Руководство пользователя CONFident\_tool

# Содержание

- Введение

- Установка

- Основные возможности

- Использование

- Параметры командной строки

- Форматы вывода

- Интерпретация результатов

- Устранение обнаруженных уязвимостей

- Устранение неполадок

# Введение

CONFident\_tool — это инструмент для автоматизированного анализа конфигурационных файлов веб-серверов (Nginx, Apache) на предмет ошибок настройки и потенциальных уязвимостей. Данный инструмент помогает системным администраторам и специалистам по безопасности своевременно выявлять и устранять проблемы в конфигурациях веб-серверов.

# Установка

## Предварительные требования

- Python 3.6 или выше

- Операционная система: Linux, macOS или Windows

## Шаги установки

1. Клонируйте репозиторий:

git clone https://github.com/vsosh-anonym/CONFident\_tool.git  
cd CONFident\_tool

2. Установите зависимости:

pip install -r requirements.txt

# Основные возможности

- Анализ конфигураций Nginx и Apache

- Обнаружение распространенных уязвимостей в настройках

- Формирование подробных отчетов с рекомендациями

- Поддержка различных форматов вывода (консоль, JSON, HTML)

- Возможность указания пользовательского пути к конфигурационным файлам

# Использование

Базовый синтаксис команды:

conf-ident/main.py --server-type <nginx/apache> [--config-path /path/to/configs] [--output <console/json/html>]

## Примеры использования

Сканирование конфигураций Nginx с выводом в консоль:

conf-ident/main.py --server-type nginx

Сканирование конфигураций Apache из указанной директории с сохранением отчета в HTML формате:

conf-ident/main.py --server-type apache --config-path /etc/apache2/ --output html

# Параметры командной строки

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | Описание | Обязательный | Значения по умолчанию |
| `--server-type` | Тип веб-сервера для сканирования | Да | - |
| `--config-path` | Путь к директории или файлу конфигурации | Нет | Стандартные пути конфигураций |
| `--output` | Формат вывода результатов | Нет | console |

# Форматы вывода

## Консольный вывод (console)

Выводит результаты сканирования напрямую в терминал с цветовым выделением уязвимостей разной степени критичности.

## JSON (json)

Создает структурированный JSON-файл с результатами сканирования, который можно использовать для интеграции с другими инструментами.

## HTML (html)

Генерирует HTML-отчет с подробным описанием найденных уязвимостей, их критичностью и рекомендациями по устранению.

# Интерпретация результатов

После завершения сканирования будет показана информация о найденных уязвимостях, включая:

- Название уязвимости

- Степень серьезности (низкая, средняя, высокая, критическая)

- Описание проблемы

- Рекомендации по устранению

- Затронутые файлы и строки конфигурации

# WEB-панель

Для удобства, можно использовать веб-панель.

python3 conf-ident/web-panel/app.py

Веб-панель предоставляет следующие возможности:

- Интуитивно понятный графический интерфейс для запуска сканирований

- Выбор типа веб-сервера и пути к конфигурациям через веб-формы

- Визуализация результатов сканирования в удобном формате

- Интерактивные подсказки по устранению найденных уязвимостей

- История проведенных сканирований

- Возможность экспорта отчетов в различных форматах

# Устранение обнаруженных уязвимостей

## Общие рекомендации

1. Внимательно изучите описание каждой найденной уязвимости

2. Ознакомьтесь с рекомендациями по устранению

3. Внесите необходимые изменения в соответствующие конфигурационные файлы

4. Проверьте синтаксическую корректность измененных конфигураций

5. Перезапустите веб-сервер для применения изменений

6. Запустите сканирование повторно, чтобы убедиться в устранении уязвимостей

## Распространенные уязвимости и их устранение

1. **Directory Listing Enabled**

- Проблема: Включен листинг содержимого директорий

- Решение: Замените `autoindex on;` на `autoindex off;` или полностью удалите эту директиву

2. **No Request Size Limit**

- Проблема: Не установлено ограничение на размер запроса

- Решение: Добавьте директиву `client\_max\_body\_size 10m;` (или другое подходящее значение)

3. **Unsafe PHP Execution Configuration**

- Проблема: Небезопасная конфигурация выполнения PHP-скриптов

- Решение: Добавьте `try\_files $uri =404;` перед директивой `fastcgi\_pass`

4. **Directory Indexing Enabled**

- Проблема: Включен листинг содержимого директорий

- Решение: Замените `Options Indexes FollowSymLinks` на `Options -Indexes +FollowSymLinks`

5. **Unrestricted CGI Execution**

- Проблема: Неограниченное выполнение CGI-скриптов

- Решение: Ограничьте выполнение CGI конкретной директорией и используйте `ScriptAlias`

6. **Unrestricted .htaccess Usage**

- Проблема: Неограниченное использование .htaccess файлов

- Решение: Замените `AllowOverride All` на `AllowOverride None` или укажите конкретные категории

# Устранение неполадок

## Инструмент не находит конфигурационные файлы

1. Убедитесь, что у вас есть доступ к директориям с конфигурационными файлами

2. Используйте параметр `--config-path` для явного указания пути к конфигурационным файлам

3. Проверьте, что файлы имеют расширение `.conf`

## Ошибка при запуске

1. Убедитесь, что у вас установлен Python 3.6 или выше

2. Проверьте, что все зависимости установлены корректно

3. Убедитесь, что скрипт имеет права на выполнение (`chmod +x conf-ident/main.py`)

## Неполные результаты сканирования

1. Проверьте, что сканируются все необходимые конфигурационные файлы, включая включаемые файлы

2. Используйте параметр `--config-path` для указания директории, содержащей все конфигурационные файлы