PhishSCAN

API Reference

Date: 11 September 2025

Contact: support@phishscan.com | +61 2 9123 4567

Address: Level 12, 1 Market Street, Sydney, NSW 2000, Australia

API Reference

The PhishSCAN API provides developers and researchers with an accessible interface for integrating phishing detection capabilities into their own applications. The API follows RESTful design principles, uses standard HTTP methods, and communicates primarily in JSON format. Base URL (local development): http://localhost:5000/api/ Key Endpoints: 1. POST /scan This endpoint accepts a JSON object containing a URL to be analyzed. Example request: { "url": "http://example.com" } Example response: { "status": "suspicious", "confidence": 0.87 } The status may be "legit", "suspicious", or "phishing". Confidence values range between 0 and 1, reflecting the model's certainty. 2. GET /history This endpoint retrieves a list of all URLs scanned during the current session. It is useful for reviewing past scans and tracking outcomes. The data is cleared when the backend restarts or when explicitly cleared by the user. 3. POST /clear-history This endpoint clears all scan records from memory. It allows users to reset their session and ensures that no long-term data is retained. Error Handling: If a request is malformed or missing required fields, the API returns a structured error response. For example: { "error": "Invalid request format" } Security Notes: In the academic deployment, the API runs locally and accepts requests from the browser extension via localhost. In a production environment, HTTPS encryption, API keys, and rate limiting should be implemented to ensure secure usage. Intended Use: The API is lightweight and designed for demonstration purposes, proof-of-concept projects, and educational training environments. It is not intended as a replacement for enterprise-grade security services but as a tool to raise awareness and provide practical hands-on experience.