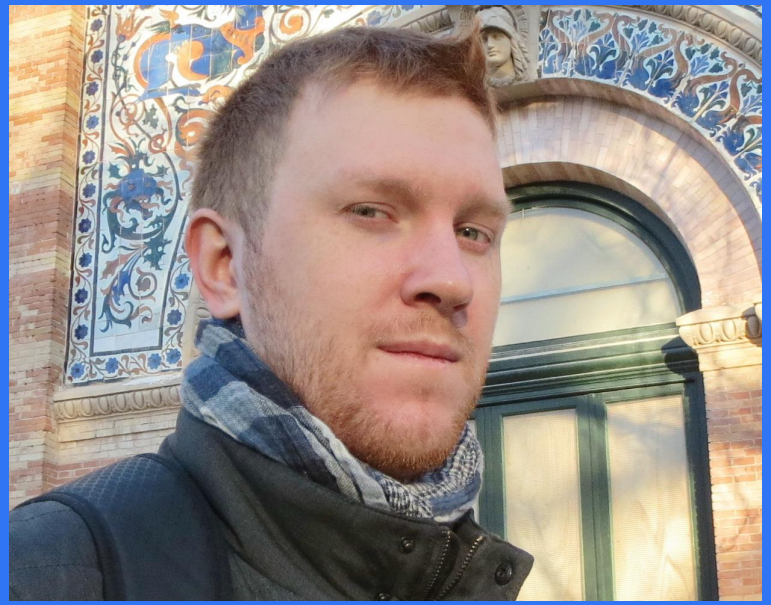
Безопасность web-приложений

Как ломать и не ломаться

skyeng

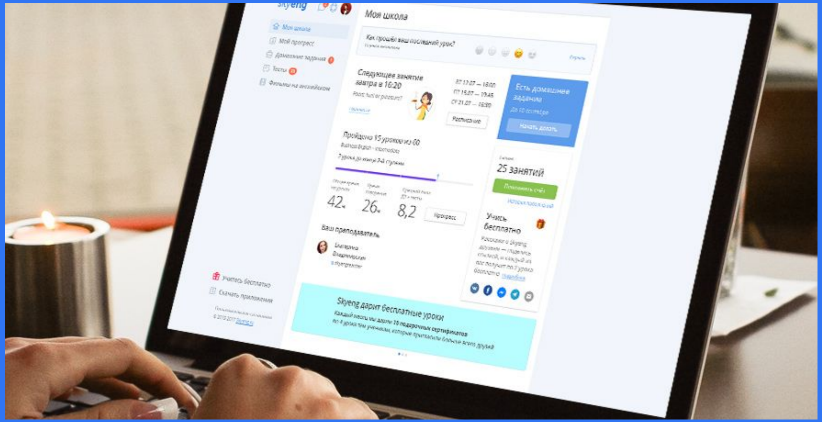


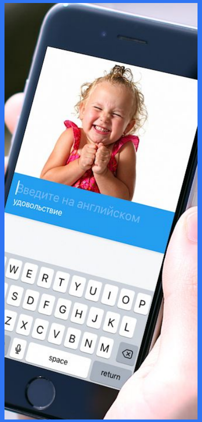
Денис Юрьев

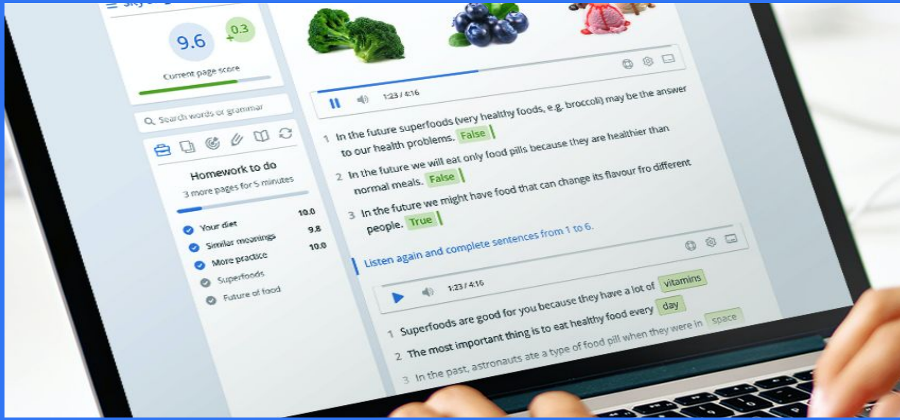
Teamlead @ Skyeng

d.yuriev@skyeng.ru
tg: @vrs_x

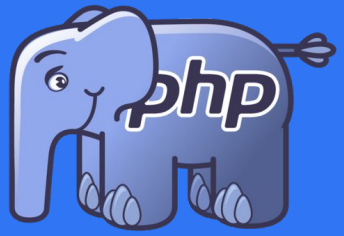
skyeng


Моя школа
Следующее занятие завтра в 10:20
Есть домашнее задание
25 занятий
Ваш преподаватель
Учись бесплатно
Skyeng дарит бесплатные уроки


Введите на английском
удовольствие
space
return


9.6
0.3
Current page score
Search words or grammar
Homework to do
Your diet
Similar meanings
More practice
Superfoods
Future of food
1 In the future superfoods (very healthy foods, e.g. broccoli) may be the answer to our health problems. False
2 In the future we will eat only food pills because they are healthier than normal meals. False
3 In the future we might have food that can change its flavour fro different people. True
Listen again and complete sentences from 1 to 6.
1 Superfoods are good for you because they have a lot of vitamins
2 The most important thing is to eat healthy food every day

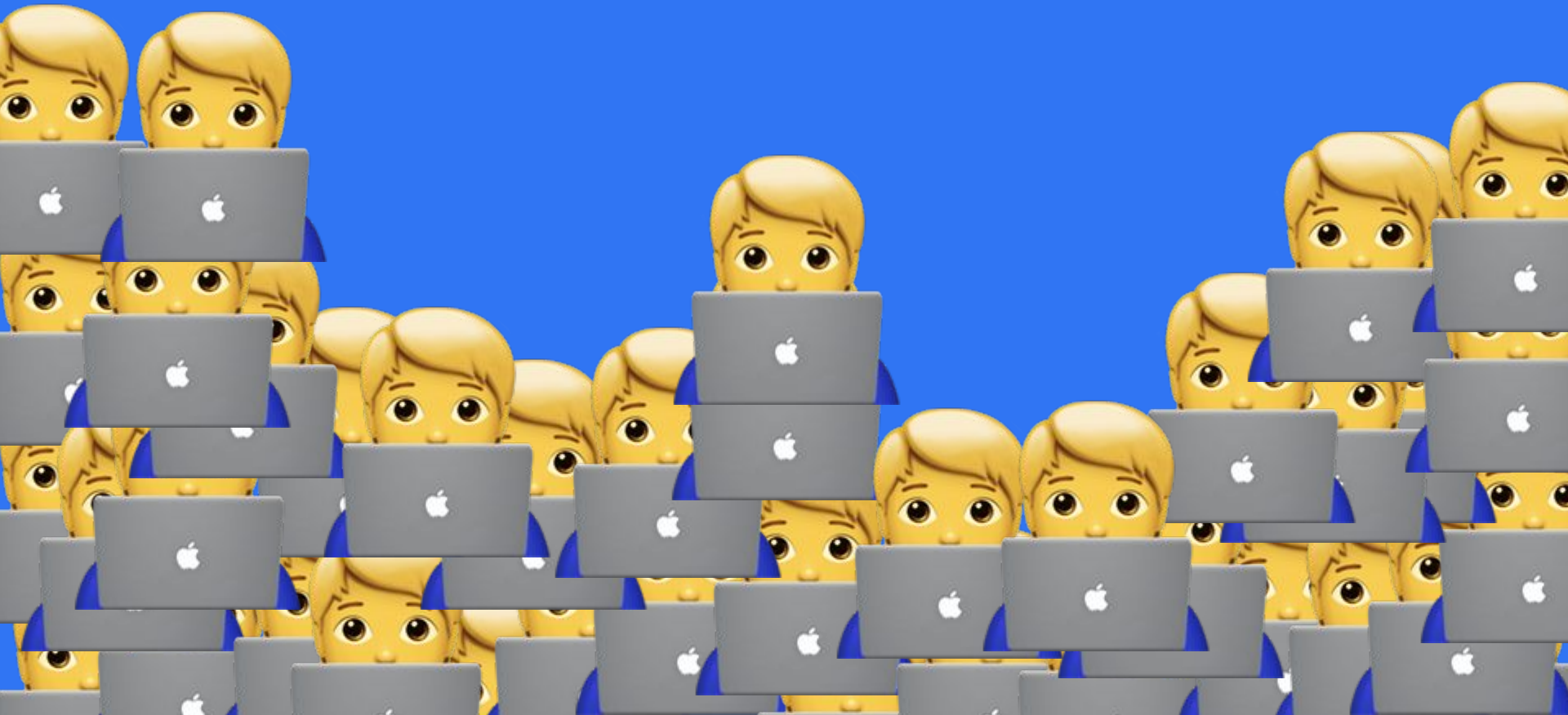
skyeng



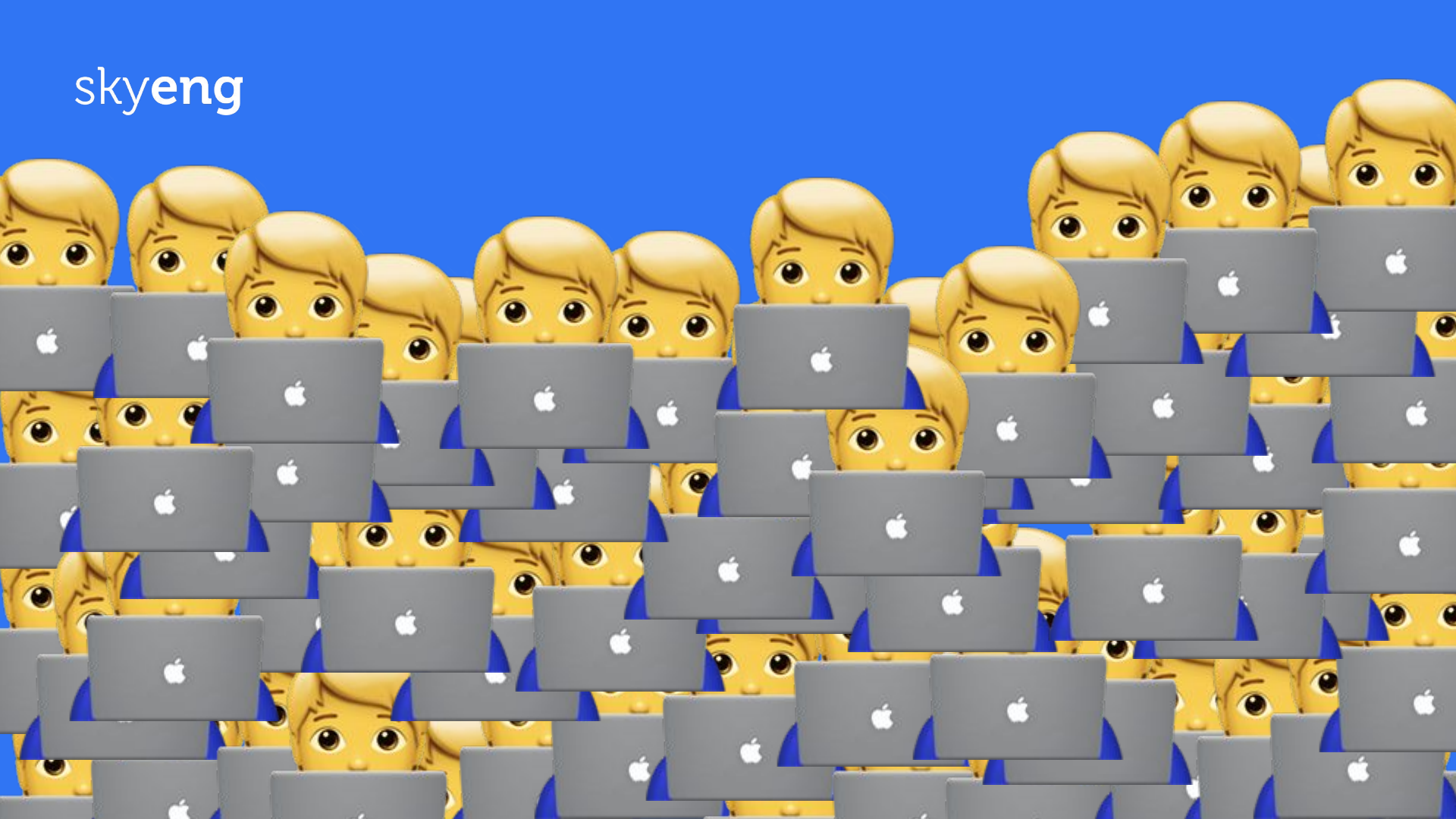
skyeng

skyeng

skyeng



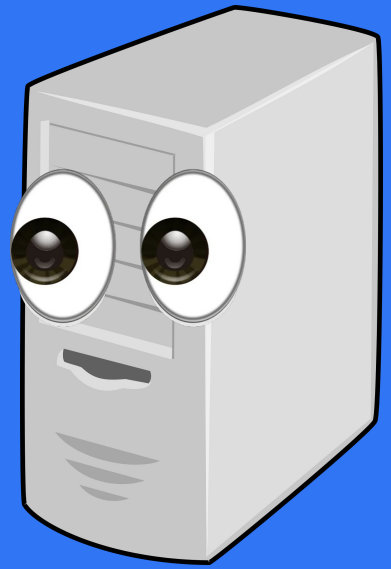
skyeng



Безопасность для разработчика – да/нет/мэйби?

skyeng

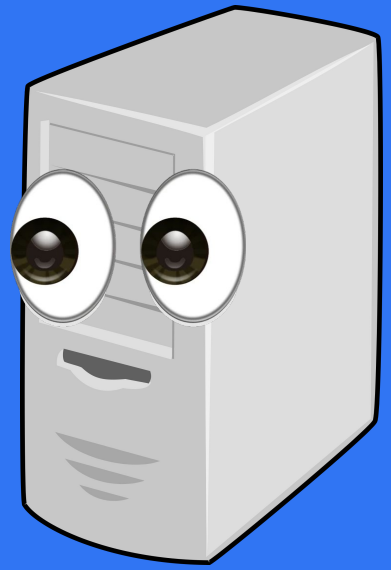
Знакомимся



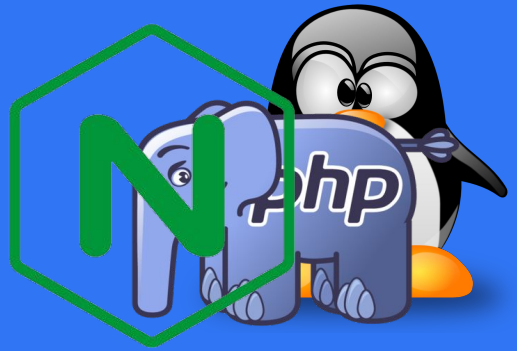
Толик

веб-сервис

Знакомимся



Толик
веб-сервис

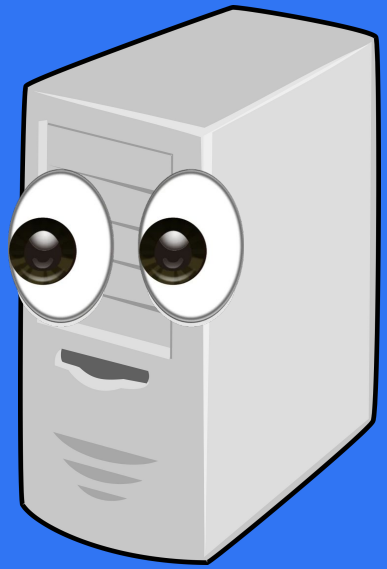


Код, веб-сервер, ОС
окружение

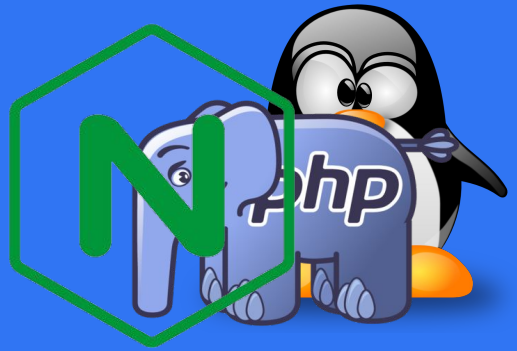
skyeng

Знакомимся

Разработчики Толика
разработчики



Толик
веб-сервис

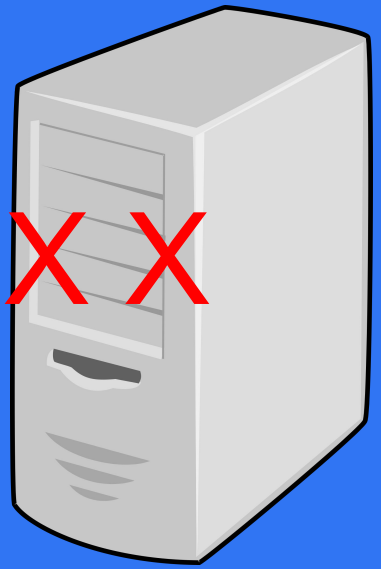


Код, веб-сервер, ОС
окружение

skyeng

Прощаемся?

Разработчики Толика
разработчики



Толик
веб-сервис

Код, веб-сервер, ОС
окружение

skyeng

Что было

skyeng

1

Слив БД

2

Получение чужих данных

3

Редактирование, удаление данных

4

Нагрузка от «левых» сайтов

5

Раскрытие секретных данных

6

Выполнение кода на сервере

Что было

skyeng

1

Слив БД

2

ых

3

Редактирование, удаление данных

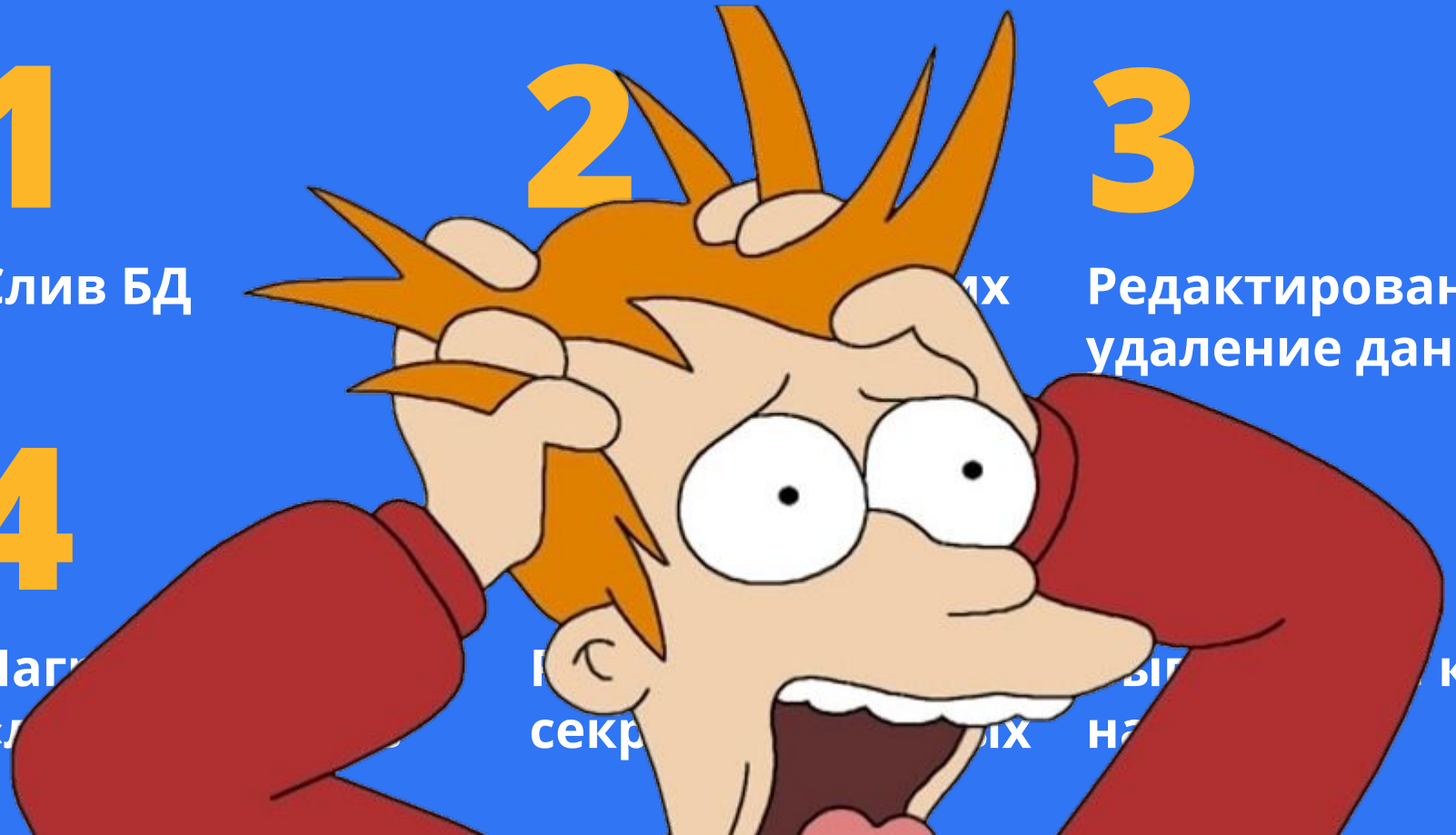
4

Наг

«л

кода

на



Что делать?

skyeng

Менеджер

Что делать?

skyeng

Нанять!

Что делать?

skyeng

Но как?

Что делать?

skyeng

Тогда изучить!

Что делать?

skyeng

Ок

Что делать?

skyeng

И предотвратить!

Что делать?

skyeng

Воу воу,
полегче

Что делать?

skyeng

Что делать?

skyeng

Я ещё вернусь!

Про актуальность

https://owasp.org/

Top 10 Web Application Security Risks

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting XSS
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

Систематизируем

Внешние

Сторонние

Внутренние

skyeng

Внешние

Транспорт, веб-сервер

skyeng

Веб-сервер

когда кода вроде нет, но он есть

```
if ($http_origin ~ <%= ENV['ROOT_DOMAIN'].gsub(".", "\\.") %>$) {
  set $allow_origin "${http_origin}";
}
if ($request_method = OPTIONS) {
  ...
  add_header "Access-Control-Allow-Origin" "${allow_origin}";

  return 200;
}
```

Веб-сервер

когда кода вроде нет, но он есть

```
if ($http_origin ~ <%= ENV['ROOT_DOMAIN'].gsub(".", "\\.") %>$) {
  set $allow_origin "${http_origin}";
}
if ($request_method = OPTIONS) {
  ...
  add_header "Access-Control-Allow-Origin" "${allow_origin}";

  return 200;
}
```

Веб-сервер

когда кода вроде нет, но он есть

```
if ($http_origin ~ <%= ENV['ROOT_DOMAIN'].gsub(".", "\\.") %>$) {
  set $allow_origin "${http_origin}";
}
if ($request_method = OPTIONS) {
  ...
  add_header "Access-Control-Allow-Origin" "${allow_origin}";

  return 200;
}
```

Веб-сервер

когда кода вроде нет, но он есть

```
if ($http_origin ~ <%= ENV['ROOT_DOMAIN'].gsub(".", "\\.") %>$) {
  set $allow_origin "${http_origin}";
}
if ($request_method = OPTIONS) {
  ...
  add_header "Access-Control-Allow-Origin" "${allow_origin}";

  return 200;
}
```

Веб-сервер

когда кода вроде нет, но он есть

```
if ($http_origin ~ <%= ENV['ROOT_DOMAIN'].gsub(".", "\\.") %>$) {
  set $allow_origin "${http_origin}";
}
if ($request_method = OPTIONS) {
  ...
  add_header "Access-Control-Allow-Origin" "${allow_origin}";

  return 200;
}
```

Веб-сервер

когда кода вроде нет, но он есть

```
if ($http_origin ~ \.yoursite\.com$) {
  set $allow_origin "${http_origin}";
}
if ($request_method = OPTIONS) {
  ...
  add_header "Access-Control-Allow-Origin" "${allow_origin}";

  return 200;
}
```

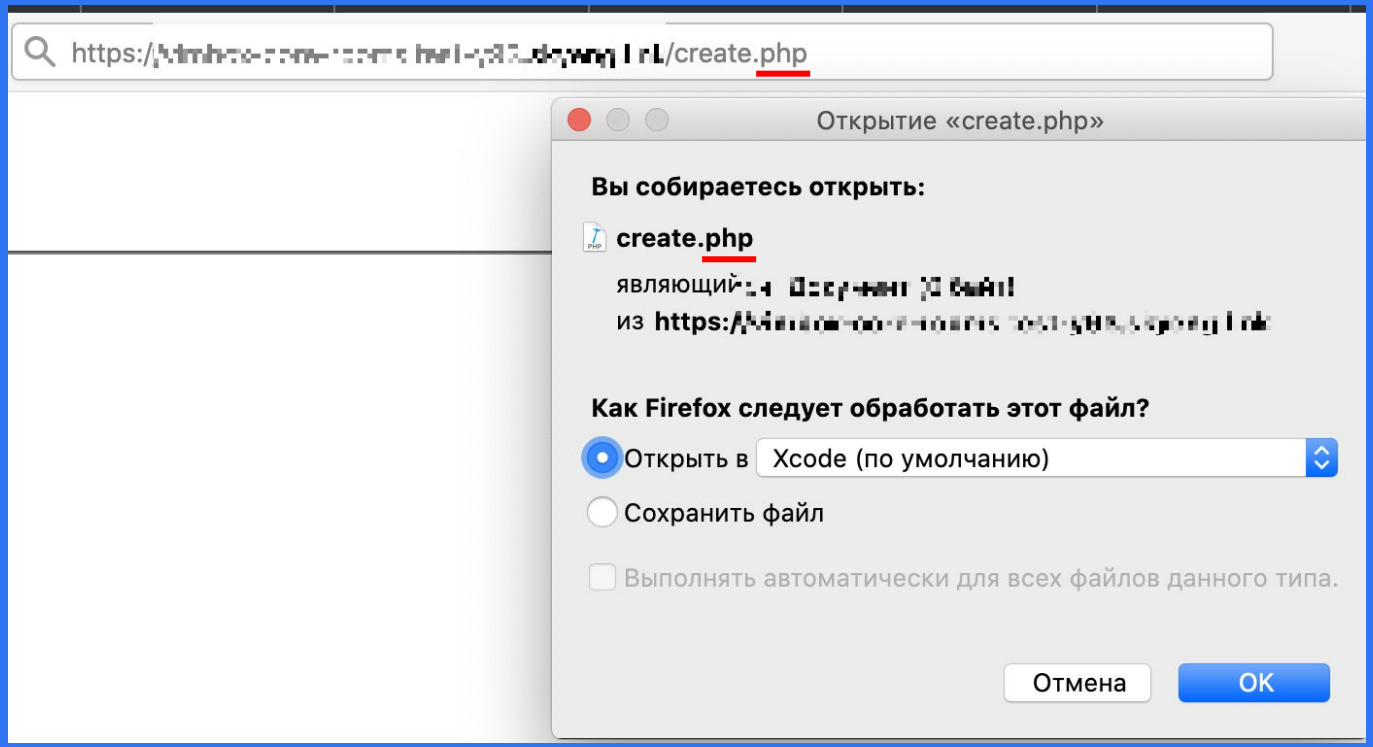
Веб-сервер

когда кода вроде нет, но он есть

```
if ($http_origin ~ .yoursite\.com$) {
  set $allow_origin "${http_origin}";
}
if ($request_method = OPTIONS) {
  ...
  add_header "Access-Control-Allow-Origin" "${allow_origin}";

  return 200;
}
```

Веб-сервер
когда код есть, а его должно не быть



skyeng

Где такое ловить?

Код-ревью

очень сложно читается, разносится копипастой (должно лежать в проекте)

CI

Где такое ловить?

Код-ревью

CI

Проверка быстрая и настроить несложно, но лениво

skyeng

Сторонние

Подключаемые пакеты в приложении, системные модули в ОС

skyeng

Внутри приложения

composer.lock

package.lock

yarn.lock

skyeng

Внутри приложения

composer.lock

npm

package.lock

yarn

yarn.lock

https://github.com/sensiolabs/security-checker

skyeng

Внутри приложения

composer.lock

https://github.com/sensiolabs/security-checker

package.lock

npm audit

yarn.lock

skyeng

Внутри приложения

composer.lock

https://github.com/sensiolabs/security-checker

package.lock

npm audit

yarn.lock

(барабанная дробь)

skyeng

Внутри приложения

composer.lock

https://github.com/sensiolabs/security-checker

package.lock

npm audit

yarn.lock

yarn audit

skyeng

Что делаем?

1

Сканируем

skyeng

Что делаем?

1

Сканируем

2

Добавляем в CI

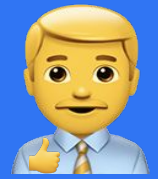
skyeng

Что делаем?

1
Сканируем

2
Добавляем в CI

3
Оцениваем на берегу



skyeng

Снаружи приложения

ОС

Модули

ПО юзеров

skyeng

Снаружи приложения

denis-19 8 марта 2020 в 09:50

Исследователи обнаружили уязвимости в процессорах AMD на базе микроархитектур Bulldozer, Piledriver, Steamroller и Zen

Информационная безопасность, Настольные компьютеры, Процессоры

Что делаем?

1

Читаем новости

skyeng

Что делаем?

1
Читаем новости

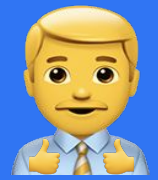
2
Сообщаем коллегам

skyeng

Что делаем?

1
Читаем новости

2
Сообщаем коллегам

3

Вводим процесс обновления

skyeng

Внутренние

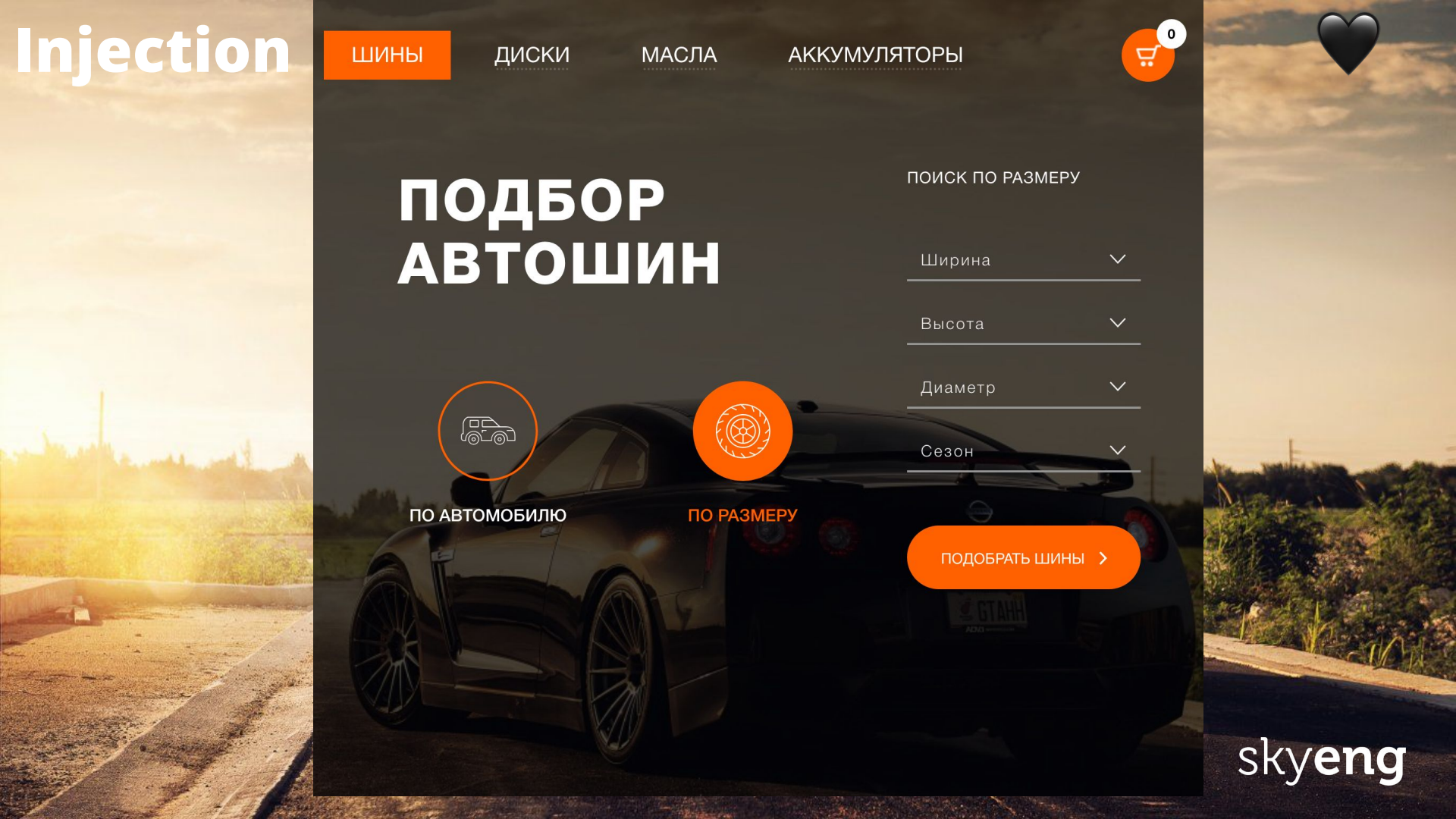
Код приложения

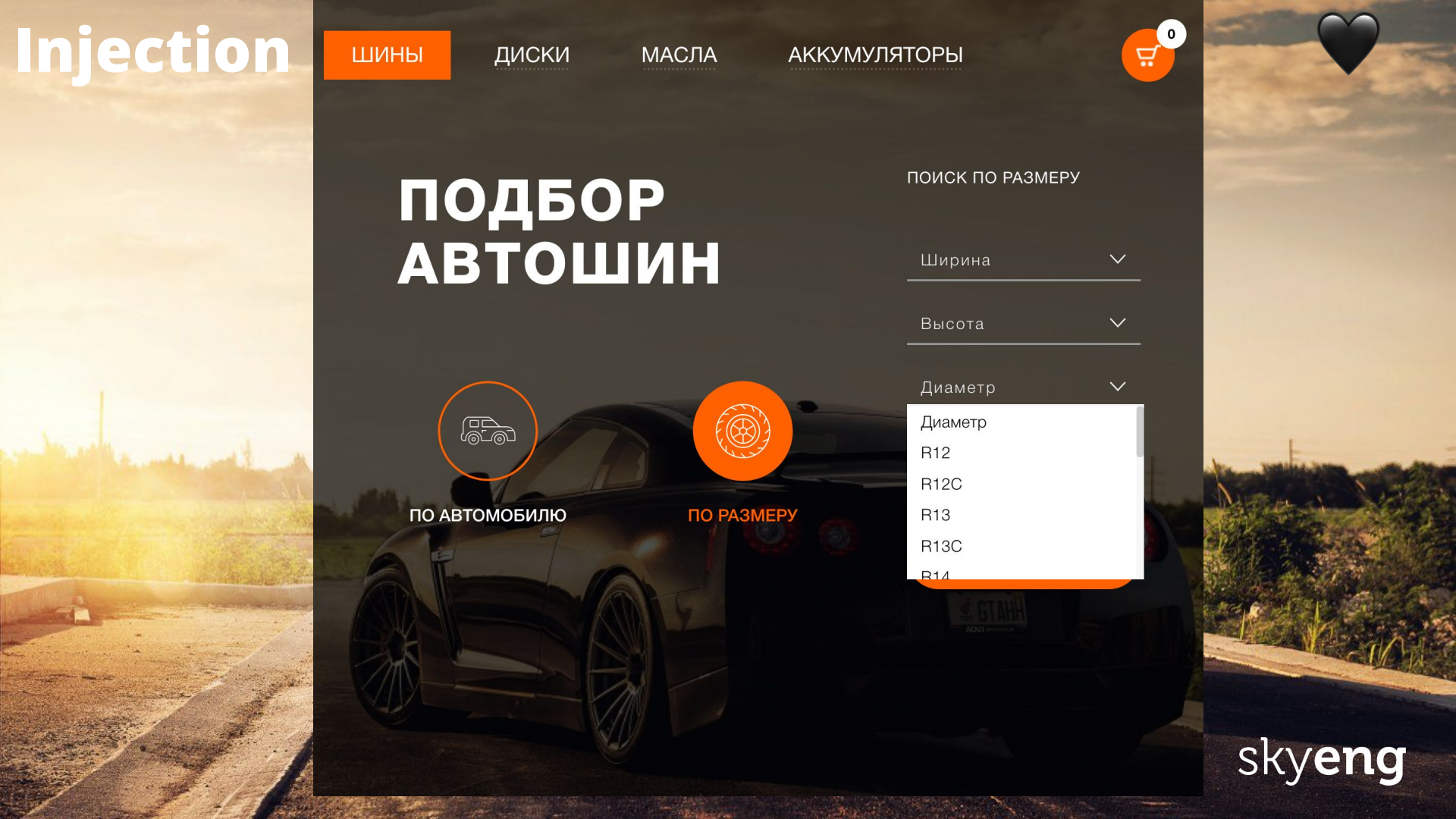
skyeng

Что Здесь?

Top 10 Web Application Security Risks

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting XSS
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring


Injection
ШИНЫ
ДИСКИ
МАСЛА
АККУМУЛЯТОРЫ
0
ПОДБОР АВТОШИН
ПОИСК ПО РАЗМЕРУ
Ширина
Высота
Диаметр
Сезон
ПО АВТОМОБИЛЮ
ПО РАЗМЕРУ
ПОДОБРАТЬ ШИНЫ
skyeng


Injection
ШИНЫ
ДИСКИ
МАСЛА
АККУМУЛЯТОРЫ
0
ПОДБОР АВТОШИН
ПОИСК ПО РАЗМЕРУ
Ширина
Высота
Диаметр
Диаметр
R12
R12C
R13
R13C
R14
ПО АВТОМОБИЛЮ
ПО РАЗМЕРУ
skyeng

https://.../?FILTER[DIAMETR]=R12C

ШИНЫ ДЛЯ ЛЕГКОВЫХ АВТОМОБИЛЕЙ

Главная / Автошины

Легковые | Грузовые | Мото

По размеру

По автомобилю

Ширина: Ширина

Высота: Высота

Диаметр: R12C

сбросить

Показать: 24

Сортировка: по популярности

Injection

https://.../?FILTER[DIAMETR]=R12C 123

ШИНЫ ДЛЯ ЛЕГКОВЫХ АВТОМОБИЛЕЙ

Главная / Автошины

Легковые | Грузовые | Мото

По размеру

По автомобилю

Ширина: Ширина

Высота: Высота

Диаметр: R12C

123

Диаметр
R12
R12C
R13
R13C
R14
R14C

Показать: 24

Сортировка: по популярности

Injection

https://.../?FILTER[DIAMETR]=R12C Хороший сайт</sp

ШИНЫ ДЛЯ ЛЕГКОВЫХ АВТОМОБИЛЕЙ

Главная / Автошины

Легковые | Грузовые | Мото

По размеру

По автомобилю

Ширина | Высота | Диаметр

Ширина | Высота | R12C

Хороший сайт!

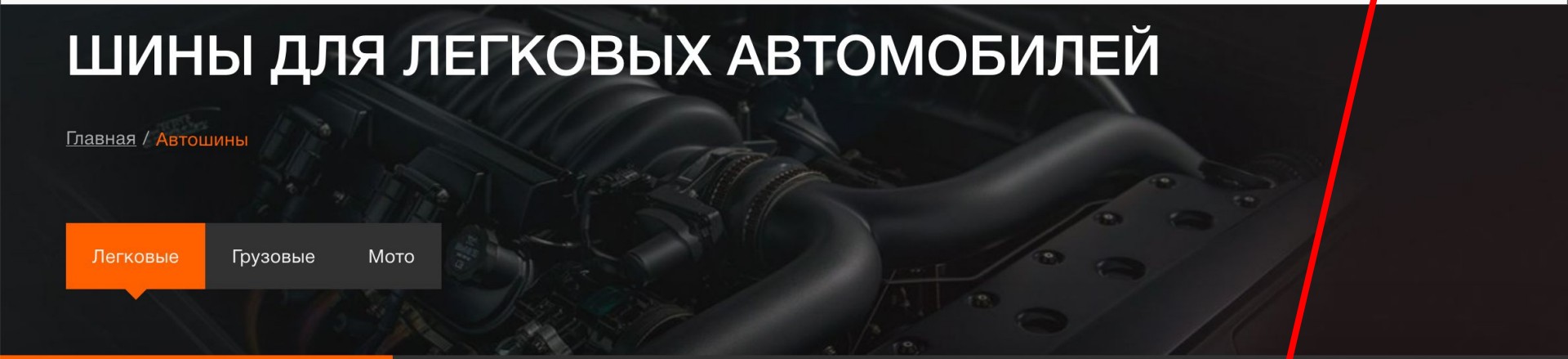
Диаметр
R12
R12C
R13
R13C
R14
R14C

Показать: 24

Сортировка: по популярности

Injection

https://.../?FILTER[DIAMETR]=R12C Хороший сайт</sp



По размеру

По автомобилю

Ширина

Ширина

Высота

Высота

Диаметр

R12C

Хороший сайт!

Диаметр
R12
R12C
R13
R13C
R14
R14C

Показать: 24

Сортировка: по популярности

XSS

```php
<?php
    $uid = $_REQUEST['uid'];
?>
<!DOCTYPE html>
<html>
<head>
```

...

```
function init_like() {
    VK.Widgets.Like("vk_like", {type: "button"}, <?= $uid ?>);
    VK.Observer.subscribe("widgets.like.liked", function f() {
        top.postMessage({action: "stop", status: true}, host_name);
    });

    $(window).on('mousemove', function (e) {
```

XSS

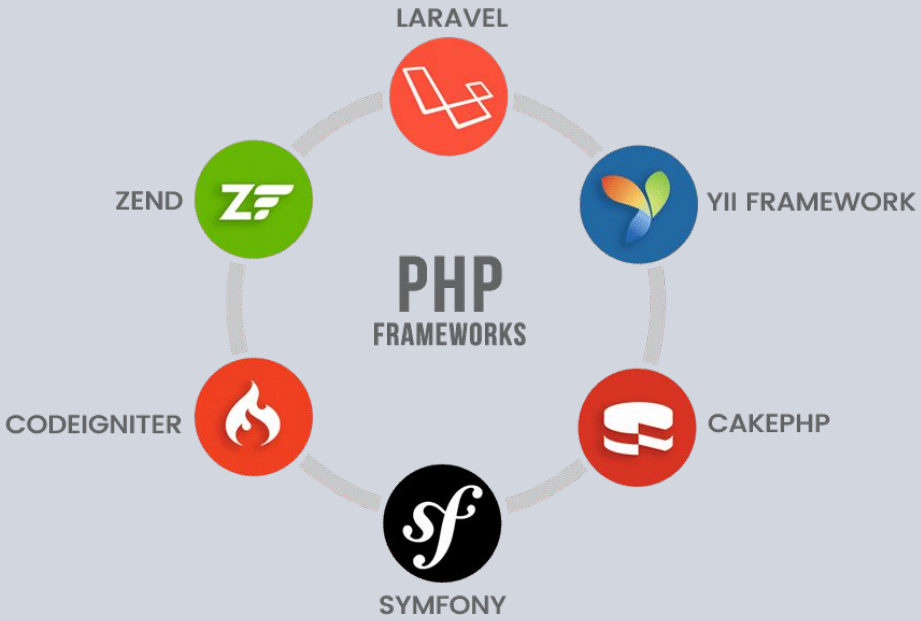
```php
<?php
    $uid = $_REQUEST['uid'];
?>
<!DOCTYPE html>
<html>
<head>
```

. . .

```
function init_like() {
    VK.Widgets.Like("vk_like", {type: "button"}, <?= $uid ?>);
    VK.Observer.subscribe("widgets.like.liked", function f() {
        top.postMessage({action: "stop", status: true}, host_name);
    });

    $(window).on('mousemove', function (e) {
```

Особое упоминание



skyeng

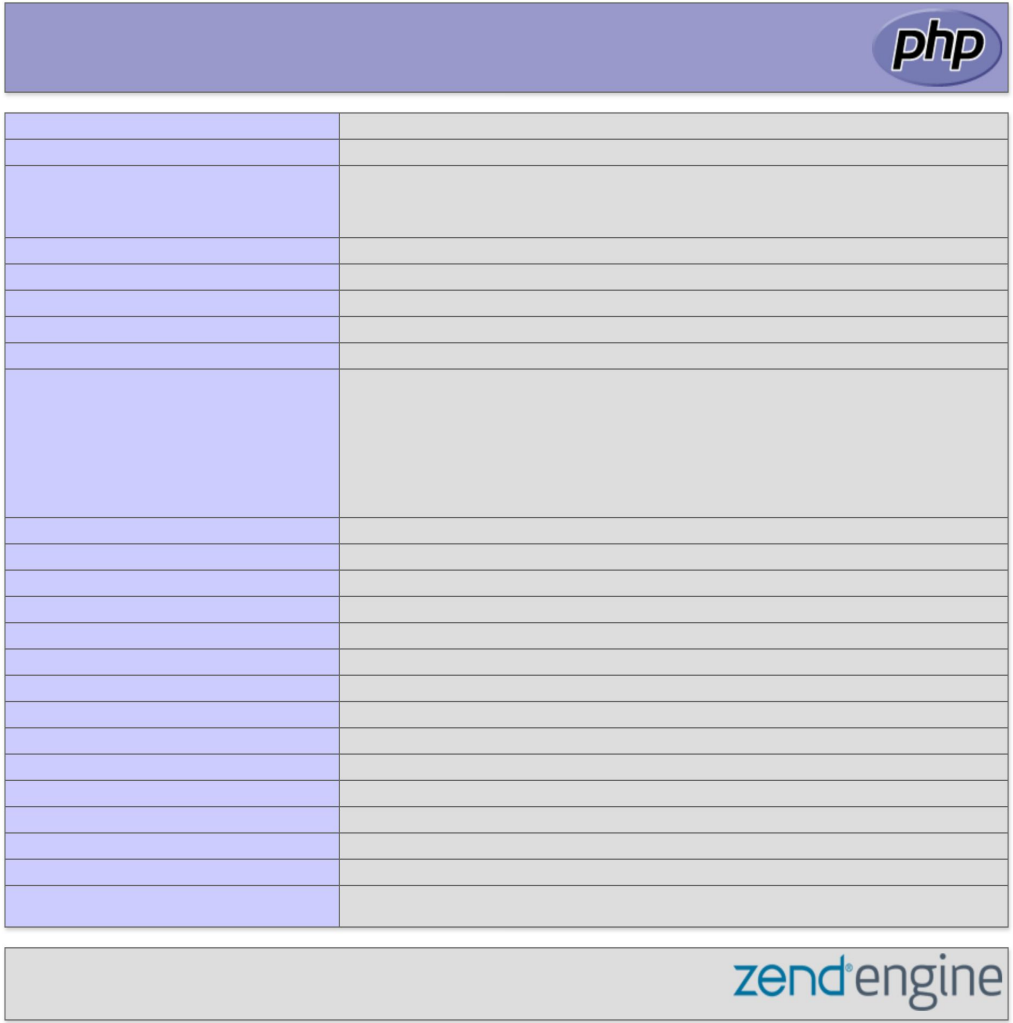
Пример ошибки с контролем доступа

```php
/**
 * Скачивание договора
 *
 * @param DownloadOfferRequest $request
 * @param $offerId
 * @return \Illuminate\Http\Response
 */
public function downloadOffer(DownloadOfferRequest $request, $offerId)
{
    /**
     * @var $offer Offer
     */
    $offer = Offer::find($offerId);
    return $offer->toPdf()->download('Оферта№' . $offer->id . '.pdf');
}
```

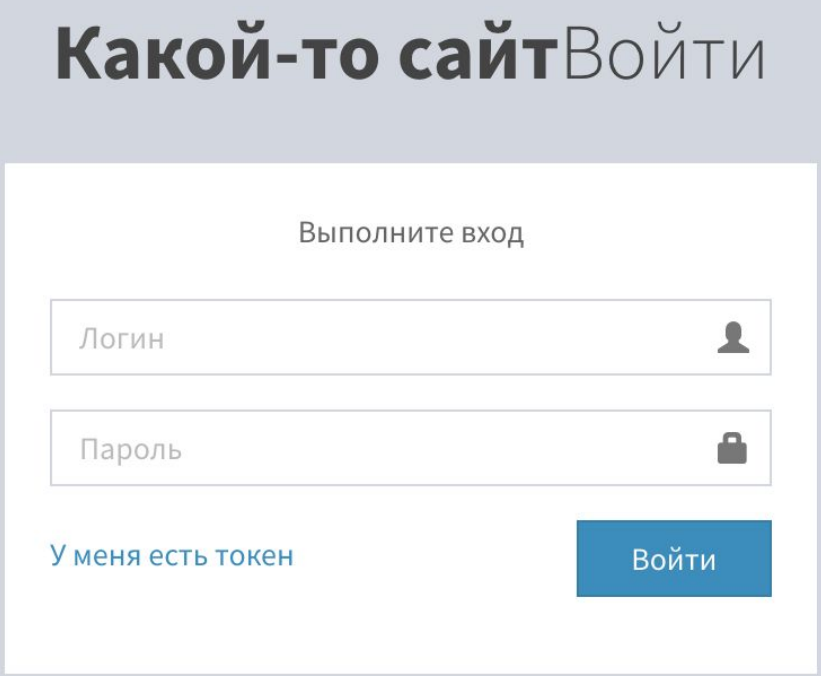
Пример ошибки с контролем доступа

```php
/**
 * Скачивание договора
 *
 * @param DownloadOfferRequest $request
 * @param $offerId
 * @return \Illuminate\Http\Response
 */
public function downloadOffer(DownloadOfferRequest $request, $offerId)
{
    /**
     * @var $offer Offer
     */
    $offer = Offer::find($offerId);
    return $offer->toPdf()->download('Оферта№' . $offer->id . '.pdf');
}
```

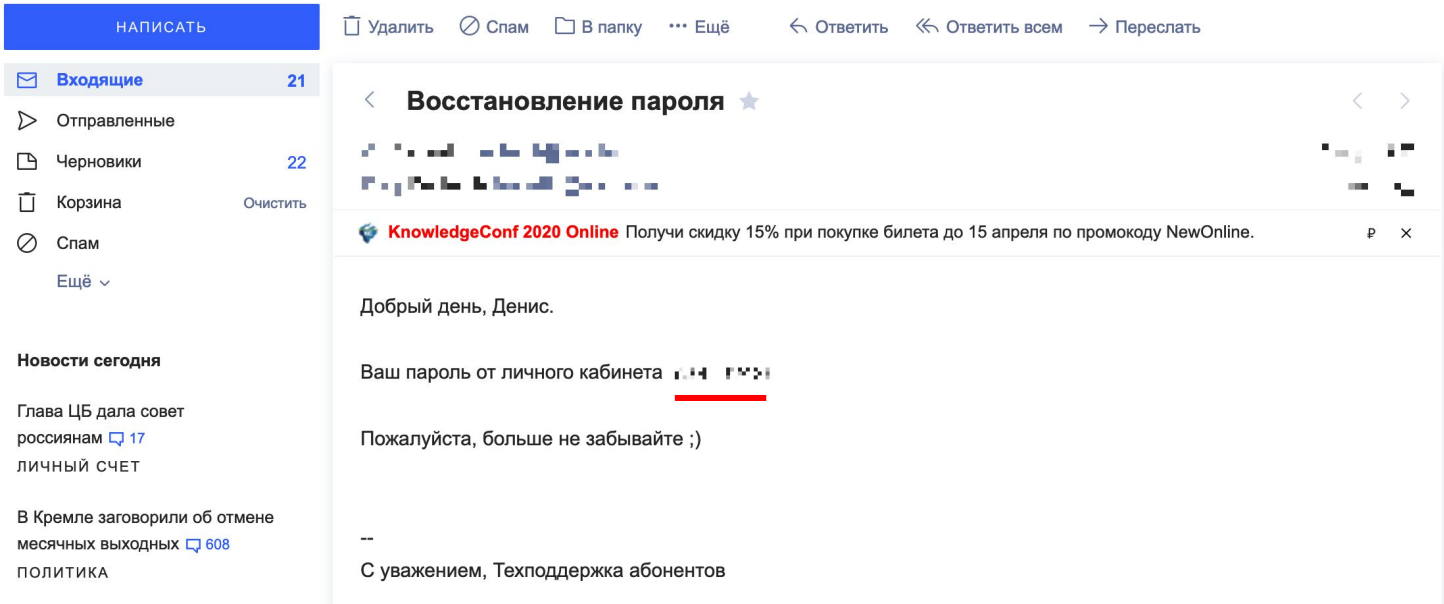
Дебаг



Особое упоминание



Почетное упоминание



Бонусное упоминание

GET /logout
GET /update?id=1&name=2

Что делаем?

1

Фильтрация, Prepared statements

2

Whitelist > blacklist

3

Экранируем данные из БД

4

Проверяем доступы

5

Используем токены

6

GET – чтение, POST – изменения

Что делаем?

Extra 

Продумываем логирование подозрительных действий заранее

skyeng

Итого

Внешние

Сторонние

Внутренние

skyeng

Итого

Версионируются и обновляются

Внешние

Сторонние

Внутренние

skyeng

Итого

Версионируются и обновляются

Внешние

Сторонние

Внутренние

Проверяются, мониторятся, обрабатываются

skyeng

Итого

Разработчики Толика

разработчики

skyeng

Итого

Разработчики Толика
разработчики

Разработчики Толика
крутые разработчики

skyeng

Итого

Разработчики ****

разработчики

Разработчики ****

крутые разработчики

skyeng

Наши советы

Профдеформируйся!
owasp, хабр, хакер

Просвещай!

Автоматизируй

skyeng

Наши советы

Профдеформируйся!

Просвещай!
микро-доклады, новости

Автоматизируй

skyeng

Наши советы

Профдеформируйся!

Просвещай!

Автоматизируй
CI, Burp, security-checker

skyeng

Спасибо за внимание

Вопросы?

или tg:@vrs_x