**Наименование**: Проверка возможности взаимодействия с API по защищенному протоколу https;

**Краткое описание:** Проверяется возможность взаимодействия с API по защищенному протоколу https;

**Предусловие:** Тестируемое приложение должно быть доступно для взаимодействия через API;

**Шаги к выполнению:**

1. Отправить GET запрос по защищённому протоколу https на следующий URL: https://api.apilayer.com/exchangerates\_data/symbols

**Постусловие: -**

**Ожидаемый результат:**

1. Код статуса равен 200 «OK».

**Наименование:** Проверка работы аутентификации через API key

**Краткое описание:** Проверяется работа аутентификации в API через метод API key;

**Предусловие:**

1. Тестируемое приложение должно быть доступно для взаимодействия через API;
2. Получить API key для успешной аутентификации.

**Шаги к выполнению:**

1. Направить запрос на любую из конечных точек, описанных в документации, без авторизации;
2. Направить запрос на любую из конечных точек, описанных в документации, с валидным API ключом;
3. Направить запрос на любую из конечных точек, описанных в документации, с невалидным API ключом.

**Постусловие: -**

**Ожидаемый результат:**

1. Для работы c API требуется аутентификация;
2. Аутентификация с помощью ключа API выполнена успешно, запрос успешно обработан, был получен код 2XX;
3. Аутентификация с помощью ключа API не выполнена, получен код не равный 2XX.

**Наименование:** Проверка отсутствия отладочной и конфигурационной информации в ответах на запросы.

**Краткое описание:** Проверяется отсутствие отладочной и конфигурационной информации в ответах на запросах к API;

**Предусловие:**

1. Тестируемое приложение должно быть доступно для взаимодействия через API;
2. Изучить информацию, возвращаемую в ответах на запросы, в документации.

**Шаги к выполнению:**

1. Последовательно направить запросы к конечным точкам API, описанным в документации, и записать заголовки, код статуса и тело ответов в файл.

**Постусловие: -**

**Ожидаемый результат:**

1. Результаты запросов проанализированы ответственным специалистом и получена резолюция, что в ответах системы не содержится информации, относящиеся к отладочной и/или конфигурационной.

**Наименование:** Проверка отсутствия конечных точек неописанных в документации.

**Краткое описание:** Проверяется отсутствие в системе неописанных в документации конечных точек.

**Предусловие:**

1. Ознакомится с описанными в документации кончеными точками;
2. Развернуть в виртуальной среде копию тестируемого приложения, описанные ниже шаги должны выполняться в приложении, развернутом в виртуальной среде.
3. Тестируемое приложение, развернутое в виртуальное среде, должно быть доступно для взаимодействия через API;

**Шаги к выполнению:**

1. Выполнить GET запросы на конечные точки, описанные в файле, расположенному по следующему URL: <https://github.com/danielmiessler/SecLists/blob/master/Discovery/Web-Content/api/api-endpoints-res.txt>, сохраняя заголовки, код статуса и тело ответов в документ.

**Постусловие:** При необходимости приостановить работу виртуальной среды тестирования.

**Ожидаемый результат:**

1. Результаты запросов проанализированы ответственным специалистом и получена резолюция, что в тестируемом приложении отсутствую конечные точки, неописанные в документации.

**Наименование:** Проверка недоступности старых версий API

**Краткое описание:** Проверяется невозможность обработки запросов, направленных к старым версиям API

**Предусловие:**

1. Тестируемое приложение должно быть доступно для взаимодействия через API;
2. Изучить варианты выбора версии в документации к API системы;

**Шаги к выполнению:**

1. Отправить запрос на конечную точку c указанием неактуальной версии API;

**Постусловие: -**

**Ожидаемый результат:**

1. Код ответа не равен 2xx.

**Наименование:** Проверка доступности только задокументированных HTTP-методов

**Краткое описание:** В Системе проверяется факт обработки только тех HTTP-методов, которые задокументированы.

**Предусловие:**

1. Ознакомится с методами, которые поддерживают, описанные в документации, конечные точки.
2. Развернуть в виртуальной среде копию тестируемого приложения, описанные ниже шаги должны выполняться в приложении, развернутом в виртуальной среде;
3. Тестируемое приложение, развернутое в виртуальное среде, должно быть доступно для взаимодействия через API.

**Шаги к выполнению:**

1. Выполнить запросы на конечные точки, описанные в документации, по методам, описанным в файле, расположенному по следующему URL: <https://github.com/danielmiessler/SecLists/blob/master/Fuzzing/http-request-methods.txt>, сохраняя заголовки, код статуса и тело ответов в документ.

**Постусловие:**

1. При необходимости приостановить работу виртуальной среды тестирования.

**Ожидаемый результат:**

1. Результаты запросов проанализированы ответственным специалистом и получена резолюция, что система успешна отклоняет запросы с методами, не описанными в документации API.

**Наименование:** Проверка подверженности SQL-инъекциям.

**Краткое описание:**

**Предусловие:**

1. Тестируемое приложение должно быть доступно для взаимодействия через API;
2. Ознакомится с методами, которые поддерживают, описанные в документации, конечные точки.
3. Развернуть в виртуальной среде копию тестируемого приложения, описанные ниже шаги должны выполняться в приложении, развернутом в виртуальной среде.

**Шаги к выполнению:**

1. Выполнить сканирование конечных точек, используя утилиту nuclei с шаблонами sql инъекций.

**Постусловие:**

1. При необходимости приостановить работу виртуальной среды тестирования.

**Ожидаемый результат:**

1. Результат работы утилиты nuclei не содержит информации о найденный sql инъекциях.

**Наименование:** Проверка использования неустаревших версий TLS.

**Краткое описание:**

**Предусловие:**

1. Тестируемое приложение должно быть доступно для взаимодействия через API;

**Шаги к выполнению:**

1. Выполнить сканирование конечных точек, используя утилиту nuclei с шаблонами ssl.

**Постусловие: -**

**Ожидаемый результат:**

1. Результат работы утилиты nuclei не содержит информации о поддержки версий TLS ниже 1.2.