Модуль 3.Сканирование приложений на уязвимости (vo_HW)

Задание № 3.3.Детектирование заголовков с помощью Nuclei

Описание шаблона

Данный шаблон используется для обнаружения дефолтных логинов в API Apache Airflow. Он нацелен на тестирование API на наличие уязвимости через использование стандартных или слабых логинов и паролей, что может позволить злоумышленникам получить доступ к системе без предварительного взлома. Шаблон включает в себя проверку на дефолтные учетные записи, такие как "airflow" и "admin", с соответствующими паролями.

Детальное описание и функциональное назначение каждой конструкции в шаблоне

Секция `info`

Секция `info` предоставляет основную информацию о шаблоне, включая его название, автора, уровень серьезности и теги.

- **name**: Название шаблона. В данном случае шаблон проверяет дефолтные логины в API Apache Airflow.
- **author**: Автор шаблона — Павел Пархомец.
- **severity**: Уровень серьезности. Указано "critical", что означает, что уязвимость имеет высокий уровень риска.
- **tags**: Теги, которые помогают классифицировать шаблон. Здесь указаны теги, которые указывают, что шаблон относится к API, Apache Airflow, дефолтным логинам и использованию брутфорса.

Секция `requests`

Секция `requests` описывает HTTP-запросы, которые будут отправляться для обнаружения уязвимости.

- **method**: Метод HTTP-запроса. В данном случае используется GET-запрос для получения информации о "dags" (DAGs - Directed Acyclic Graphs) в Apache Airflow.
- **path**: Путь для API-запроса. Здесь используется переменная {{BaseUrl}}, которая будет заменена на базовый URL целевой системы. Путь /api/v1/dags указывает на API-эндпоинт для получения данных о DAGs.

Секция `headers`

- **Authorization**: Заголовок для авторизации. В данном случае используется Basic Authentication с кодированием в base64 для логина и пароля. В шаблоне будут тестироваться пары логин/пароль с базовыми значениями, например "airflow" и "admin".
- **Content-Type**: Тип содержимого, который должен быть отправлен в запросе. Здесь указан "application/json", что подразумевает отправку данных в формате JSON. Однако есть ошибка в значении: должно быть "application/json", а не "applixation/json".

Секция `payloads`

В разделе payloads перечисляются возможные значения для логинов и паролей, которые будут использоваться в запросах.

- **username и password**: Списки возможных значений для логинов и паролей, которые будут протестированы (в данном случае "airflow" и "admin").
- **attack**: Тип атаки. Используется "clusterbomb", что означает, что будет произведена брутфорс-атака, комбинируя все возможные логины и пароли.
- **matchers-condition**: Условие, которое указывает, что все проверяемые строки должны совпадать (логика "and").
- **matcher**: Этот блок указывает, что нужно искать в ответах от сервера:
- **Первый type**: word ищет слово "dag_id" в теле ответа. Это проверка, чтобы убедиться, что API работает правильно.
- **Второй type**: word ищет слово "kafka_server_sockerservermetrics_successful_reauthentication_rate" в теле ответа и проверяет, что оно отсутствует (параметр negative: true).
- **stop-at-first-match**: Указывает, что если найдено первое совпадение, дальнейшие попытки тестирования не будут выполнены.