



# Введение в ИБ, или Курс ЭТИЧНОГО тестировщика

# Что будет на занятии



База про ИБ



Что такое уязвимость



Какие бывают уязвимости

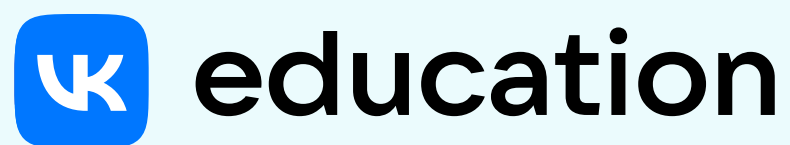


Правила поиска уязвимостей



Лайфхаки от ИБ ВКонтакте





Что такое  
информационная  
безопасность?

# Информационная безопасность

Информационная безопасность — это набор мер, предназначенных для защиты данных и устройств от угроз.

Основные 3 составляющих ИБ:

- целостность
- доступность
- конфиденциальность



# Важные определения

**Уязвимость** — ошибка в программном обеспечении или оборудовании, позволяющая получить несанкционированный доступ к информации, либо нарушить работу сервиса

**Приватность** — защита данных пользователя от третьих лиц



# Два вида уязвимостей в приложениях

**Client-side** — уязвимости, срабатывающие на стороне пользователя

**Server-side** — уязвимости, которым подвержено приложение на стороне сервера (бэкенд)



# SQL-инъекции

```
GET /walls/top?offset=0&last_date=0&count=10'&tab=top HTTP/2
Host: ██████████
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: application/json, text/plain, */*
```

```
HTTP/2 200 OK
Date: Thu, 13 Apr 2023 15:34:00 GMT
Content-Type: application/json; charset=utf-8
X-Powered-By: PHP/8.1.2-1ubuntu2.11
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: HEAD, GET, POST, PUT, PATCH, DELETE, OPTIONS
Cf-Cache-Status: DYNAMIC
Report-To:
{"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=NVSNGpVaACBEbK78QKbVHa35IOrBIHGkAW9zWVtBOaaP1
9XaihOvF%2Bm%2F58coM3AGHzQlAMxgU4J2OdFBpqUXy%2BhSOyM255Rjh5yrM%2FL5ztcAVBCyA%3D%3D"}],"group":"cf-
-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 7b74c54f3f0e3a4a-FRA
Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

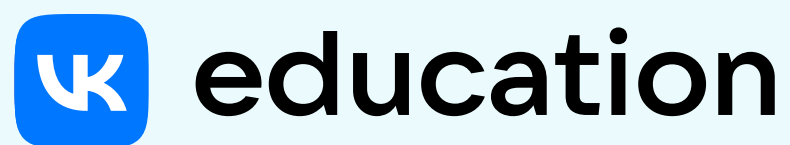
<br/>
<b>Fatal error: Uncaught [
  42000
]-SQLSTATE[
  42000
]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server
version for the right syntax to use near 'OFFSET 0--keep-cache' at line 1
trace: #0 /var/www/fastuser/data/www/██████████base/rb-mysql.php(1175):
RedBeanPHP\Driver\RPDO->runQuery('SELECT walllik...',
Array)
#1 /var/www/fastuser/data/www/██████████base/rb-mysql.php(4374): RedBeanPHP\Driver\RPDO->getAll('SELECT
'walllik...',
Array)
#2 /var/www/fastuser/data/www/██████████base/rb-mysql.php(6615): RedBeanPHP\Adapter\DBAdapter->get('SELECT
'walllik...',
Array)
#3 /var/www/fastuser/data/www/██████████base/rb-mysql.php(8453):
RedBeanPHP\QueryWriter\AQueryWriter->queryRecord('walllikes',
Array,
'date_create_wal...',
```



'XOR(if(now())=sysdate(),sleep(5\*5),0))OR'

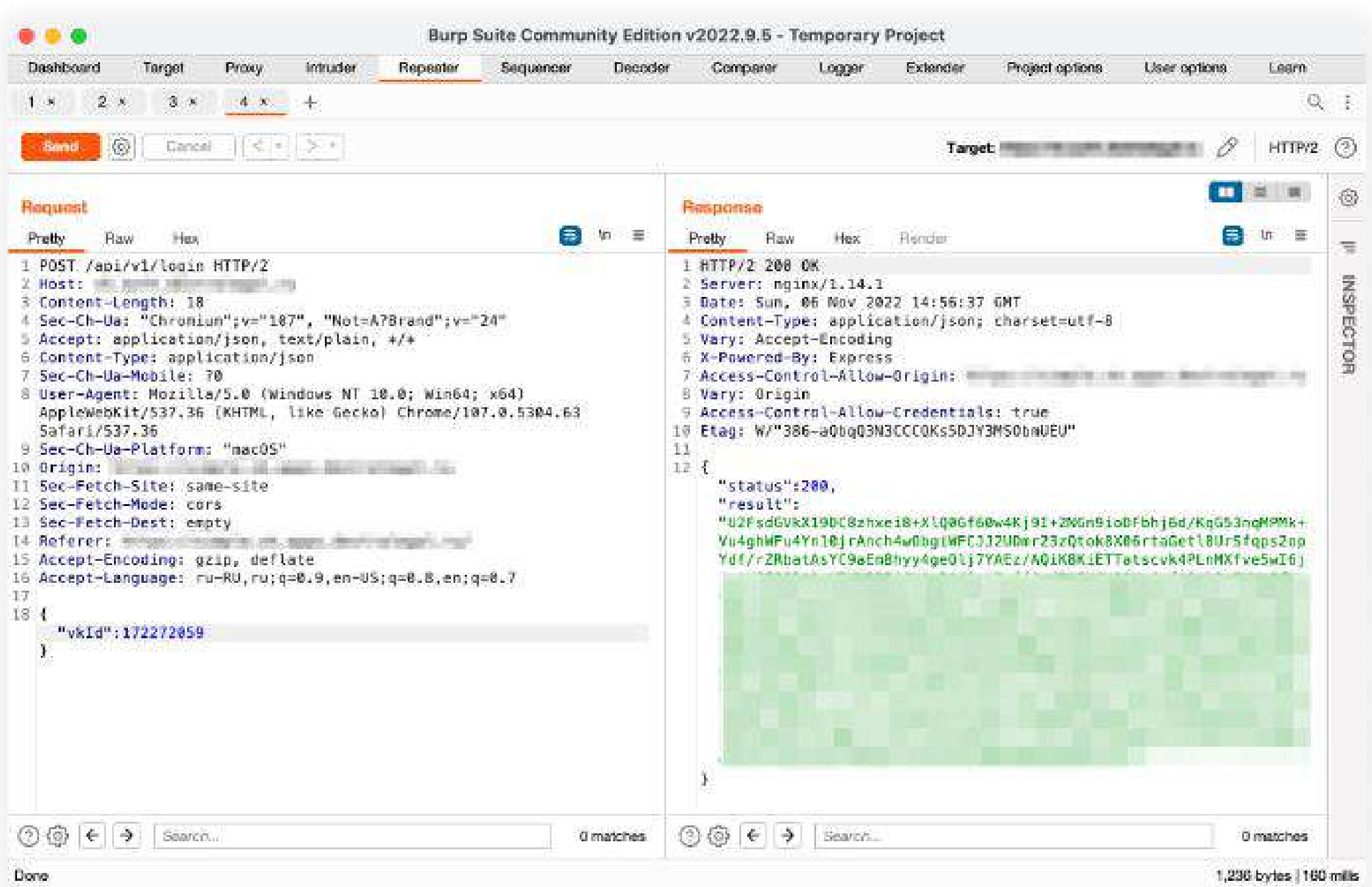






# Сломанный контроль доступа

# Отсутствие проверки подписи

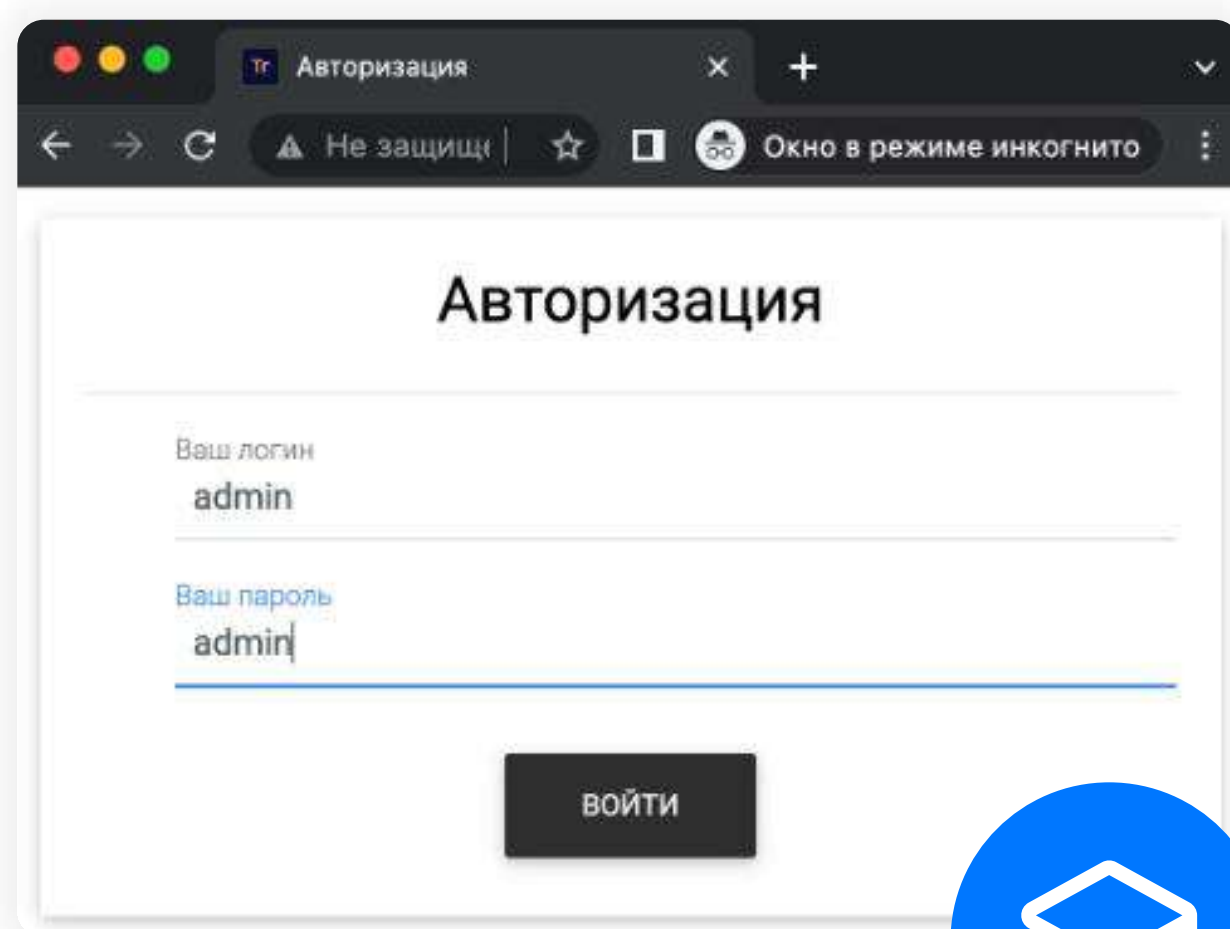


Авторизация происходит посредством простой передачи VK ID пользователя

# Слабый пароль или его отсутствие

Часто используемые пароли:

- admin
- 123456
- 123456789
- qwerty
- 12345
- password
- 12345678



Авторизация

Ваш логин  
admin

Ваш пароль  
admin

ВОЙТИ





# Раскрытие информации

# Дебаг-режим

```
← → ↺ ↻ ↵ /remote_users?pk_user_id="><script>alert(1)</script>"
UnboundLocalError at /remote_users
local variable 'users' referenced before assignment

Request Method: GET
Request URL: /remote_users?pk_user_id="%22%3E%3Cscript%3Ealert(1)%3C/script%3E"
Django Version: 3.2.6
Exception Type: UnboundLocalError
Exception Value: local variable 'users' referenced before assignment
Exception Location: /home/.../social1b/remote_db.py, line 168, in user
Python Executable: /home/.../bin/python
Python Version: 3.9.5
Python Path: ['/home/...',
              '/usr/lib/python3.9.zip',
              '/usr/lib/python3.9/',
              '/usr/lib/python3.9/lib-dynload',
              '/home/sellerunner/.local/share/.../lib/python3.9/site-packages']
Server time: Tue, 12 Oct 2021 18:01:59 +0000

Traceback (Switch to copy and paste view)
/home/.../.local/share/.../lib/python3.9/site-packages/django/core/handlers/exception.py, line 47, in inner
47.         response = get_response(request)
    Local vars

/home/.../.local/share/.../lib/python3.9/site-packages/django/core/handlers/base.py, line 181, in _get_response
181.         response = wrapped_callback(request, *callback_args, **callback_kwargs)
    Local vars

/home/.../.local/share/.../lib/python3.9/site-packages/django/views/decorators/csrf.py, line 54, in wrapped_view
54.         return view_func(*args, **kwargs)
    Local vars

/home/.../.local/share/.../lib/python3.9/site-packages/django/views/generic/base.py, line 70, in view
70.         return self.dispatch(request, *args, **kwargs)
    Local vars

/home/.../.local/share/.../lib/python3.9/site-packages/django/framework/views.py, line 509, in dispatch
509.         response = self.handle_exception(exc)
    Local vars

/home/.../.local/share/.../lib/python3.9/site-packages/django/framework/views.py, line 469, in handle_exception
469.         self.raise_uncaught_exception(exc)
    Local vars

/home/.../.local/share/.../lib/python3.9/site-packages/django/framework/views.py, line 480, in raise_uncaught_exception
```



# Поиск утечек в коде

1

Открыть DevTools, нажав F12

2

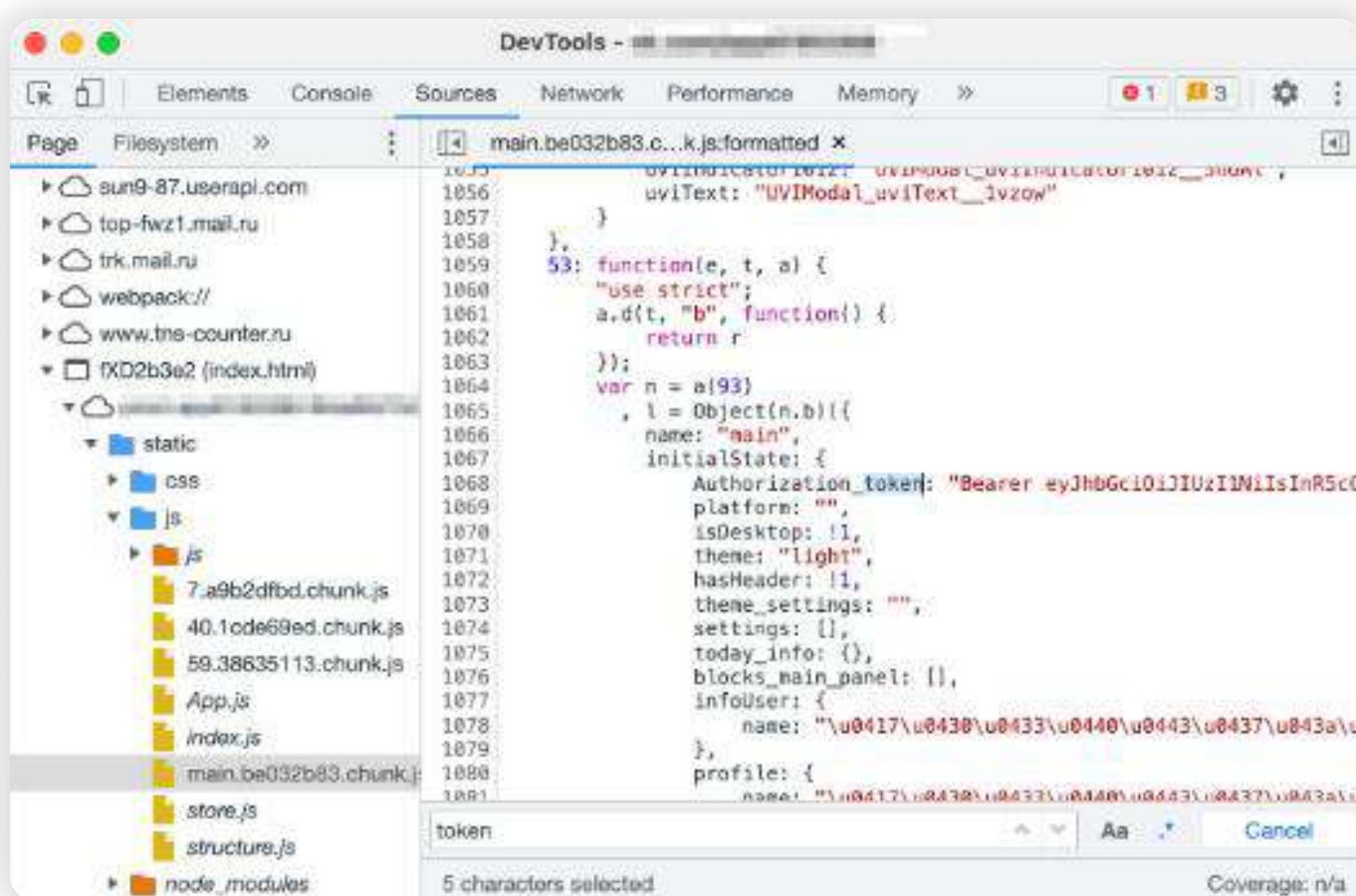
Перейти во вкладку Source

3

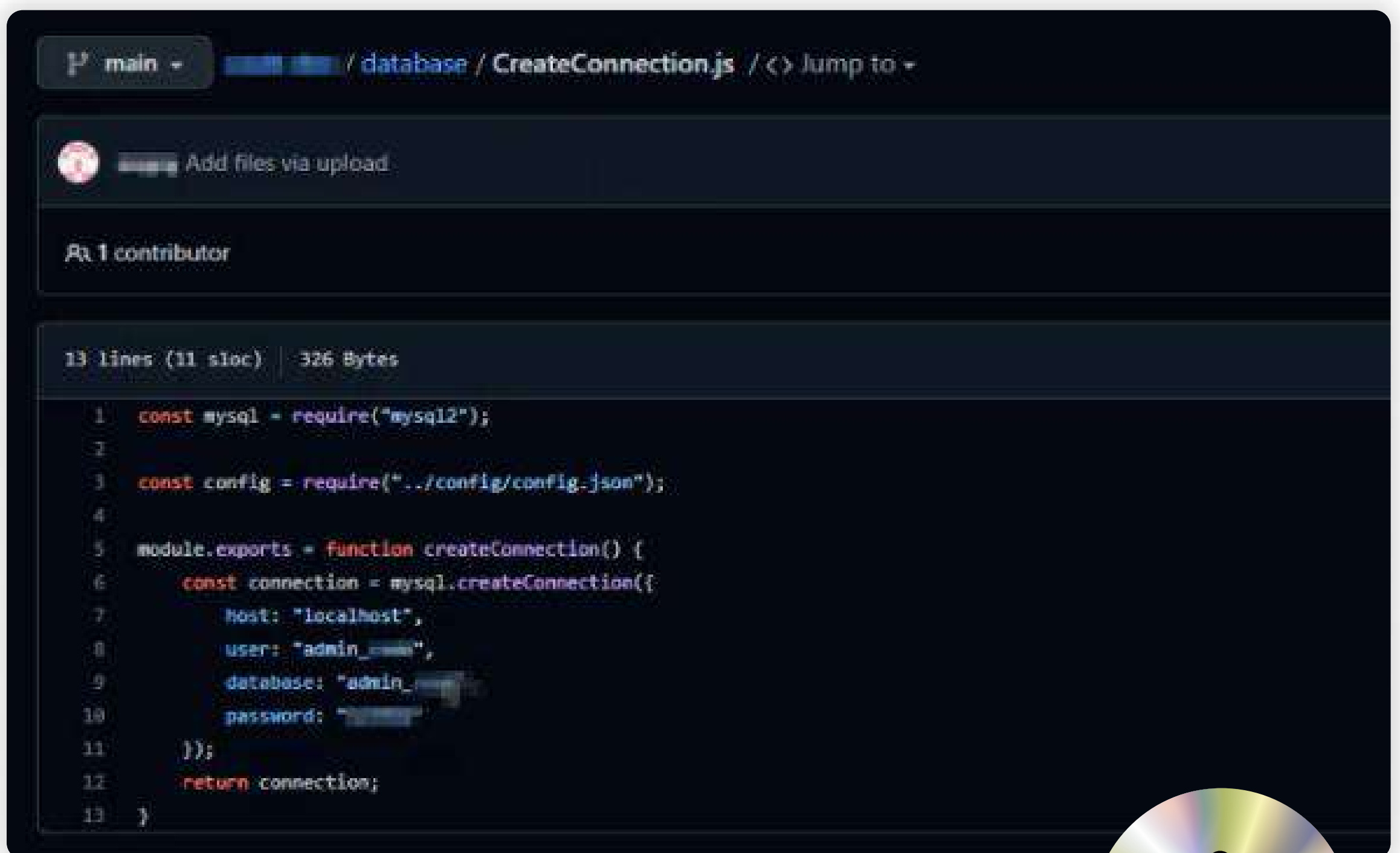
Открыть js-код приложения

4

Ctrl + F: access | token | http | key



# Открытые репозитории



The screenshot displays a GitHub repository interface. At the top, the breadcrumb navigation shows the path: `main` / `database` / `CreateConnection.js`. Below this, there is a button labeled "Add files via upload" and a note indicating "1 contributor". The main area shows the content of the `CreateConnection.js` file, which is 13 lines long (11 lines of code) and 326 bytes in size. The code is as follows:

```
1  const mysql = require("mysql2");
2
3  const config = require("../config/config.json");
4
5  module.exports = function createConnection() {
6    const connection = mysql.createConnection({
7      host: "localhost",
8      user: "admin_user",
9      database: "admin_db",
10     password: "password"
11   });
12   return connection;
13 }
```





# Race Condition





# Ботвинья на воде

## Ботвинья на воде

01:00   Русская   Первые блюда

### Энергетическая ценность на 6 порций

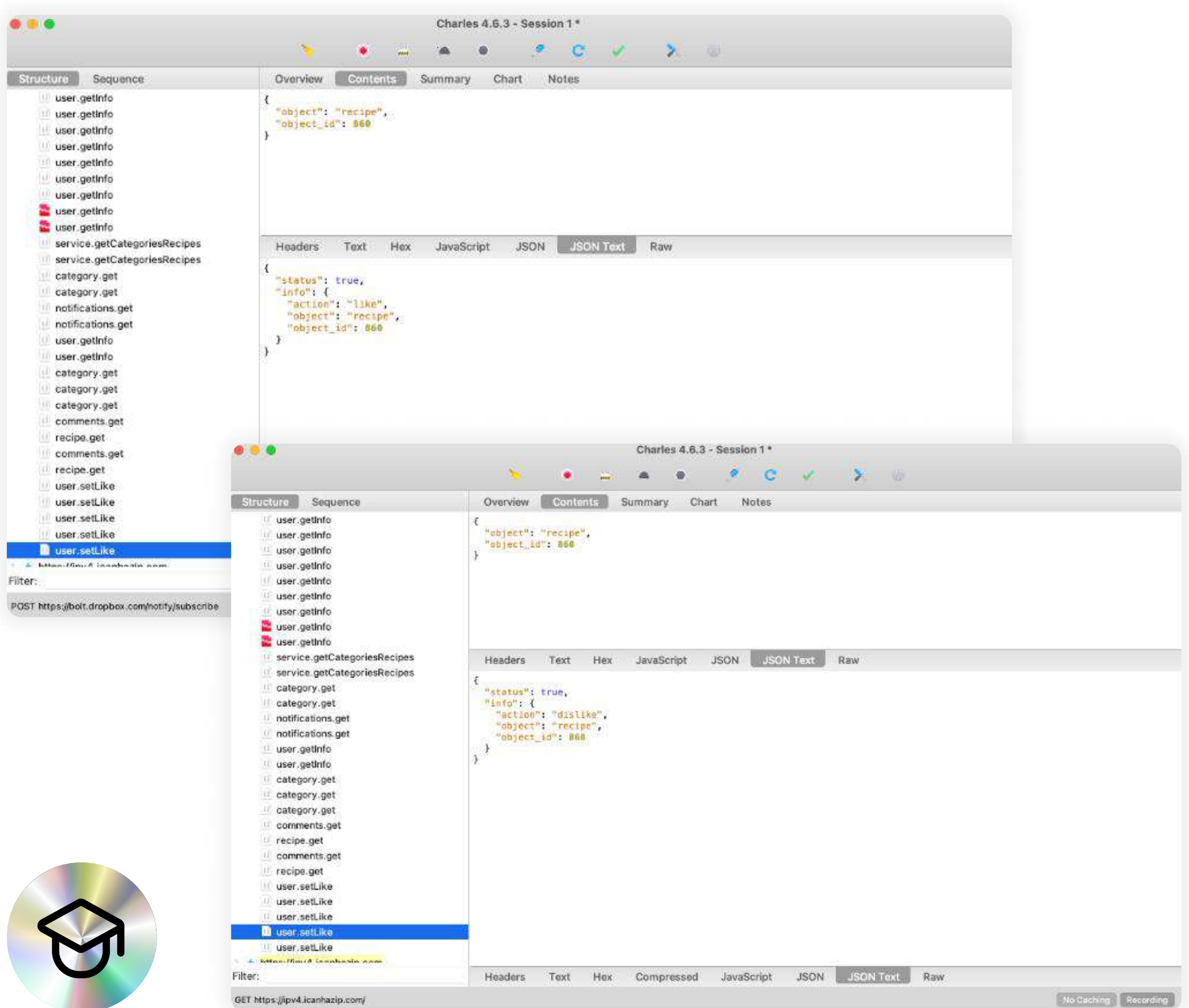
Ценность ?	Белки ?	Жиры ?	Углеводы ?
11.65	0.11	1.01	0.60
ккал	грамм	грамм	грамм

7   0

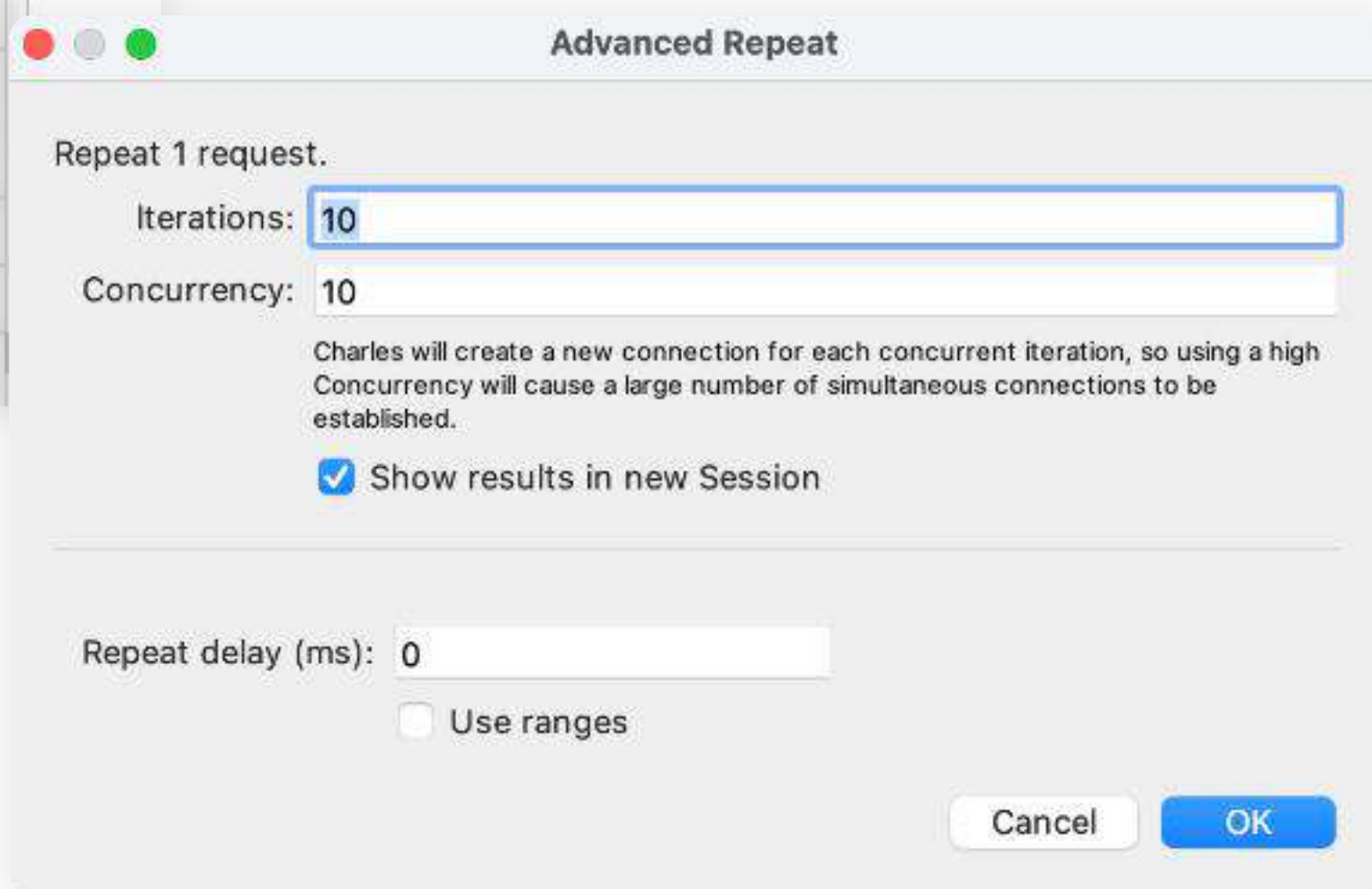
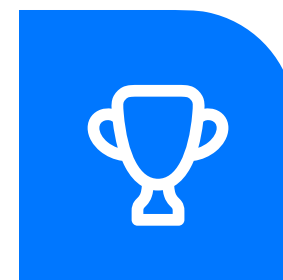
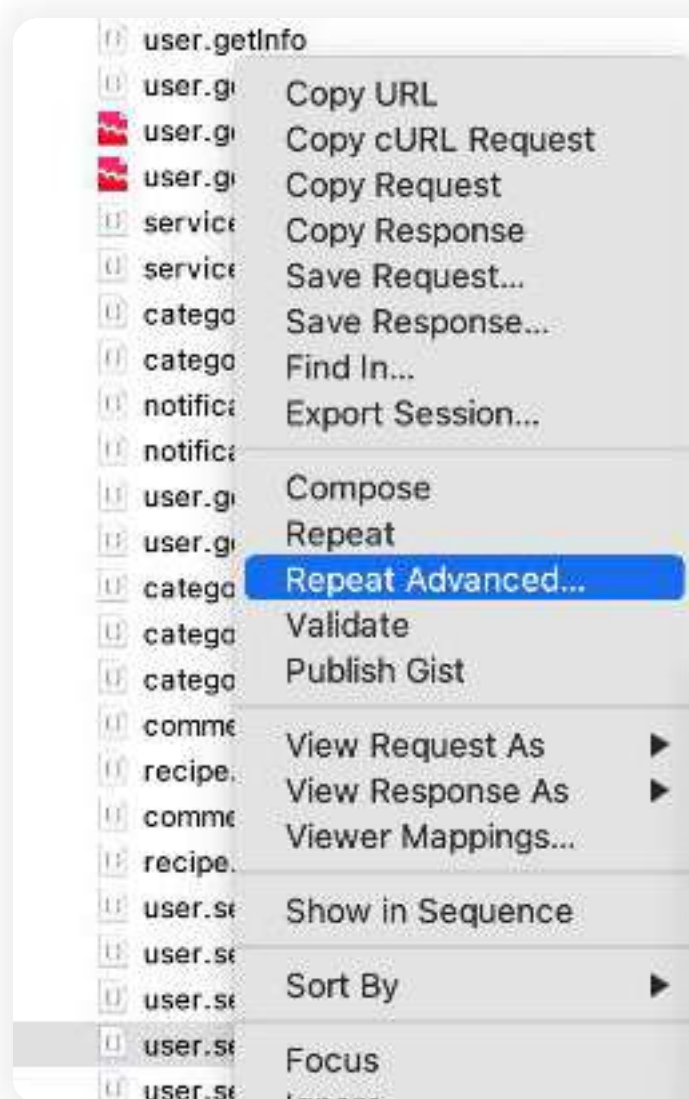
303

Нравится

# Смотрим, какие запросы уходят



# Отправляем 10 запросов в 10 потоков



# Смотрим результат



Charler 4.8.3 - Session 2

Session 1Session 2

StructureSequenceOverviewContentsSummaryChartNotes

user.setLike  
user.setLike  
user.setLike  
user.setLike  
user.setLike  
user.setLike  
user.setLike  
user.setLike  
user.setLike  
user.setLike

```
{
  "object": "recipe",
  "object_id": 888
}
```

HeadersTextHexJavaScriptJSONJSON TestRaw

```
{
  "status": true,
  "info": {
    "action": "setLike",
    "object": "recipe",
    "object_id": 888
  }
}
```

Filter

Ботвинья на воде

🕒 01:00

🍴 Русская

🍽️ Первые блюда

Энергетическая ценность на 6 порций

Ценность ?	Белки ?	Жиры ?	Углеводы ?
11.65	0.11	1.01	0.60
ккал	грамм	грамм	грамм

👍 -1

💬 0

👁️ 303

👎 Не нравится

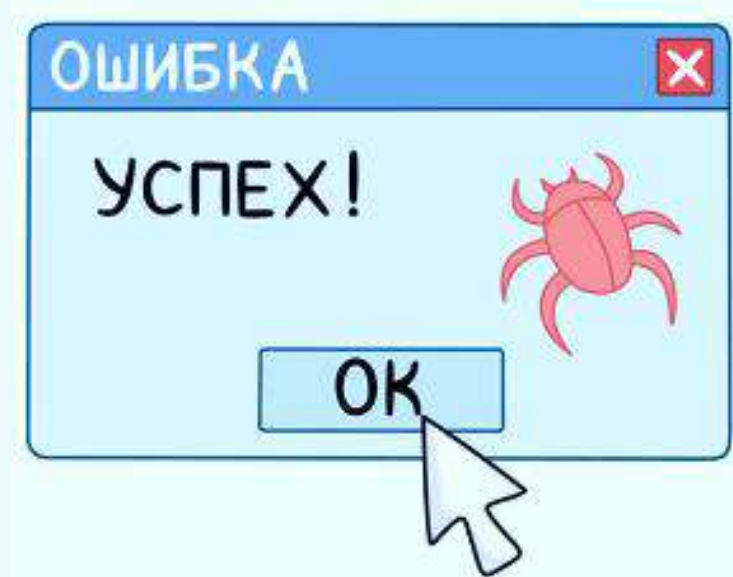
# Где стоит проверять?

- ➔ Пополнение счёта / вывод денежных средств со счёта
- ➔ Покупка/перевод
- ➔ Создание нескольких сущностей там, где предполагается одна
- ➔ Активация бонусов
- ➔ Везде, где есть ограничение на выполнение действия



# XSS

## (межсайтовый скриптинг)



# Stored XSS

**Адрес**

1

— Россия, Ленинградская область, Всеволожский район, Мурино, Новая улица, 7

Редактировать

Удалить

НАЗВАНИЕ

АДРЕС

✓

КВАРТИРА

1

ЭТАЖ

1

ПОДЪЕЗД

1

ДОМОВЫЙ

1

ЛИФТ

есть

Подтвердите действие на странице 

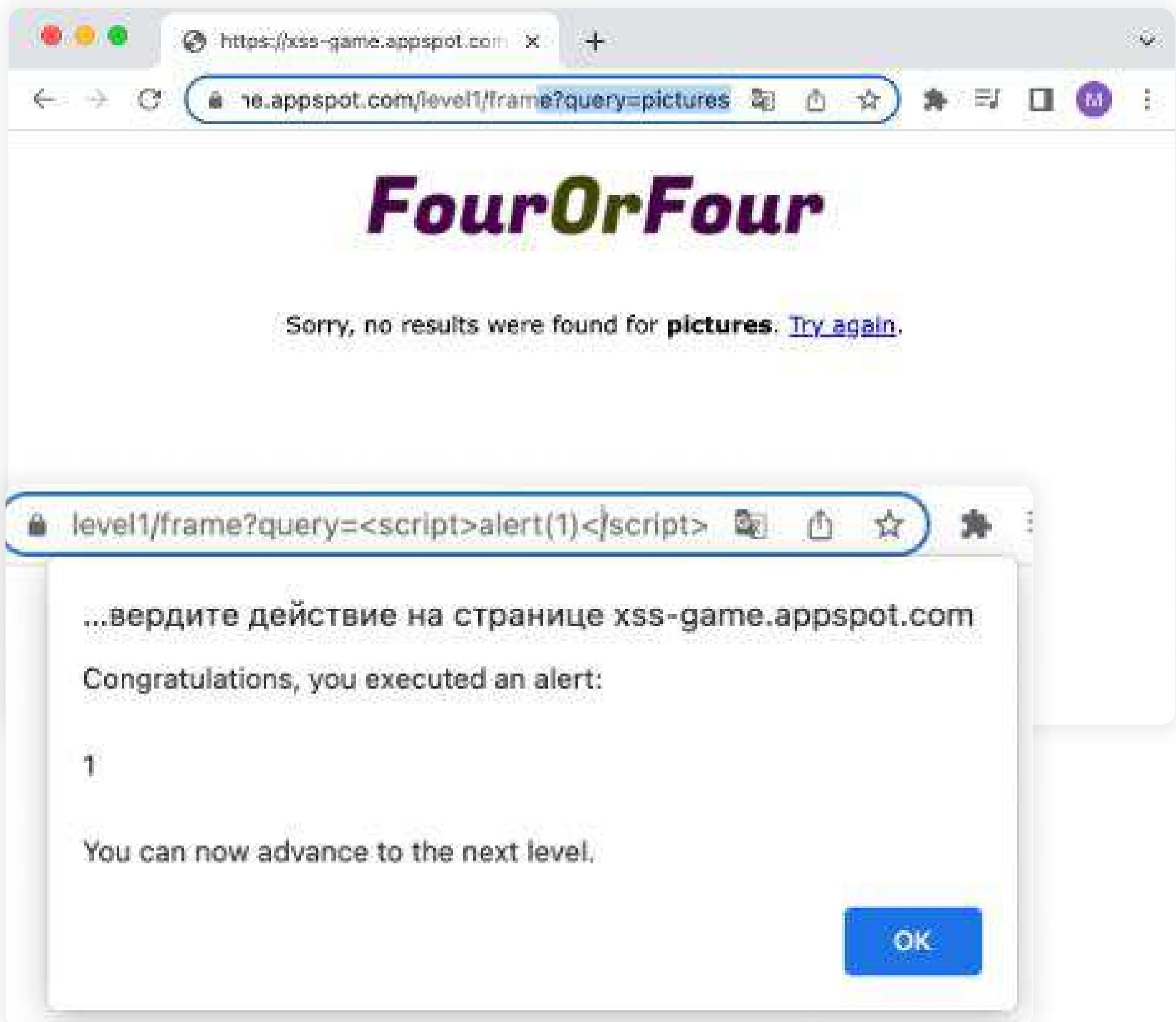
test

OK

`<script>alert('test')</script>`



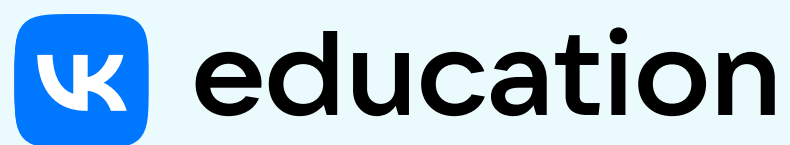
# Reflected XSS



Domain?query=<script>alert(1)</script>







Больше  
уязвимостей нет?

Конечно, есть!



# Правила поиска уязвимостей

1

Соблюдайте установленные ограничения по количеству запросов

2

Для тестирования используйте только собственные аккаунты

3

Не раскрывайте уязвимости другим

4

Сомневаетесь в поведении — уточните у [/testpool](#)

5

Используйте недеструктивные нагрузки и не выводите из строя ресурс



# Немного советов



Изучите тестируемый ресурс



Заготовьте шаблоны нагрузок



Не бойтесь изучать что-то новое



Следите за трендами в ИБ





ПОКА!