

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 lomakkeen 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

```
1  <!DOCTYPE html>
2  <html>
3
4    <head>
5      <title>Add Customer</title>
6    </head>
7
8    <body>
9      <h1>Add Customer</h1>
10
11     <form method="POST" action=" ../customers">
12
13       {{ csrf_field() }}
14
15       <div>
16         <input type="text" name="name" placeholder="Customer Name">
17       </div>
18
19       <div>
20         <input type="text" name="birth_date" value="1999-09-09">
21       </div>
22
23       <div>
24         <button type="submit">Save</button>
25       </div>
26
27     </form>
28
29   </body>
30
31 </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:

```
1 | <input type="hidden" name="_token" value="4avLrM09jjv6LK1lWJe
```

29.02 Lomakedatan tallentaminen tietokantaan

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

```
1 | ...
2 | Route::post('/customers', 'CustomerController@store');
```

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

```
1 | public function store() {
2 |     return request()->all();
3 |     // return request('name');
4 |     // return request('birth_date');
5 | }
```

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.

```
1 | {
2 |   "_token": "4avLrM09jjv6LK1lWJeLnbfXwwqmmx9MjA2kCwhX",
3 |   "name": "Vainio Elo",
4 |   "birth_date": "1999-09-09"
5 | }
```

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.

```
1   public function store() {
2
3       $customer = new Customer();
4
5       $customer->name = request('name');
6       $customer->birth_date = request('birth_date');
7
8       $customer->save();
9
10      /*
11      Customer::create([
12          'name' => request('name'),
13          'birth_date' => request('birth_date')
14      ]);
15      */
16
17      return redirect('/customers');
18  }
```