Authentication

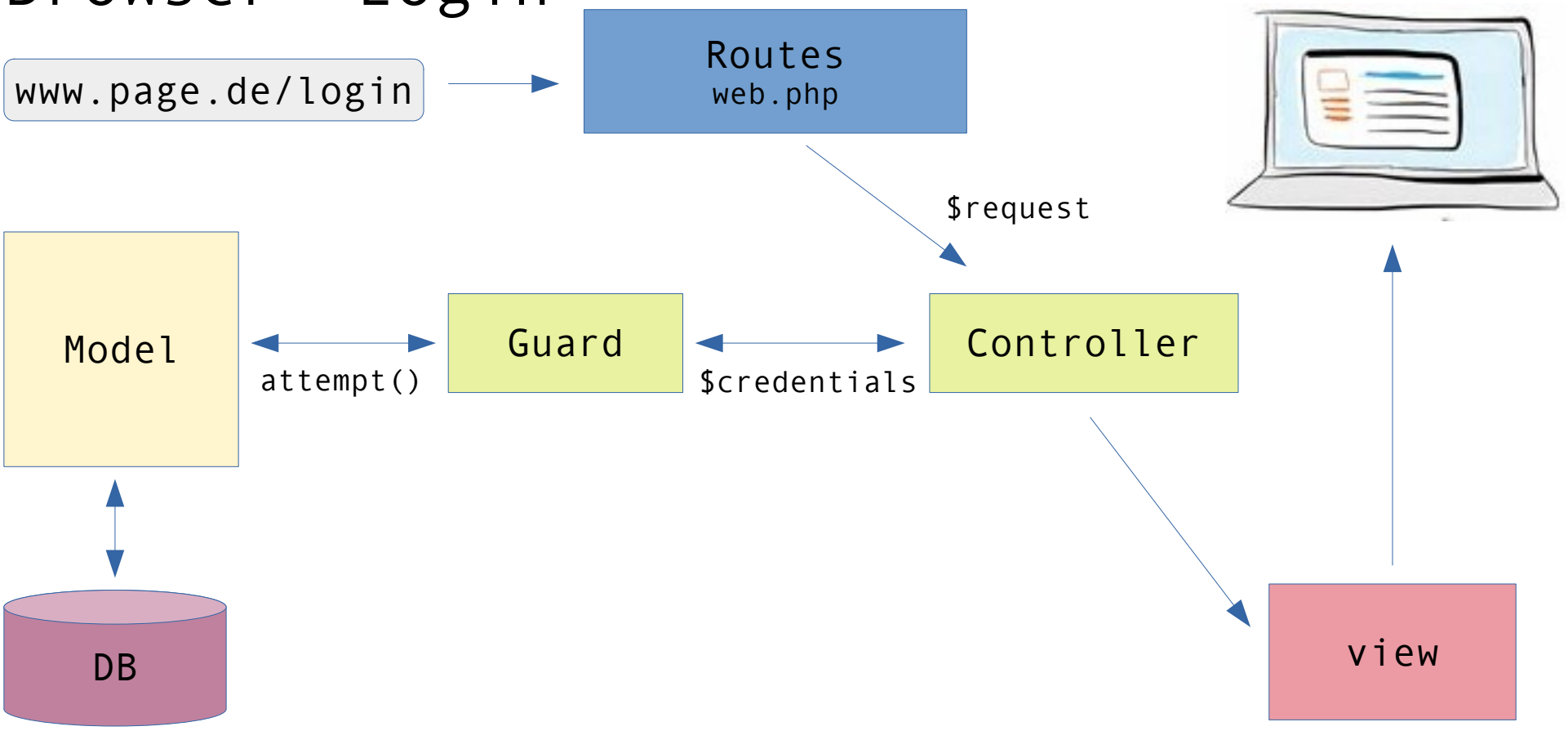
- Key Concepts
- Built in authentication services
- Custom Guards
- Password Confirmation
- Packages/Starter Kits

Laravel Framework Praktikum
Karin Haslauer, 07/15/22

Key Concepts

- Authentication = proof identity to server
  - Browser: sessions
  - or 3rd party API: token

Browser -Login



Key Concepts (2)

- Guards
  - Define how users are authenticated for each request

  → which driver: session, token

  → which providers: table
- Where? config/auth.php

Guards

- Example of default guards in config/auth.php

```
'guards' => [

    'web' => [
        'driver' => 'session',
        'provider' => 'users',
    ],

    'api' => [
        'driver' => 'custom-token',
    ],
],
```

Built in auth services

Install with:

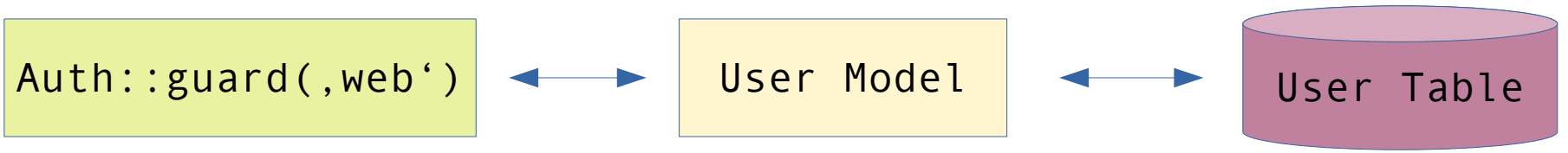
- composer require laravel/ui
- php artisan ui bootstrap –auth
- npm install && npm run dev
- npm install bootstrap@latest bootstrap-icons @popperjs/core --save-dev (for bootstrap)
- npm install && npm run dev

Built in auth services

Useful methods:

- Use Illuminate\Support\Facades\Auth;
  Auth::user(), Auth::id()
- Check if user is authenticated:
  1) if(Auth::check()){…};
  2) Route::get()→middleware('auth');
  3) Apply middleware to __construct() method of Controller
  4) Define your own middleware:
     - php artisan make:middleware AdminOnly
     - Edit handle() function → Auth::check()

Adding custom guards (multiauth)



- By default: auth:web for User Model
- New Model needs to extend Authenticable
- Define new guard in config/auth.php
- Define routes in web.php and add middleware([‘auth:new’]) with new guard
- Controller uses new guard, e.g.:
  - Auth::guard('new')→attempt($credentials) //login
  - Auth::guard('new')→logout(); //logout

Password Confirmation

- Implement views and routes
- If passwords match, use
  - `$request→session()→passwordConfirmed();`
  - Sets a timestamp in the user‘s session
- Protect routes with built-in
  - `->middleware(['password.confirm']);`

Logout on other devices

- Confirm password and log out on all other devices
- Apply auth.session middleware
- Auth::logoutOtherDevices($newPassword);

Starter kits overview

Breeze • Minimal: login, registration, password reset and confirmation, email verification • Only one auth for users • No api auth • Frontend: Blade + Tailwind CSS	Fortify • Everything: • Two-Factor authentication, teams, profile management • API (using Sanctum) • Only backend (no views)
Sanctum • For single page apps, mobile apps 1) API Tokens: Generates „personal access token“ for users 2) SPA authentication via web authentication guard (cookie)	Jetstream • Combines Fortify with Frontend (Tailwind Css, …)
Passport • Complex API token package • Using OAuth2 authentication provider	

Sources

- image: https://techwarn.com/wp-content/uploads/2020/08/2-factor-authentication-2-1536x832.jpg
- Laravel documentation
- https://www.youtube.com/watch?v=KBA22pSeoe4&t=1099s