

Задача 1

Краткое описание запросов коллекции и процесса получения токена для сайта [Safe Browsing API](#)

Для использования Safe Browsing API был получен API-ключ из Кабинета разработчика

С помощью Postman была протестирована работа следующих методов:

- a. Получение информации об актуальных списках Safe Browsing, хранящихся на серверах Яндекса.

Запрос возвращает информацию об актуальных списках Safe Browsing, хранящихся на серверах Яндекса

Запрос:

GET <https://sba.yandex.net/v4/threatLists?91b10dca-adc0-4741-a79e-0fbd45e14af2>

Ответ:

```
{
  "threatLists": [
    {
      "threatType": "MALWARE",
      "platformType": "WINDOWS",
      "threatEntryType": "URL"
    },
    {
      "threatType": "MALWARE",
      "platformType": "LINUX",
      "threatEntryType": "URL"
    }
  ]
}
```

- b. Проверка двух URL на содержание в списках Safe Browsing. Также было составлено тело запроса.

Запрос позволяет узнать, содержатся ли проверяемые URL в [списках Safe Browsing](#), размещенных на сервере Яндекса. Если URL ресурса найден хотя бы в одном из списков, возвращается информация об угрозе, которую ресурс представляет для пользователя.

Запрос:

POST <https://sba.yandex.net/v4/threatMatches:find?key=91b10dca-adc0-4741-a79e-0fbd45e14af2>

Тело запроса

```
{
  "threatInfo": {
    "threatTypes": ["MALWARE"],
    "platformTypes": ["WINDOWS"],
    "threatEntryTypes": ["URL"],
    "threatEntries": [
      {"url": "https://yandex.ru/dev/safebrowsing/doc/quickstart/concepts/lookup.html"}
    ]
  }
}
```

Ответ:

Если ни один из проверяемых URL не обнаруживается в списках Safe Browsing, тело ответа возвращается пустым. Если совпадения есть, ответ должен содержать подробную информацию об опасности, представляемой каждым из найденных ресурсов.