**AI-Implemented Phishing & SQL Injection Detection Tool**

**1. Introduction**

Phishing attacks and SQL injection vulnerabilities are major security concerns in the digital world. This project aims to develop an AI-powered tool that detects phishing websites and SQL injection attempts using machine learning and heuristic analysis. The tool extracts various features from URLs, website structures, and user inputs to classify threats effectively.

**2. Objectives**

* Detect phishing websites using URL-based, content-based, and reputation-based features.
* Identify and prevent SQL injection attempts in web applications.
* Provide a user-friendly interface for security analysis.
* Utilize AI/ML models for real-time threat classification.
* Generate security reports for further analysis.

**3. System Architecture**

**3.1 Components**

* **Frontend:** Web interface for user input and report generation.
* **Backend:** Django for processing security checks.
* **Database:** Stores analyzed URLs, detected threats, and security logs.
* **AI/ML Engine:** Machine learning model for phishing and SQL injection detection.
* **External APIs:** Google Safe Browsing, VirusTotal (optional) for threat validation.

**3.2 Workflow**

1. User submits a URL or input data.
2. The system extracts features from the URL or input query.
3. AI model/classifier analyzes the data.
4. The tool classifies it as safe or malicious.
5. The result is displayed, and logs are stored.

**4. Feature Implementation**

**4.1 Phishing Detection Features**

* **URL-Based Features:** Checking for IP usage, long URLs, shortened links, special symbols, and redirections.
* **Content-Based Features:** Examining SSL certificates, favicon inconsistencies, and external resource loading.
* **User Interaction-Based Features:** Detecting popup windows, right-click disabling, and iframe redirections.
* **Reputation-Based Features:** Analyzing domain age, traffic rank, and Google index status.

**4.2 SQL Injection Detection Features**

* **Pattern-Based Detection:** Identifies SQL keywords in user inputs.
* **Behavioral Analysis:** Detects anomalies in database queries.
* **Web Application Firewall (WAF) Integration:** Prevents malicious queries.
* **Logging and Alerts:** Records attempted attacks for further review.

**5. Machine Learning Integration**

* **Model Used:** Supervised ML model (e.g., Random Forest, SVM, Neural Networks).
* **Dataset:** Trained on phishing URLs and SQL injection attack patterns.
* **Training and Testing:** Uses real-world datasets for better accuracy.
* **Adaptive Learning:** Improves detection over time based on new threats.

**6. User Interface**

* **Dashboard:** Allows users to enter URLs or text inputs for scanning.
* **Threat Alert System:** Displays warnings and security statuses.

**7. Deployment & Integration**

* Can be hosted on a cloud server.
* Browser extension integration for phishing alerts.
* API for third-party security tools.

**8. Future Enhancements**

* Enhancing detection accuracy with deep learning.
* Expanding threat database with real-time updates.
* Developing a mobile application for on-the-go security analysis.

**9. Conclusion**

This project provides an effective security solution by combining AI-driven phishing detection and SQL injection prevention. By integrating multiple security features, this tool enhances web security and helps mitigate cyber threats efficiently.