of suspicious IP addresses
- **Attack Pattern Recognition:** SQL injection, XSS, and directory traversal detection
- **Security Scoring:** Real-time threat level assessment
- **Behavioral Analysis:** Bot detection and traffic pattern analysis

📊 Rich Visualizations

- **Interactive Dashboards:** Plotly-powered charts and graphs
- **Cluster Analysis:** PCA-based dimensionality reduction visualization
- **Time Series Analysis:** Traffic patterns and seasonal trends
- **Heatmaps:** Geographic and temporal activity mapping

⚡ Performance Features

- **Parallel Processing:** Multi-threaded analysis for large datasets
- **Memory Optimization:** Efficient handling of files up to 1GB
- **Progress Monitoring:** Real-time processing feedback
- **Caching:** Optimized for repeated analysis

🛠️ Installation

Prerequisites

- Python 3.8 or higher
- pip package manager
- 4GB+ RAM recommended for large log files

> ### Quick Start
>
> #### 1. Clone the repository
>
> ```
> git clone https://github.com/Akxt09/advanced-log-analysis.git
> cd advanced-log-analysis
> ```
>
> #### 2. Create virtual environment
>
> ```
> python -m venv venv
>
> # Activate virtual environment
> # Windows: venv\Scripts\activate
> # Linux/macOS: source venv/bin/activate
> ```
>
> #### 3. Install dependencies
>
> ```
> pip install -r requirements.txt
> ```
>
> #### 4. Configure environment
>
> ```
> # Copy environment template
> cp .env.example .env
>
> # Edit .env file with your settings
> SECRET_KEY=your-secure-secret-key-here
> FLASK_DEBUG=False
> UPLOAD_FOLDER=uploads
> ```
>
> #### 5. Run the application
>
> ```
> python app.py
> ```
>
> #### 6. Access the web interface
>
> ```
> http://localhost:5000
> ```

📁 Input Formats Supported

Apache Common Log	Apache Extended Log
CSV & TSV logs	Custom tab-separated logs

Made with ❤️ for developers, sysadmins, and data enthusiasts.
⭐ Star this repo to support the project!