CONFident\_tool - Техническая документация

# Обзор проекта

CONFident\_tool - это программное решение для автоматизированного анализа конфигурационных файлов веб-серверов (Nginx, Apache) на предмет ошибок настройки и потенциальных уязвимостей. Инструмент позволяет выявлять распространенные проблемы безопасности, связанные с неправильной конфигурацией, и предоставляет рекомендации по их устранению.

# Архитектура

Проект построен по модульной архитектуре и состоит из следующих компонентов:

## Основные модули

1. \*\*Сканеры (scanners)\*\* - отвечают за анализ конфигурационных файлов конкретных веб-серверов

- `BaseScanner` - абстрактный базовый класс для всех сканеров

- `NginxScanner` - сканер для конфигураций Nginx

- `ApacheScanner` - сканер для конфигураций Apache

2. \*\*Уязвимости (vulnerabilities)\*\* - содержит определения типов уязвимостей

- `Vulnerability` - базовый класс для представления уязвимостей

- `nginx\_vulns.py` - уязвимости, характерные для Nginx

- `apache\_vulns.py` - уязвимости, характерные для Apache

3. \*\*Утилиты (utils)\*\* - вспомогательные классы и функции

- `Logger` - для ведения логов

- `ConfigFinder` - для поиска конфигурационных файлов

- `ReportGenerator` - для генерации отчетов в различных форматах

4. \*\*Шаблоны (templates)\*\* - эталонные безопасные конфигурации

- `secure\_nginx.conf` - эталонная конфигурация для Nginx

- `secure\_httpd.conf` - эталонная конфигурация для Apache

# Технические детали

## Сканеры

Сканеры работают по следующему алгоритму:

1. Поиск конфигурационных файлов

2. Парсинг конфигурации

3. Проверка на наличие уязвимостей

4. Формирование отчета о найденных проблемах

Специализируется на проверке конфигурационных файлов Nginx и выявляет такие уязвимости как:

- Включенный листинг директорий

- Отсутствие ограничений на размер запроса

- Небезопасная конфигурация выполнения PHP

Специализируется на проверке конфигурационных файлов Apache и выявляет такие уязвимости как:

- Включенный индексинг директорий

- Неограниченное выполнение CGI скриптов

- Неограниченное использование .htaccess файлов

## Обнаружение уязвимостей

Для поиска уязвимостей используются регулярные выражения, которые анализируют содержимое конфигурационных файлов и выявляют потенциально опасные настройки. Каждый тип уязвимости имеет определенные паттерны, которые указывают на наличие проблемы.

## Генерация отчетов

Отчеты могут быть сгенерированы в трех форматах:

- Консольный вывод - отображает результаты сканирования в терминале

- JSON - создает структурированный файл с результатами

- HTML - генерирует веб-страницу с детальной информацией о найденных уязвимостях

# Расширение функциональности

## Добавление новых типов уязвимостей

1. Создайте новый класс уязвимости в соответствующем файле (nginx\_vulns.py или apache\_vulns.py)

2. Унаследуйте его от базового класса Vulnerability

3. Реализуйте методы для поиска этой уязвимости в сканере

## Добавление поддержки новых веб-серверов

1. Создайте новый класс сканера, унаследованный от BaseScanner

2. Реализуйте методы find\_config\_files, parse\_config и check\_vulnerabilities

3. Создайте файл с определениями уязвимостей для нового веб-сервера

4. Добавьте поддержку нового типа сервера в main.py

# Требования и зависимости

- Python 3.6+

- ОС: Linux, macOS, Windows

- Без дополнительных внешних зависимостей для базовой функциональности

# Технические ограничения

- Сканер работает только с текстовыми конфигурационными файлами

- Не поддерживается анализ включаемых конфигураций через директивы include

- Отсутствует проверка синтаксической корректности конфигурационных файлов

# Безопасность

CONFident\_tool не вносит изменений в анализируемые конфигурационные файлы и не требует привилегированного доступа для базового функционала. Однако, для автоматического поиска конфигурационных файлов в стандартных системных директориях может потребоваться запуск с повышенными привилегиями.