

My Phonebook

Xây dựng ứng dụng web **My Phonebook** hỗ trợ các chức năng sau:

- Chứng thực người dùng (đăng ký, đăng nhập)
- Sau khi đăng nhập, người dùng có thể xem, thêm, sửa, xóa các contact của mình. Thông tin mỗi contact gồm có tên (name), số điện thoại (phone number) và ghi chú (notes)

Hiệu chỉnh một contact:

1. Vào thư mục *views/contacts*, tạo tập tin *edit.php*. Sao chép nội dung *contacts_edit.txt* đã cho vào *edit.php*
2. Thêm định nghĩa các route sau vào tập tin *index.php*:

```
Router::get('/contacts/edit/(:num)', '\App\Controllers\ContactsController@edit');
Router::post('/contacts/(:num)', '\App\Controllers\ContactsController@update');
```

3. Thêm định nghĩa các hàm sau vào *app/Controllers/ContactsController.php*:

```
public function edit($contactId)
{
    $contact = Contact::find($contactId);
    if (! $contact || ($contact->user_id !== Guard::user()->id)) {
        $this->notFound();
    }

    $formValues = session_get_once('form');
    $data = [
        'errors' => session_get_once('errors'),
        'contact' => (count($formValues) > 0) ?
            array_merge($formValues, ['id' => $contact->id]) :
            $contact->toArray()
    ];
    echo $this->view->render('contacts/edit', $data);
}

public function update($contactId)
{
    $contact = Contact::find($contactId);
    if (! $contact || ($contact->user_id !== Guard::user()->id)) {
        $this->notFound();
    }

    $data = $this->getContactData();
    if ($contact->validate($data)) {
        $contact->fill($data)->save();
    }
}
```

```

        redirect('/');
    }

    $this->saveFormValues();
    redirect('/contacts/edit/'.$contactId, ['errors' => $contact->getErrors()]);
}

```

4. Thêm nút "Edit" vào trang home (*contacts/home.php*):

```

...
            <td><a href="/contacts/edit/?=$this->e($contact->id)?>"
                class="btn btn-xs btn-warning">
                <i alt="Edit" class="fa fa-pencil"> Edit</i></a></td>
            </tr>
        <?php endforeach ?>
    </tbody>
</table>
...

```

5. Kiểm tra lại chức năng hiệu chỉnh contact vừa cài đặt

Xóa một contact:

1. Thêm định nghĩa route sau vào tập tin *index.php*:

```

Router::post('/contacts/delete/(:num)',
    '\App\Controllers\ContactsController@delete');

```

2. Thêm định nghĩa hàm delete vào *app/Controllers/ContactsController.php*:

```

public function delete($contactId)
{
    $contact = Contact::find($contactId);
    if (! $contact || ($contact->user_id !== Guard::user()->id)) {
        $this->notFound();
    }

    $contact->delete();
    redirect('/');
}

```

3. Thêm nút "Delete" và hộp thoại xác nhận vào trang home (*contacts/home.php*):

```

<td><a href="/contacts/edit/?=$this->e($contact->id)?>"
    class="btn btn-xs btn-warning">
    <i alt="Edit" class="fa fa-pencil"> Edit</i></a>
    <form class="delete" action="/contacts/delete/?=$this->e($contact->id)?>"
        method="POST" style="display: inline;">
        <button type="submit" class="btn btn-xs btn-danger"
            name="delete-contact">
            <i alt="Delete" class="fa fa-trash"> Delete</i>
        </button>
    </form>

```

```

</td>

...

<div id="delete-confirm" class="modal fade" role="dialog">
  <div class="modal-dialog">
    <div class="modal-content">
      <div class="modal-header">
        <button type="button" class="close"
          data-dismiss="modal">&times;</button>
        <h4 class="modal-title">Confirmation</h4>
      </div>
      <div class="modal-body">Do you want to delete this contact?</div>
      <div class="modal-footer">
        <button type="button" data-dismiss="modal"
          class="btn btn-danger" id="delete">Delete</button>
        <button type="button" data-dismiss="modal"
          class="btn btn-default">Cancel</button>
      </div>
    </div>
  </div>
</div>
<?php $this->stop() ?>

...

<script>
  $(document).ready(function(){
    ...
    $('button[name="delete-contact"]').on('click', function(e){
      var $form=$(this).closest('form');
      e.preventDefault();
      $('#delete-confirm').modal({ backdrop: 'static', keyboard: false })
        .one('click', '#delete', function() {
          $form.trigger('submit');
        });
    });
  });
</script>

```

4. Kiểm tra lại chức năng xóa contact vừa cài đặt

Bài tập:

1. Hiển thị thông báo dạng alert khi người dùng thực hiện tác vụ thành công trên trang home (tác vụ thêm, sửa, xóa contact thành công) và trên trang đăng nhập (khi người dùng đăng ký thành công)
2. Thêm khả năng ngăn ngừa tấn công CSRF (Cross-Site Request Forgery) bằng phương pháp chèn thêm token ẩn vào mỗi form trong ứng dụng