Technical Test – Backend Developer

1. Overview

This test is designed for Backend Developers applying for a position at [redacted]. Your task is to build a robust, scalable API using Laravel, demonstrating your expertise in backend development, API design, and integration techniques.

2. Task Description

Your mission is to create an API that manages **assets and vulnerabilities**. The system should integrate with a public vulnerability database (e.g., **NVD API**) to enrich device data with CVEs.

The API should allow CRUD operations on assets, link vulnerabilities, and expose aggregated risk scores.

3. Requirements

Entities

- **Assets**:
    - Name
    - Description
    - Device type (Router, Switch, Server, etc.)
    - IP address
    - Location
    - Status
- **Vulnerabilities (linked to Assets)**:
    - CVE ID
    - Severity (Critical, High, Medium, Low)
    - Description
    - Date Published

Core Features

1. CRUD operations for Assets and Vulnerabilities.
2. Integration with **NVD API** to fetch vulnerability details by CVE ID.
3. Endpoint to calculate a **risk score per asset** based on attached vulnerabilities.

Mandatory Stack

- PHP 8.3
- Laravel 12 + Octane + Swoole
- PostgreSQL
- ClickHouse (for aggregated queries)

4. Instructions

- Follow SOLID, Clean Code, and Clean Architecture.
- Apply authentication (JWT or Laravel Sanctum).
- Add **Datadog logging/tracing hooks** where applicable.
- Document API endpoints (Swagger/OpenAPI).

5. Optional

- PHPUnit tests (mock NVD responses).
- Docker containerisation.

6. Evaluation Criteria

- Functionality, API design, best practices, performance, security, testing, documentation, Git usage.