1.Создать **политику** для **дальнейшего** использования при **edit/update/destroy** (т. е. - **в независимости от** **Front-показа** иконок **невозможность edit/update/destroy чужих** сообщений):

**app\Policies\ApimessagePolicy.php**

<?php

namespace App\Policies;

use App\Models\ {User, **Apimessage**};

class **Apimessage**Policy extends Policy

{

/\*\*

\* Determine whether the user can manage the comment.

\*

\* @param \App\Models\User $user

\* @param \App\Models\Apimessage $message

\* @return mixed

\*/

public function manage(User $user, **Apimessage $message**)

{

return $user->id === **$message**->user\_id;

}

}

**app\Providers\AuthServiceProvider.php**

…

**use App\Models\Apimessage;**

**use App\Policies\ApimessagePolicy;**

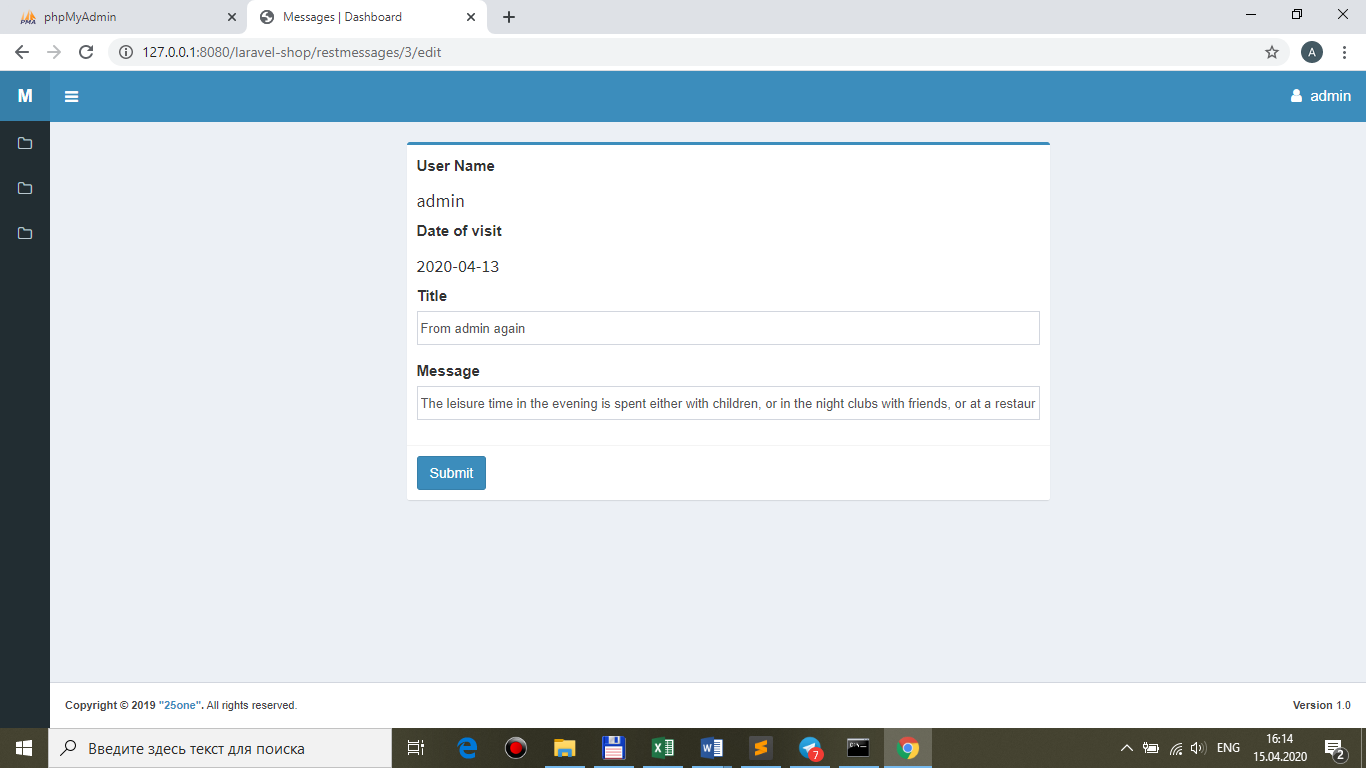
protected $policies = [

// 'App\Model' => 'App\Policies\ModelPolicy',

**Apimessage::class => ApimessagePolicy::class,**

];

2.Реализовать **RESTful-edit** for **messages**:



**routes\web.php**

Route::prefix('')->namespace('Front')->group(function () {

...

Route::middleware('auth')->group(function () { //!!!ONLY AUTH-USERS

...

**Route::resource('restmessages', 'MessageController');**

});

**resouces\views\front\messages\restmessages\ → edit.blade.php, create.blade.php, template.blade.php + components (from views\back\messages laravel-message)**

**resouces\views\front\messages\brick-standard.blade.php**

@if($message->user\_id == auth()->user()->id || auth()->user()->role == 'admin')

<td class="center widthbutton"><a class="btn btn-danger listbuttonremove" href="#"><i class="fa fa-trash-o" aria-hidden="true"></i></a></td>

<td class="col-md-6 col-sm-6 col-xs-6 center widthbutton"><a class="btn btn-primary listbuttonupdate" **href="{{route('restmessages.edit', $message->id)}}"**><i class="fa fa-edit" aria-hidden="true"></i></a></td>

…

**resouces\views\front\messages\restmessages\edit.blade.php**

@extends('front.**messages.restmessages**.template')

@section('form-open')

<form method="post" action="{{ **route('restmessages.update', $message->id)** }}">

{{ csrf\_field() }}

{{ method\_field('PUT') }}

@endsection

**resouces\views\front\messages\restmessages\template.blade.php**

@extends('**front.messages**.layout')

…

@if (session('message-ok'))

@component('**front.messages**.components.alert')

@slot('type')

success

@endslot

{!! session('message-ok') !!}

@endcomponent

@endif

…

**MessageController.php**

use App\ {

Http\Controllers\Controller,

Repositories\MessageRepository**,**

**Models\Apimessage**

};

...

/\*\*

\* Show the form for editing the specified resource.

\*

\* @param \App\Models\Apimessage $message

\* @return \Illuminate\Http\Response

\*/

public function **edit(Apimessage $restmessage)**

{

**$this->authorize('manage', $restmessage);**

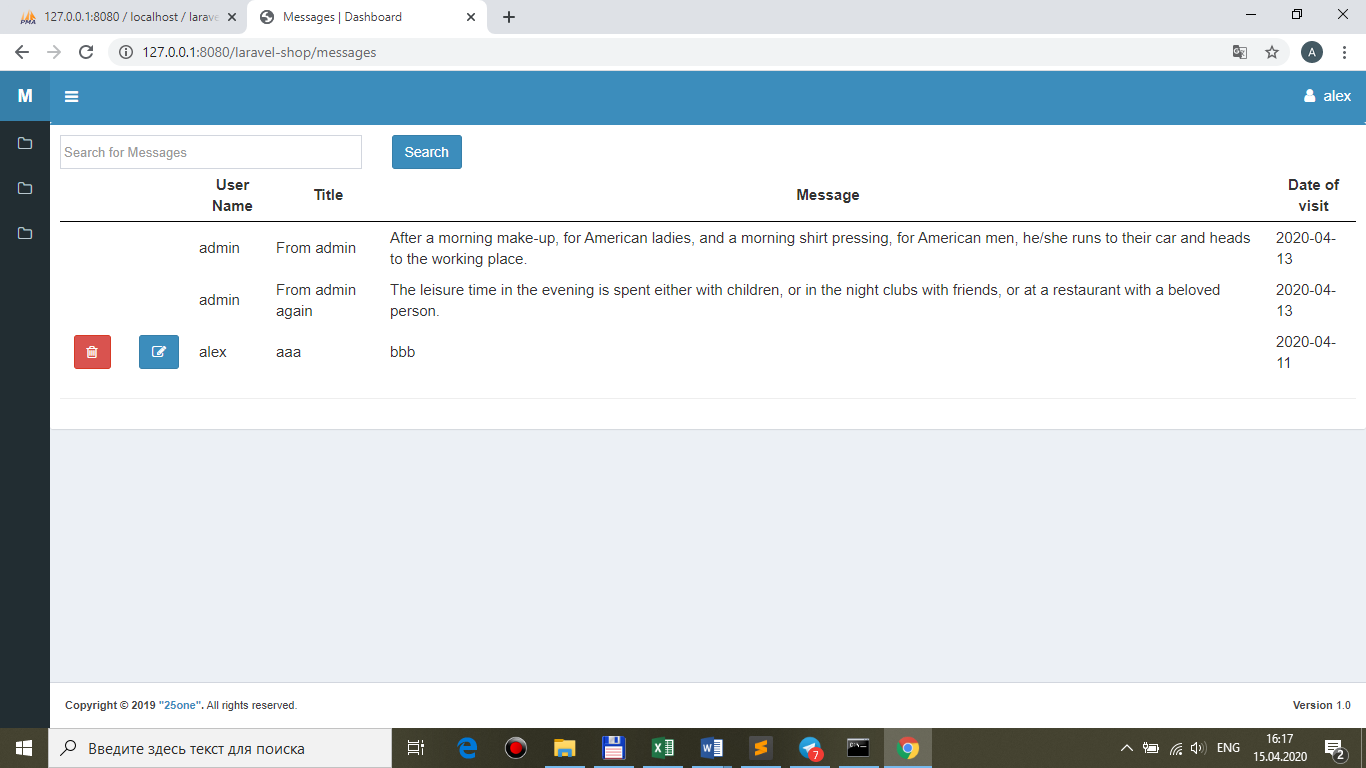
**$message = $restmessage; //because view edit use $message**

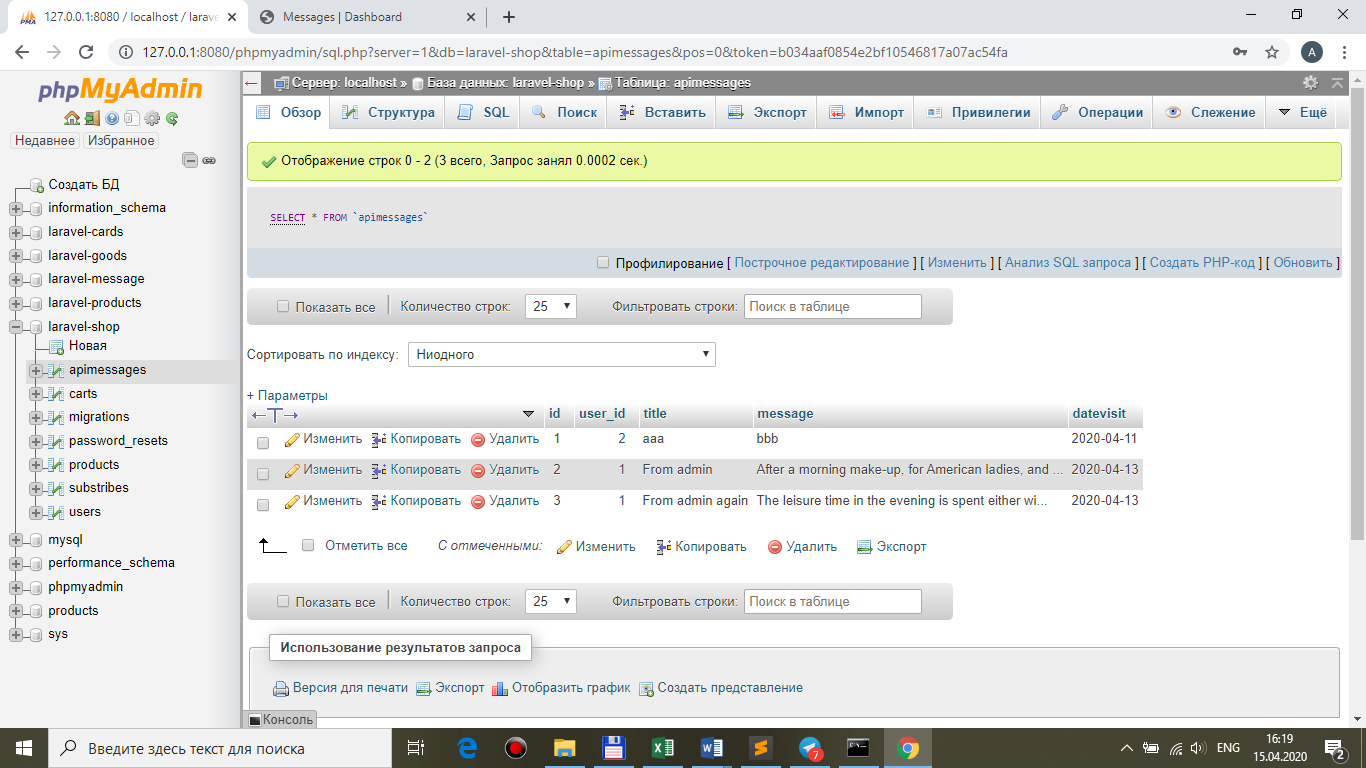
return view(**'front.messages.restmessages.edit', compact('message')**); //because view edit use $message

}

3.Проверить работу **Policy** (**4 — id message of serg, not alex**):

…у **alex** есть один message с **id=1**





…**попытка подмены** цифры (**id=2 - admin**) через **url**

