Lomakedata tietokantaan ja CSRF-suojaus

29.01 Lisäyslomake

Luodaan oheinen HTML-lomake datan tallentamiseksi tietokantaan.

Luodaan rivillä 1 näkyvä uusi reitti `routes/web.php`-tiedostoon lomakkeen näyttämiseksi. Tärkeää on että rivin 1 reitti tulee ennen rivillä 3 näkyvää jo aiemmin lisättyä reittiä, jotta se tulee huomioiduksi

```
1 Route::get('/customers/create', 'CustomerController@create');
2 ...
3 Route::get('/customers/{id}', 'CustomerController@show');
```

Lisätään `CustomerController`-kontrolleriin `create()`-metodi lomakkeen näyttämiseksi

```
1 public function create() {
2    return view('customers/create');
3 }
```

ja lisätään HTML-lomakkeen sisältämä varsinainen näkymätiedosto `resources/views/customer/create.blade.php`. Huomioi lomakkeesta seuraavat asiat

- lähetysmetodi on `POST` ja action-määrite `../customers`. Koska lomake on saatavilla reitillä /customers/create, niin em. viittaukset tarkoittavat että lomakkeelta lähetettävä data käsitellään reittimäärityksellä `Route::post('/customers', ...`
- Laravel vaatii lomakkeissa käytettäväksi CSRF-tokenia `{{ csrf_field() }}`, jonka käyttö estää Cross-site scripting -uhat ja parantaa näin merkittävästi sovelluksesi tietoturvaa.

- Huomaa lisäksi, että lomakkee kahden syöttökentän name-määritteiden arvot (name ja birth_date) vastaavat tietokannan kenttien nimiä.
- Syntymäpäiväkenttään on asetettu valmiiksi oikeamuotoinen päivämääräarvo testaamisen helpottamiseksi

resources/views/customer/create.blade.php

```
<!DOCTYPE html>
<html>

  <head>
    <title>Add Customer</title>
  </head>

  <body>
    <h1>Add Customer</h1>

    <form method="POST" action="../customers">

      {{ csrf_field() }}

      <div>
        <input type="text" name="name" placeholder="Customer
      </div>

      <div>
        <input type="text" name="birth_date" value="1999-09-0
      </div>

       <div>
         <button type="submit">Save</button>
       </div>

     </form>

  </body>

</html>
```

Testaa lopuksi reitin, kontrollerin ja näkymän toiminta osoitteessa http://192.168.1.126/~testi/projekti01/public/customers/create

Tutkimalla selaimeen tulostuneen lomakkeen lähdekoodia (CTRL+U) huomaat CSRF-tokenin tuottaneen lomakkeeseen koodin:

```
<input type="hidden" name="_token" value="4avLrMO9jjv6LK1lWJe
```

29.02 Lomakedatan tallentaminen tietokantaan

Luodaan uusi reitti `routes/web.php`-tiedostoon lomakkeen tietojen tallentamiseksi. Huomaa nyt reitissäkin lomakkeeseen määritelty post-metodi.

```
...
Route::post('/customers', 'CustomerController@store');
```

Lisätään `CustomerController`-kontrolleriin `store()`-metodi lomakedatan tallentamiseksi. Ensimäisessä versiossa vain tulostetaan lomakkeelta lähetetty data selaimeen JSON-muodossa. Testaa myös ohjelmakoodiin kommentoitujen rivien toiminta.

```
  public function store() {
    return request()->all();
        // return request('name');
        // return request('birth_date');
  }
```

Testaa toiminta lomakkeella. Lomakkeen tietojen "tallennuksen" seurauksena selaimen osoiterivillä näkyy URL http://192.168.1.126/~testi/projekti01/public/customers ja tulostus näyttää JSON-mutoiselta esim.

```
{
"_token": "4avLrMO9jjv6LK1lWJeLnbfXwwqmmx9MjA2kCwhX",
"name": "Vainio Elo",
"birth_date": "1999-09-09"
}
```

Varsinainen tallentaminen tietokantaan voidaan tehdä nyt kirjoittamalla `store()`-metodi oheiseen muotoon, jossa käytetään aiemmin tinkerillä esiteltyä menetelmää datan tallentamiseksi. Onnistuneen tallentamisen jälkeen käyttäjä ohjataan `redirect()`-metodilla näkemään muuttunut asiakaslista..
Kommentoituna tiiviimpi tapa tallentaa `create()`-metodilla, jonka toimiminen

vaatii aiemmassa luvussa esitetyn `mass assignment` -asettamisen sallituiksi kentille `name` ja `birth_date`. Kokeile myös sitä.

```
  public function store() {

    $customer = new Customer();

    $customer->name = request('name');
    $customer->birth_date = request('birth_date');

    $customer->save();

    /*
    Customer::create([
      'name' => request('name'),
      'birth_date' => request('birth_date')
    ]);
    */

    return redirect('/customers');
}
```