# Vulnerability Chatbot Documentation

## Objective

This chatbot helps developers and security professionals identify and fix security vulnerabilities in their systems. It analyzes user-provided vulnerability data (e.g., CVE IDs) and offers actionable remediation suggestions.

## Key Technologies

1. **Streamlit**: Provides a user-friendly web interface for input and output.
2. **NVD API**: Retrieves detailed information about vulnerabilities.
3. **Hugging Face (GPT-2)**: Generates fix suggestions for vulnerabilities.

---

## Features

1. **Chatbot Interface**:
    - Simple and interactive web-based input for vulnerability details (CVE ID or description).
    - Displays retrieved vulnerability details and generated fix suggestions.
2. **Fetch Vulnerability Data**:
    - Integrates with the National Vulnerability Database (NVD) API to fetch:
        - CVE ID
        - Description
        - Severity
        - CVSS score
3. **Fix Suggestions**:
    - Provides practical remediation advice for vulnerabilities based on retrieved data.
4. **Testing**:
    - Robustly tested to handle a variety of vulnerabilities.

---

## System Architecture

1. **User Input**: Users provide a CVE ID or vulnerability description through the Streamlit app.
2. **Data Fetching**:
    - The app queries the NVD API for details related to the vulnerability.
3. **Data Processing**:
    - Extracts key information such as severity, CVSS score, and description.
4. **Suggestion Generation**:
    - A Hugging Face GPT-2 pipeline processes the vulnerability details and generates remediation advice.
5. **Output**:
    - Displays fetched vulnerability details and generated suggestions in the web interface.

---

## Setup Instructions

**Prerequisites**

- Python 3.8+
- Install dependencies:

```
pip install streamlit requests transformers
```

**Usage**

1. Clone the repository or download the script.
2. Run the Streamlit app:

```
streamlit run vol2.py
```

3. Input a CVE ID or vulnerability description and press "Analyze Vulnerability."

**Configuration**

- Replace the `apiKey` in `fetch_vulnerability_data` with your NVD API key.

---

## Testing

Test the application with different CVE IDs:

1. Common vulnerabilities (e.g., CVE-2021-44228).
2. Invalid or non-existent CVE IDs to test error handling.

---

## Limitations

- The chatbot relies on the accuracy of data from the NVD API and GPT-2. Ensure updates for optimal performance.
- Certain complex vulnerabilities may not generate actionable advice.