# Rapport d’audit de qualité de code et de performance


**ToDo & Co - ToDoList**

# Table des matières

# 1. Synthèse de l'audit

## 1.1 Contexte et présentation

TO DO LIST est une application de la startup ToDO & Co qui permet de gérer ses tâches quotidiennes.
L'application a été développée en MVP (Minimum Viable Product), c'est à dire rapidement afin de pouvoir présenter le concept à de potentiels investisseurs.
Aujourd'hui, les fonds sont levés et il s'agit de développer l'application pour sa mise en service, avec une première évolution des prestations à ajouter.

## 1.2 Points forts de l'existant

- ☐ Applicatif découpé en services
- ☐ Facilité à produire des tests automatisés
- ☐ Nommage cohérent pour une compréhension facilitée
- ☐ Code plutôt documenté dans l'ensemble
- ☐ Standard de développement respecté

## 1.3 Points faibles de l'existant

- ☐ Version de PHP et de Symfony non maintenues
- ☐ Tests unitaires et fonctionnels à créer après la migration vers la version LTS

## 1.4 Sécurité globale

- ☐ Les versions de PHP et Symfony non maintenues peuvent engendrer des failles de sécurité qui ne peuvent pas être corrigées sur l'applicatif métier

## 1.5 Synthèse de recommandations

| Thème | Situation actuelle | Actions | Priorité | Temps estimé |
|---|---|---|---|---|
| Architecture Symfony | Présence de failles de sécurité | Migration vers une version LTS 4.4 ou LSR 5.3 | Haute | 1,5 J |
| | Cette version n'est plus maintenue | | Moyenne | 10 J |
| Best Practice Symfony : Standard de développement | Standard de développement (PSR) partiellement respecté | Utilisation de l'outil **PHP_CodeSniffer** permettant de détecter les erreurs / warnings potentiels.<br>Utilisation de l'outil **PHP Code Beautifer And Fixer** pour corriger certains warnings et erreurs restant | Faible | 1 J |
| Best Practice Symfony : Formulaires | Pas de vérification sur le formulaire, à la soumission | En plus de l'utilisation de la méthode **isValid()**, utiliser la méthode **isSubmitted()** | Haute | 0,5 J |

| | | | | |
|---|---|---|---|---|
| Tests automatisés | Aucun test automatisé actuellement présent | Ajouter des tests automatisés permettrait de faciliter les futures évolutions de version et ainsi garantir en permanence le fonctionnel de l'applicatif | Haute | 5 J |
| Performance | Optimisation des requêtes SQL | Ajouter un cache Doctrine | Moyenne | 2 J |
| | | Mise en place d'index sur les entités afin d'accélérer la recherche par index | Moyenne | 2 J |
| | Optimisation des requêtes HTTP | Ajout d'un cache applicatif pour les requêtes safe et idempotente | Moyenne | 3 J |
| | Accès local à Bootstrap et Jquery | Utilisation de CDN pour accéder à Bootsrap et Jquery | Haute | 0,2 J |

# 2. Architecture technique

## 2.1 PHP

### 2.1.1 Version actuelle

- ☐ PHP 5.5.9
- ☐ Cette version n'est plus maintenue depuis le 10 juillet 2016 (https://endoflife.date/php)

### 2.1.2 Commentaires et améliorations

- ☐ Risques élevés de failles de sécurité dus à l'obsolescence de la version de PHP

→ Recommandation :

- Augmenter la version de PHP pour avoir un support plus long : 7.4 ou 8.0

## 2.2 MYSQL

Rien à signaler

## 2.3 Symfony

### 2.3.1 Version actuelle

- ☐ Symfony 3.1.6
- ☐ Cette version n'est plus maintenue depuis fin juillet 2017 (https://symfony.com/releases)

### 2.3.2 Commentaires et améliorations

- ☐ Présence de failles de sécurité dues à l'obsolescence de la version de Symfony
- ☐ Voici la liste des failles de sécurité (symfony security:check) :

**swiftmailer/swiftmailer (v5.4.3)**
---

 * [CVE-2016-10074][]: Remote Code Execution when using the mail transport

**symfony/phpunit-bridge (v3.1.6)**
---

 * [CVE-2019-10912][]: Prevent destructors with side-effects from being unserialized

**symfony/symfony (v3.1.6)**
---

 * [CVE-2017-16652][]: Open redirect vulnerability on security handlers
 * [CVE-2017-16653][]: CSRF protection does not use different tokens for HTTP and HTTPS
 * [CVE-2017-16654][]: Intl bundle readers breaking out of paths
 * [CVE-2017-16790][]: Ensure that submitted data are uploaded files
 * [CVE-2018-11385][]: Session Fixation Issue for Guard Authentication
 * [CVE-2018-11386][]: Denial of service when using PDOSessionHandler
 * [CVE-2018-11406][]: CSRF Token Fixation
 * [CVE-2018-11407][]: Unauthorized access on a misconfigured LDAP server when using an empty password
 * [CVE-2018-11408][]: Open redirect vulnerability on security handlers
 * [CVE-2018-14773][]: Remove support for legacy and risky HTTP headers
 * [CVE-2018-19789][]: Temporary uploaded file path disclosure
 * [CVE-2018-19790][]: Open Redirect Vulnerability on login
 * [CVE-2019-10909][]: Escape validation messages in the PHP templating engine
 * [CVE-2019-10910][]: Check service IDs are valid
 * [CVE-2019-10911][]: Add a separator in the remember me cookie hash
 * [CVE-2019-10912][]: Prevent destructors with side-effects from being unserialized
 * [CVE-2019-10913][]: Reject invalid HTTP method overrides
 * [CVE-2019-18887][]: Use constant time comparison in UriSigner
 * [CVE-2019-18888][]: Prevent argument injection in a MimeTypeGuesser
 * [CVE-2019-18889][]: Forbid serializing AbstractAdapter and TagAwareAdapter instances
 * [CVE-2021-21424][]: Prevent user enumeration via response content in authentication mechanisms

**twig/twig (v1.27.0)**
---

 * [CVE-2019-9942][]: Sandbox Information Disclosure

- [ ] Voici les liens vers les détails de chaque CVE (Common Vulnerabilities Exposures) :

[CVE-2016-10074]: https://legalhackers.com/advisories/SwiftMailer-Exploit-Remote-Code-Exec-CVE-2016-10074-Vuln.html
[CVE-2019-10912]: https://symfony.com/cve-2019-10912
[CVE-2017-16652]: https://symfony.com/cve-2017-16652
[CVE-2017-16653]: https://symfony.com/cve-2017-16653
[CVE-2017-16654]: https://symfony.com/cve-2017-16654
[CVE-2017-16790]: https://symfony.com/cve-2017-16790
[CVE-2018-11385]: https://symfony.com/cve-2018-11385
[CVE-2018-11386]: https://symfony.com/cve-2018-11386
[CVE-2018-11406]: https://symfony.com/cve-2018-11406
[CVE-2018-11407]: https://symfony.com/cve-2018-11407
[CVE-2018-11408]: https://symfony.com/cve-2018-11408
[CVE-2018-14773]: https://symfony.com/blog/cve-2018-14773-remove-support-for-legacy-and-risky-http-headers

[CVE-2018-19789]: https://symfony.com/cve-2018-19789
[CVE-2018-19790]: https://symfony.com/cve-2018-19790
[CVE-2019-10909]: https://symfony.com/cve-2019-10909
[CVE-2019-10910]: https://symfony.com/cve-2019-10910
[CVE-2019-10911]: https://symfony.com/cve-2019-10911
[CVE-2019-10912]: https://symfony.com/cve-2019-10912
[CVE-2019-10913]: https://symfony.com/cve-2019-10913
[CVE-2019-18887]: https://symfony.com/cve-2019-18887
[CVE-2019-18888]: https://symfony.com/cve-2019-18888
[CVE-2019-18889]: https://symfony.com/cve-2019-18889
[CVE-2021-21424]: https://symfony.com/cve-2021-21424
[CVE-2019-9942]: https://symfony.com/blog/twig-sandbox-information-disclosure

→ Recommandations :

- Court terme :
  - Mise à jour du kernel de Symfony vers la version 3.4.
  - Mise à jour des dépendances liées

- Long terme :
  - Envisager une évolution vers une version LTS (Long Term Support) : 4.4 ou LSR (Latest Stable Release) 5.3
  - Effectuer la migration avec le plus grand soin :
    - Assurer la stabilité de l'applicatif existant.
    - Réaliser des tests automatisés au préalable( éviter de la régression technique)

# 3. Bonnes pratiques Symfony

## 3.1 Structure de l'application

- ☐ Un seul bundle présent

→ Recommandation :
- Aucune

## 3.2 Configuration

- ☐ Définition des paramètres canoniques dans le fichier : app/config/parameters.yaml.dist
- ☐ Le nommage des paramètres et des services doit utiliser un préfixe commun à l'intégralité de l'application

## 3.3 Nommage et format utilisé pour les services

- ☐ Présence d'un préfixe pour chaque service déclaré
- ☐ Pour une meilleure compréhension, le nom du service doit être le même que celui de la classe
- ☐ Le format .yml est utilisé pour la déclaration des services

→ Recommandation :
- Aucune

## 3.4 Doctrine

- ☐ Mapping Doctrine construit avec des annotations
- ☐ Utilisation d'un modèle anémique

→ Recommandation :

- Aucune

## 3.5 Standard de développement (PSR 1 & PSR 2)

PSR : Php Standard Recommandations

- ☐ PSR à la date de création respectées dans l'ensemble
- ☐ La PSR 12 a remplacé la PSR 2 et de ce fait, cela engendre certaines erreurs de coding style

→ Recommandations :

- Utiliser l'outil **PHP_CodeSniffer** pour être "PSR compliant"
- Utiliser l'outil **PHP Code Beautifer And Fixer** pour fixer une partie des erreurs de coding style

## 3.6 Controllers

- ☐ Les différents contrôleurs étendent bien le contrôleur du FrameworkBundle

## 3.7 Templating

- ☐ Twig est utilisé pour le templating
- ☐ Les templates sont localisés dans : app/Resources/views
- ☐ La syntaxe des templates ne contient pas d'erreur ou de warning (Utilisation de la commande **lint:twig** pour lister les erreurs de syntaxe dans les templates)

→ Recommandation :

- Utiliser l'outil additionnel **twigcs** (en plus de lint:twig), pour détecter des erreurs de respect des bonnes pratiques Twig

## 3.8 Formulaires

- ☐ Les formulaires sont localisés dans src/AppBundle/Form
- ☐ Les contraintes de validation sont utilisées en HTML5 et non pas sur les formulaires, c'est insuffisant

→ Recommandations :

- La validation des champs du formulaires doit s'effectuer dans le formulaire
- La gestion d'envoi d'un formulaire doit comporter la validation du formulaire mais aussi le fait qu'il a bien été soumis, grâce à la méthode isSubmitted()

## 3.9 Internationalisation

- ☐ Pas d'internationalisation prévue

→ Recommandation :

- Aucune

## 3.10 Sécurité

- [ ] Algorithme utilisé pour l'encodage des mots de passe : **bcrypt**
- [ ] Un seul firewall utilisé sur l'application
- [ ] Des rôles avec une hierarchie clairement définie

→ Recommandation :

- 

## 3.11 Gestion des assets

- [ ] Les assets des templates sont stockés dans le dossier web

→ Recommandation :

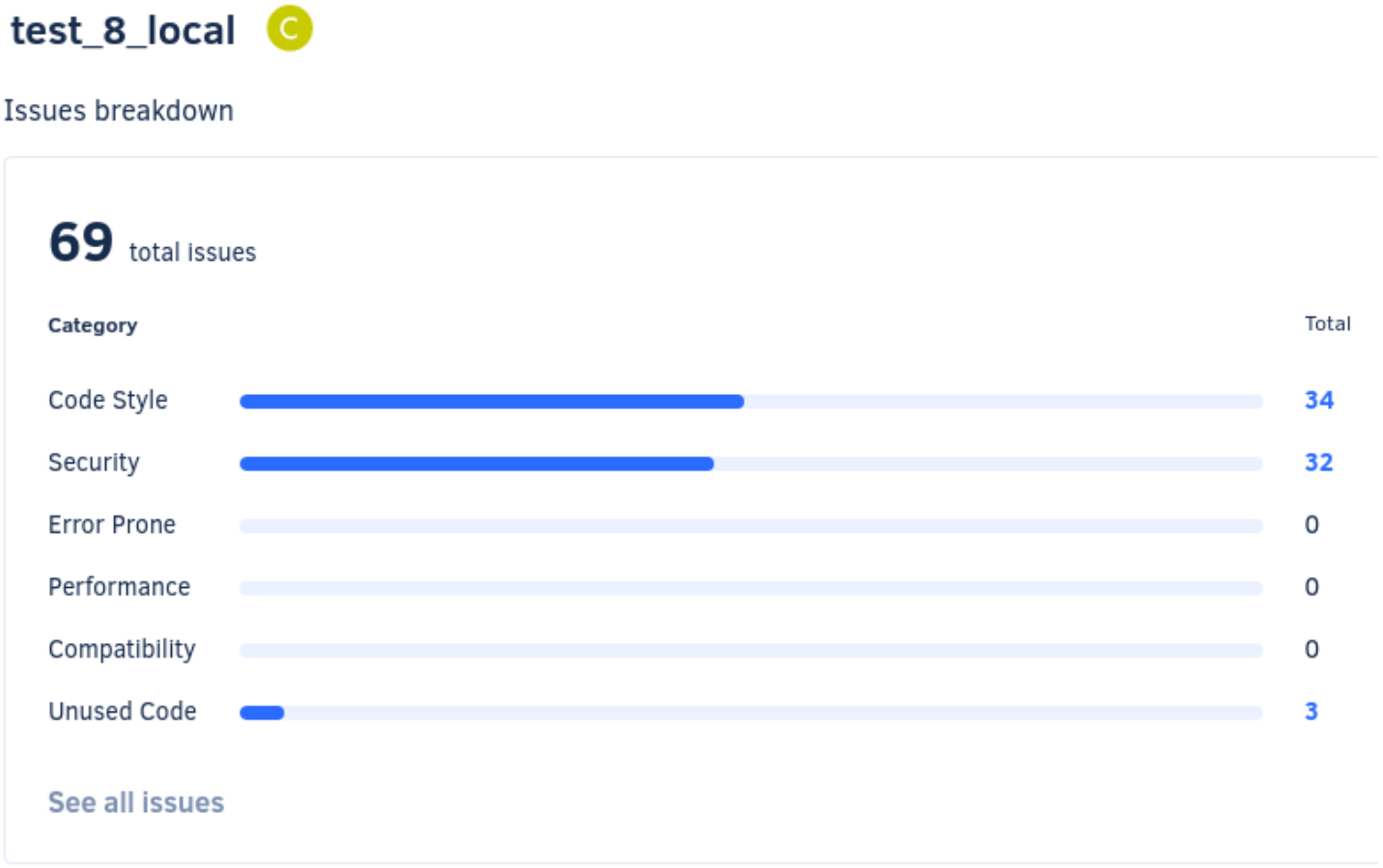
- Aucune

# 4. Tests

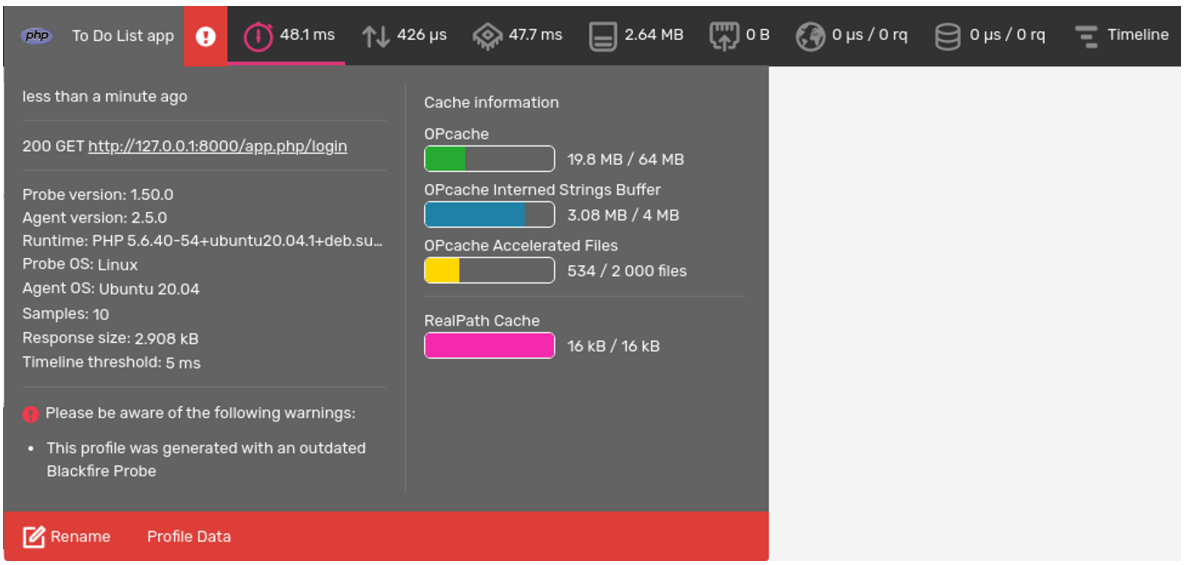
## 4.1 Tests du MVP

Mesures de la qualité du code avec Codacy et Blackfire

### 4.1.1 Qualité du code avec Codacy



# 4.1.2 Performance avec Blackfire



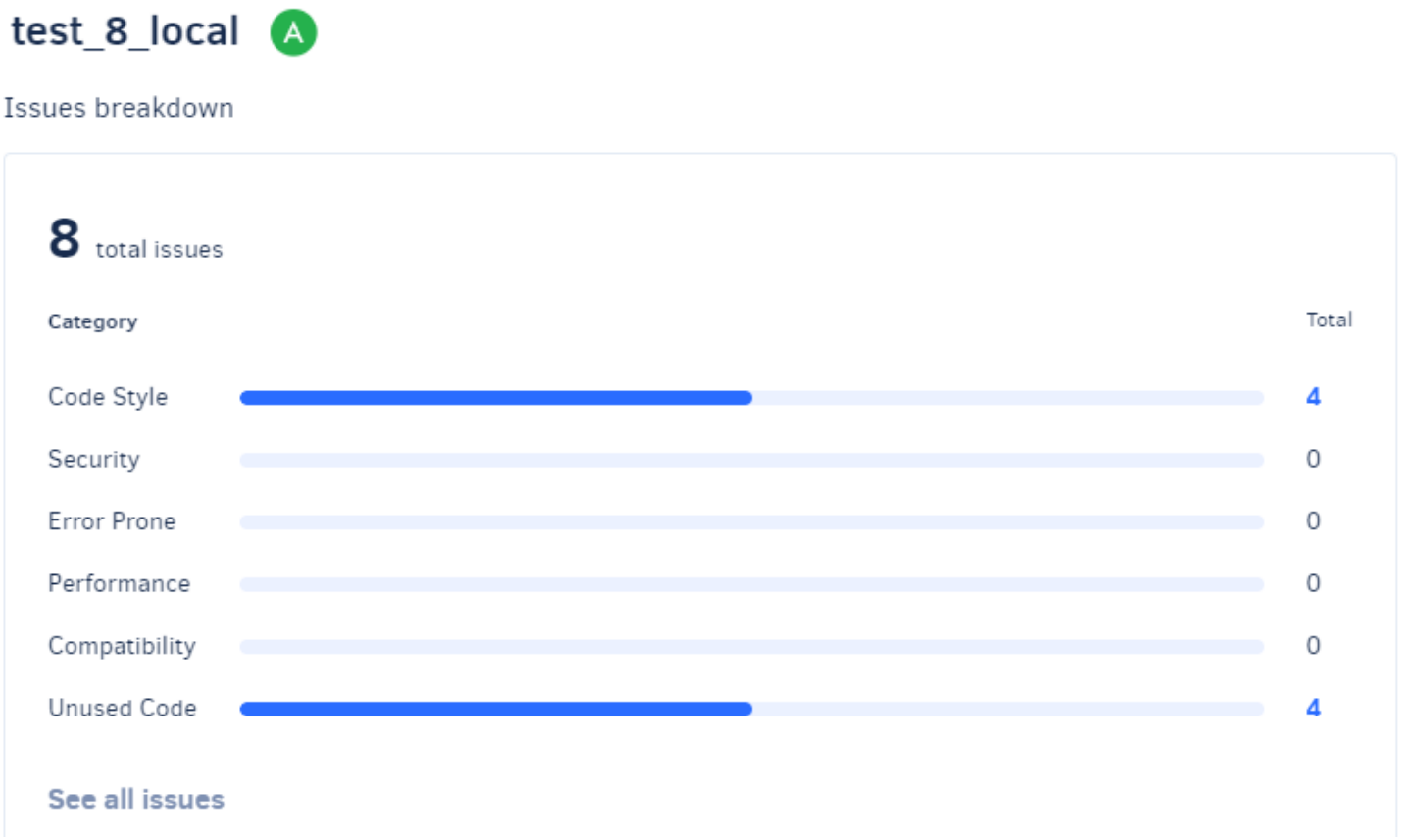

| Function calls | % Excl. | % Incl. | Calls |
|---|---|---|---|
| Composer\Autoload\includeFile | | | 179 |
| Composer\Autoload\ClassLoader::findFileWithExtension | | | 313 |
| file_exists | | | 436 |
| Composer\Autoload\includeFile@1 | | | 81 |
| appProdProjectContainer::get@2 | | | 40 |
| appProdProjectContainer::get@1 | | | 44 |
| …mponent\EventDispatcher\ContainerAwareEventDispatcher::doDispatch | | | 5 |
| Swift::autoload | | | 12 |
| base.html.twig::doDisplay | | | 1 |
| Doctrine\ORM\Persisters\Entity\BasicEntityPersister::load | | | 1 |
| Composer\Autoload\ClassLoader::findFile | | | 314 |
| appProdProjectContainer::get | | | 40 |
| Doctrine\DBAL\Driver\PDOConnection::__construct | | | 1 |
| Composer\Autoload\ClassLoader::loadClass | | | 205 |
| run_init::web/app.php | | | 1 |
| appProdProjectContainer::getTwigService | | | 1 |
| spl_autoload_call | | | 192 |
| …Component\HttpKernel\EventListener\RouterListener::onKernelRequest | | | 1 |
| Doctrine\Common\Cache\FilesystemCache::doFetch | | | 8 |
| PDOStatement::execute(…) | | | 1 |
| run_init::lib/swift_init.php | | | 1 |
| Composer\Autoload\includeFile@2 | | | 23 |
| Twig_Environment::loadTemplate | | | 1 |
| AppKernel::boot | | | 1 |
| …n_init::php/73052dcad8090a755e19a19ce8c9a262044f5853-router.php | | | 1 |
| unserialize | | | 8 |
| AppKernel::initializeContainer | | | 1 |
| Twig_Environment::addExtension | | | 16 |
| …pProdProjectContainer::getDoctrine_Orm_DefaultEntityManagerService | | | 1 |
| appProdProjectContainer::getAnnotationReaderService | | | 1 |
| …eworkExtraBundle\EventListener\ControllerListener::onKernelController | | | 1 |
| Doctrine\Common\Annotations\CachedReader::getPropertyAnnotations | | | 40 |
| Composer\Autoload\ClassLoader::loadClass@1 | | | 81 |
| Swift::autoload@1 | | | 13 |
| Symfony\Component\HttpKernel\HttpKernel::handleRaw | | | 1 |
| …ventDispatcher\ContainerAwareEventDispatcher::addSubscriberService | | | 20 |
| …trine\ORM\Mapping\ClassMetadata::_validateAndCompleteFieldMapping | | | 4 |
| spl_autoload_call@1 | | | 94 |
| Symfony\Component\ClassLoader\ClassCollectionLoader::load | | | 1 |

### 4.1.3 Test unitaires et fonctionnels avec PHPUnit

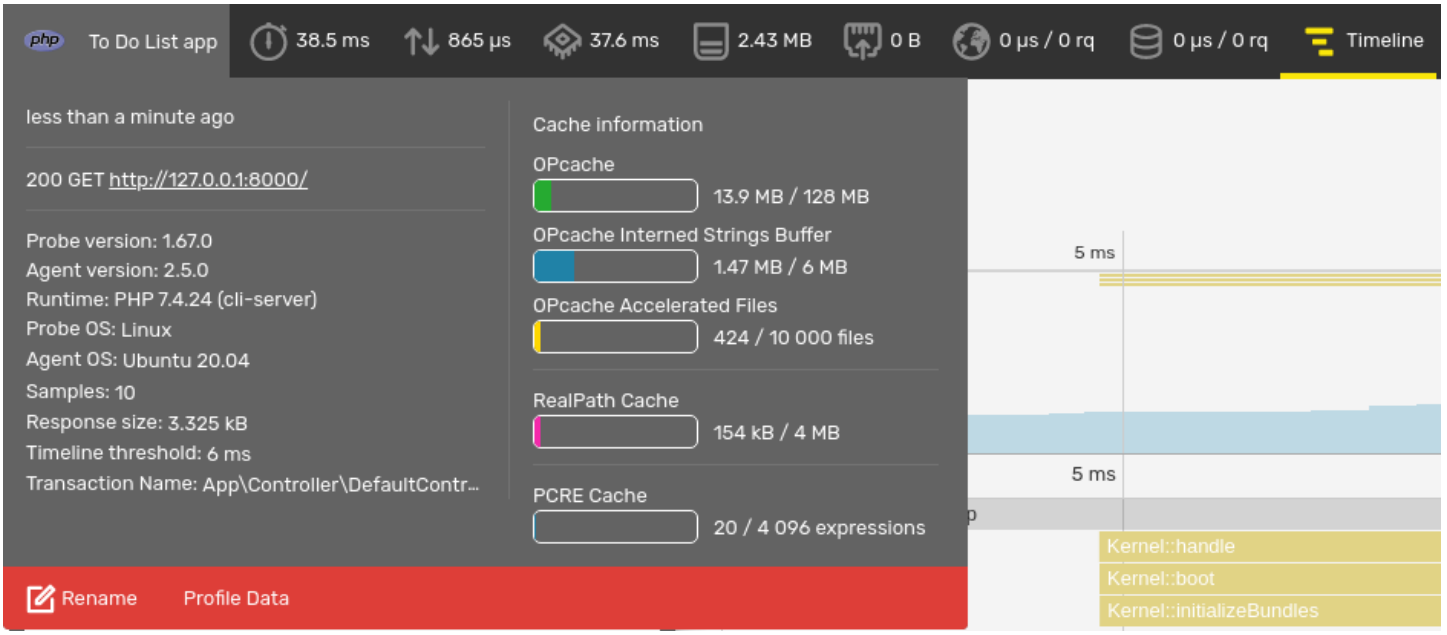
- [ ] Aucun test présent

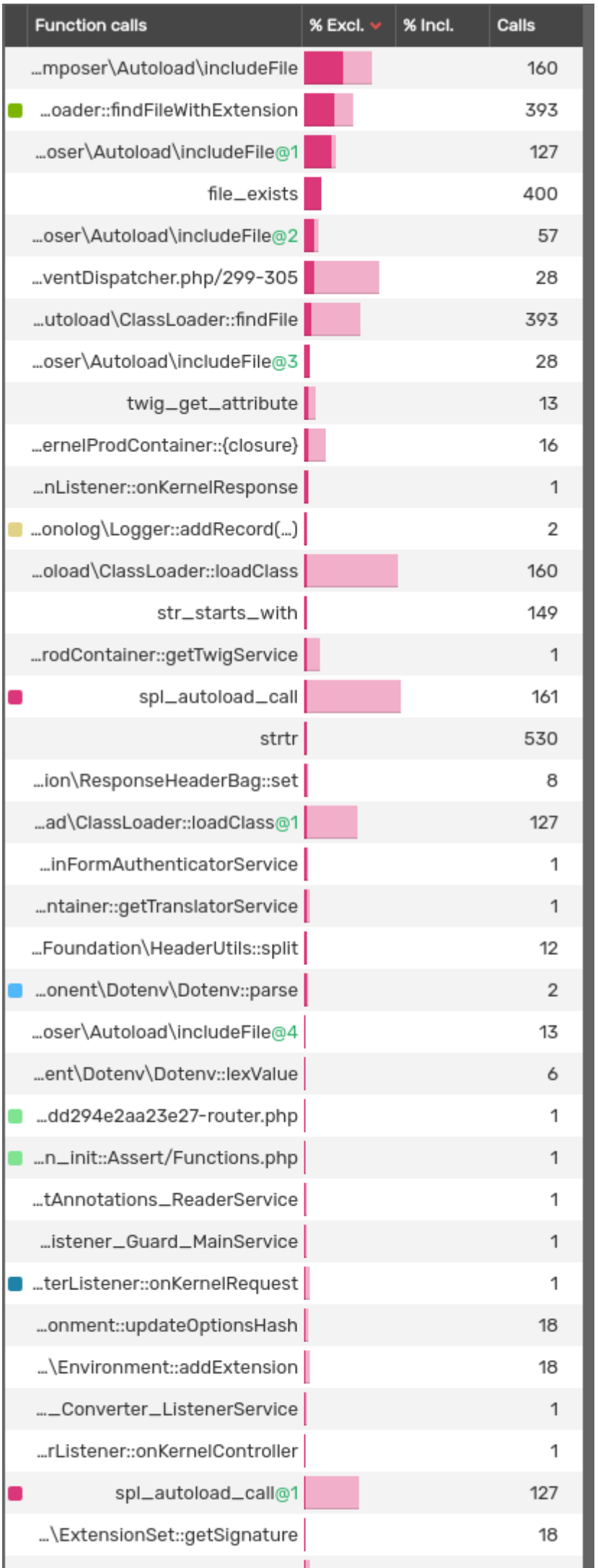
## 4.2 Tests de la version LTS

### 4.2.1 Qualité du code avec Codacy




### 4.2.2 Performance avec Blackfire





| Function calls | % Excl. | % Incl. | Calls |
|---|---|---|---|
| …mposer\Autoload\includeFile | | | 160 |
| …oader::findFileWithExtension | | | 393 |
| …oser\Autoload\includeFile@1 | | | 127 |
| file_exists | | | 400 |
| …oser\Autoload\includeFile@2 | | | 57 |
| …ventDispatcher.php/299-305 | | | 28 |
| …utoload\ClassLoader::findFile | | | 393 |
| …oser\Autoload\includeFile@3 | | | 28 |
| twig_get_attribute | | | 13 |
| …ernelProdContainer::{closure} | | | 16 |
| …nListener::onKernelResponse | | | 1 |
| …onolog\Logger::addRecord(…) | | | 2 |
| …oload\ClassLoader::loadClass | | | 160 |
| str_starts_with | | | 149 |
| …rodContainer::getTwigService | | | 1 |
| spl_autoload_call | | | 161 |
| strtr | | | 530 |
| …ion\ResponseHeaderBag::set | | | 8 |
| …ad\ClassLoader::loadClass@1 | | | 127 |
| …inFormAuthenticatorService | | | 1 |
| …ntainer::getTranslatorService | | | 1 |
| …Foundation\HeaderUtils::split | | | 12 |
| …onent\Dotenv\Dotenv::parse | | | 2 |
| …oser\Autoload\includeFile@4 | | | 13 |
| …ent\Dotenv\Dotenv::lexValue | | | 6 |
| …dd294e2aa23e27-router.php | | | 1 |
| …n_init::Assert/Functions.php | | | 1 |
| …tAnnotations_ReaderService | | | 1 |
| …istener_Guard_MainService | | | 1 |
| …terListener::onKernelRequest | | | 1 |
| …onment::updateOptionsHash | | | 18 |
| …\Environment::addExtension | | | 18 |
| …_Converter_ListenerService | | | 1 |
| …rListener::onKernelController | | | 1 |
| spl_autoload_call@1 | | | 127 |
| …\ExtensionSet::getSignature | | | 18 |

### 4.2.3 Test unitaires et fonctionnels avec PHPUnit

- ☐ Utilisation de phpunit version 9.5
- ☐ Tests présents

→ Recommandation :

- Enrichir les tests unitaires et fonctionnels afin de gagner en maintenance et en facilité d'évolution, dans l'optique de l'évolution majeure de Symfony

# 5. Performance

→ Recommandations :

- L'application gagnerait en performance grâce aux éléments suivants :
  - Cache applicatif sur les requêtes dites safe et idempotente
  - Cache Doctrine pour améliorer la performance des requêtes en base de données
  - Index sur les entités afin d'optimiser les recherches en base de données

# 6. Evolutions

- Rappel du besoin et commentaires

- Associer les utilisateurs aux tâches
  Lister toutes les tâches en cours, avec l'utilisateur associé, par ordre chronologique d'imminence
  Lister les tâches associées à chaque utilisateur
  Distinguer les tâches terminées des tâches en cours, avec règlage du nombre à afficher pour améliorer l'affichage
  → Estimation :

- Ajouter une date d'échéance d'une tâche
  Lister les tâches arrivant à échéance
  Afficher la date de création et la date d'échéance de chaque tâche
  → Estimation :

- Ajouter un rôle à chaque utilisateur
  - Rôle ADMINISTRATEUR
  - Rôle UTILISATEUR

  → Estimation :

- Autorisations
  - Seuls les ADMINISTRATEURS peuvent gérer la page des UTILISATEURS
  - Les tâches ne peuvent être supprimées que par les utilisateurs associés
  - Seuls les ADMINISTRATEUR peuvent supprimer des tâches sans utilisateur associé (=anonyme")

  → Estimation :