
TO DO LIST

1
2
3

**Audit de qualité du
code & performance
de l'application
« To Do List »**



11 MARS 2020

Valérie Bleser

<http://www.valeriebleser.fr>



SOMMAIRE

Qualité du code	3
L'échantillon	3
Code Sniffer	3
Exigences VPTCS - Technique	3
a. Diagnostique avec Recx Security Analyser :.....	4
b. Autres critères sécurité et confidentialité à corriger	6
c. Critères serveur et performance	7
Valdateur HTML W3C.....	8
a. Accueil	8
b. Page de création d'une tâche.....	8
c. Page de création d'un utilisateur	8
d. Page de consultation des tâches	8
Qualité de performance - Blackfire	9
Traitement des dépréciations	9
Passage de Symfony 3.4 à 4.4	11

Qualité du code

L'échantillon

http://127.0.0.1:8000/	Accueil
http://127.0.0.1:8000/login	Page de connexion
http://127.0.0.1:8000/users/create	Page de création d'un utilisateur
http://127.0.0.1:8000/tasks/create	Page de création d'une tâche
http://127.0.0.1:8000/tasks	Page de consultation des tâches
http://127.0.0.1:8000/tasks/1/edit	Page d'édition d'une tâche
http://127.0.0.1:8000/foobar	Page 404

Code Sniffer

Pour améliorer la qualité du code, plusieurs outils peuvent être utilisés pour permettre une meilleure lisibilité et une meilleure organisation en vue des futurs développements dans l'évolution de l'application.

Le premier que nous avons utilisé est Code Sniffer v3.0 qui permet de vérifier que le code obéit aux standards sélectionnés.

Nous avons appliqué les premiers correctifs automatisés. D'autres correctifs sont possibles et peuvent permettre d'aller plus loin dans le respect des recommandations standards pour PHP, les PSR.

Les correctifs de Code Sniffer permettent de conserver un code uniforme, particulièrement dans le cas de collaboration de plusieurs développeurs.

Exigences VPTCS - Technique

Le modèle VPTCS permet de classer et de structurer les exigences utilisateurs d'une interface.

Dans le cadre de ce premier audit, nous traiterons seulement des exigences en termes de Technique de ce modèle et nous les détaillerons dans ce rapport. Les autres exigences feront l'objet d'une autre analyse dans un second temps.

Dans le prochain chapitre, nous traiterons les aspects de sécurité, de conformité W3C.

Dans la seconde section, nous utiliserons l'outil Blackfire pour évaluer la performance.

a. Diagnostic avec Recx Security Analyser :

HTTP security headers

Name	Value	Setting secure
cache-control	max-age=0, must-revalidate, private	
x-content-type-options	Header not returned	
x-xss-protection	Header not returned	
x-frame-options	Header not returned	
content-security-policy	Header not returned	
access-control-allow-origin	Header not returned	
		

Page meta security headers

Name	Value	Setting secure
content-security-policy	N/A	
cache-control	N/A	

Cookie security options (1 cookies)

Name	Domain	Secure attribute	HTTP only attribute	Host only attribute
PHPSESSID	127.0.0.1			

All HTTP headers

Name	Value
cache-control	max-age=0, must-revalidate, private
connection	close
content-type	text/html; charset=utf-8
date	mon, 24 feb 2020 20:44:10 gmt, mon, 24 feb 2020 20:44:10 gmt
expires	mon, 24 feb 2020 20:44:10 gmt
host	127.0.0.1:8000
x-debug-token	e2de56
x-debug-token-link	http://127.0.0.1:8000/_profiler/e2de56
x-powered-by	php/7.3.12

Atouts

- Critère 195 : le serveur indique le type MIME de chaque ressource ; permet de réduire les risques de téléchargement d'un contenu dangereux dissimulé. Test OK : content-type = text/html; charset=utf-8.

Défauts

- Critère 194 : les en-têtes envoyés par le serveur désactivent la détection automatique du type MIME de chaque ressource ; permet de réduire les risques de téléchargement d'un contenu dangereux dissimulé. Solution : X-Content-Type-Options = nosniff.
- Critère 203 : le serveur envoie les informations d'activation de protection cross site scripting ; permet de Réduire les risques de téléchargement d'un contenu dangereux dissimulé. Solution : X-XSS-Protection = 1 ; mode=block.
- Critère 204 : le serveur envoie les informations indiquant les domaines autorisés à intégrer ses pages dans des cadres ; permet de réduire les risques d'utilisation trompeuse du contenu. Solution : X-Frame-Options = sameorigin.
- Critère 205 : Le site propose un mécanisme de sécurité permettant de restreindre l'origine des contenus ; permet de réduire les risques d'exécution ou d'affichage d'un contenu non désirable ou d'une source non autorisée. Solution : Content-Security-Policy = default-src 'self'.

b. Autres critères sécurité et confidentialité à corriger

Critère	Détails	Solution
186	La politique de confidentialité et de respect de la vie privée est accessible depuis toutes les pages.	Dans chaque page du site : les informations relatives à la politique de confidentialité et de respect de la vie privée du site doivent être accessibles : soit via un lien présent dans toutes les pages du site (par exemple, dans le pied de page), soit au sein des mentions légales, soit inscrites directement dans toutes les pages.
187	Le site propose une procédure de réinitialisation du mot de passe.	Ajouter un lien avec un formulaire pour permettre la réinitialisation du mot de passe : • sans être identifié sur le site, vérifier la présence d'un lien du type « Mot de passe oublié ? » à proximité du formulaire de connexion ; • vérifier la présence d'une procédure permettant la création d'un nouveau mot de passe sur la page pointée par le lien « Mot de passe oublié ? » ; • vérifier qu'il s'agit bien d'une procédure de réinitialisation et non pas d'un simple renvoi du mot de passe actuel.
188	Les mots de passe peuvent être choisis ou changés par l'utilisateur.	Ajouter une page de modification de compte, vérifier qu'il est possible de saisir le mot de passe de son choix à la création du compte ou, dans le cas où le mot de passe est automatiquement généré par le service en ligne, contrôler qu'il est possible de le modifier après l'inscription avec contrôle de la bonne pratique sur la double saisie du mot de passe.
190	Un dispositif sensibilise l'utilisateur sur le degré de sécurisation du mot de passe qu'il choisit	Lors de l'inscription ou changement de mot de passe : saisir un mot de passe et s'assurer que cette saisie donne lieu à une validation et à un retour indiquant son degré de sécurité, et ce, avant la soumission définitive du formulaire. Cette validation peut être plus ou moins exigeante : contrôle du nombre de caractères, de l'absence de l'identifiant du compte dans le mot de passe, du type de caractères présents, etc.
197	L'objectif des cookies et les limitations inhérentes à leur refus sont expliqués.	A préciser dans la politique de confidentialité du site que la navigation nécessite l'acceptation des cookies et expliquer la raison de leur utilisation, la nature des données conservées et éventuellement, fournir les liens permettant leur désactivation.

Critère	Détails	Solution
198	La procédure d'accès et de rectification des données personnelles est décrite.	La procédure d'accès et de rectification des données personnelles doit également être décrites (GDPR).

c. Critères serveur et performance

208	Le serveur envoie une page d'erreur 404 personnalisée.	Modifier la configuration du serveur web pour renvoyer l'utilisateur vers une page personnalisée lorsque la ressource demandée n'existe pas
209	Le serveur envoie une page d'interdiction 403 personnalisée.	Modifier la configuration du serveur web pour renvoyer l'utilisateur vers une page personnalisée lorsque l'accès à la ressource demandée n'est pas autorisé. Pour l'instant seul un message d'erreur est affiché.
210	Le menu principal de navigation figure sur les pages d'erreur personnalisées.	Une page d'erreur doit reprendre soit de façon dynamique soit de façon statique l'ensemble de la navigation principale du site.
211	Le serveur transmet des contenus compressés aux clients qui les acceptent.	Activer le module Gzip ou Deflate du serveur pour compresser les ressources Javascript, CSS et HTML.
215	Les scripts du site sont minifiés.	<code><script src="/js/jquery.js"></script></code> . Toutes les scripts ne sont pas minifiés.

Valdateur HTML W3C

a. Accueil

Warning: <a> attribute "href" lacks value

```
<a href="" class="btn btn-secondary">Consulter la liste des tâches terminées</a>
```

Le lien 'Consulter la liste des tâches terminées' ne pointe vers rien. Ajouter un lien vers les tâches avec le toggle=1.

b. Page de création d'une tâche

Warning: <div> anchor "task" already defined

```
<div id="task">
```

L'id « Task » a été utilisé deux fois :

```
<form name="task" method="post" action="/tasks/create" id="task">
```

```
<div id="task">
```

c. Page de création d'un utilisateur

Warning: <div> anchor "user" already defined

```
<div id="user">
```

L'id « User » a été utilisé deux fois :

```
<form name="task" method="post" action="/tasks/create" id="user">
```

```
<div id="user">
```

d. Page de consultation des tâches

Warning: trimming empty

```
<span class="glyphicon glyphicon-remove"></span>
```

A chaque affichage d'une tâche dans un cadre, se trouve une balise vide.

Qualité de performance - Blackfire

Traitement des dépréciations

Afin d'optimiser la performance de l'application et de bénéficier d'une version stable de Symfony plus récente, nous proposons de mettre à jour la version de Symfony de la version 3.4 à la version 4.4.

Les avantages de la version 4.4 sont :

- il s'agit d'une version minimaliste, sans packages inutiles
- les bundles n'ont plus besoin d'être configurés dans le config.yml grâce à Symfony Flex
- le déploiement est plus rapide et simplifié
- il permet un fonctionnement en mode projet et accroît la maintenabilité.

Afin d'effectuer cette mise à jour, nous proposons dans un premier temps de traiter les dépréciations :

Dans notre échantillon, les pages suivantes présentaient des dépréciations :

http://127.0.0.1:8000/login	Page de connexion
http://127.0.0.1:8000/users/create	Page de création d'un utilisateur
http://127.0.0.1:8000/tasks/create	Page de création d'une tâche

Leur traitement a déjà optimisé la performance. Vous trouverez ci-dessous le comparatif avant/après cette étape :

Comparison  -5.33%  -12%

From: 1st Profile S. 3.4
200 GET <http://127.0.0.1:8000/login>
7 hours ago

To: Login after depreciation solved
200 GET <http://127.0.0.1:8000/login>
less than a minute ago

Probe version: 1.31.0
Agent version: 1.32.0
Runtime: PHP 7.3.12 (cli-server)
Probe OS: WINNT
Agent OS: Windows 10 Pro 10.0
Samples: 10
Response size: 43.67 kB

[↔ Switch comparison direction](#)

Page de connexion

Comparison  -4.12%  -0.805%

From: 1st Profile S. 3.4
200 GET <http://127.0.0.1:8000/users/create>
2 minutes ago

To: Login after depreciation solved
200 GET <http://127.0.0.1:8000/users/create>
less than a minute ago

Probe version: 1.31.0
Agent version: 1.32.0
Runtime: PHP 7.3.12 (cli-server)
Probe OS: WINNT
Agent OS: Windows 10 Pro 10.0
Samples: 10
Response size: 44.95 kB

[↔ Switch comparison direction](#)

Page de création d'un utilisateur

Comparison  -3.88%  -0.826%

From: 1st Profile S. 3.4
200 GET <http://127.0.0.1:8000/tasks/create>
2 minutes ago

To: Login after depreciation solved
200 GET <http://127.0.0.1:8000/tasks/create>
less than a minute ago

Probe version: 1.31.0
Agent version: 1.32.0
Runtime: PHP 7.3.12 (cli-server)
Probe OS: WINNT
Agent OS: Windows 10 Pro 10.0
Samples: 10
Response size: 44.22 kB

[↔ Switch comparison direction](#)

Page de création d'une tâche

Enfin, lors d'une exécution des tests avec phpunit :

```
C:\Project8\4.4\Project8>vendor\bin\phpunit

Deprecated: The each() function is deprecated. This message will be suppressed on further calls in C:\Project8\4.4\Project8\vendor\phpunit\phpunit\src\Util\Getopt.php on line 38
PHPUnit 4.8.36 by Sebastian Bergmann and contributors.

.....

Time: 17.05 seconds, Memory: 44.00MB

OK (25 tests, 34 assertions)
```

Un passage à phpunit 6.5 permet de résoudre cette dépréciation :

```
C:\Project8\4.4\Project8>vendor\bin\phpunit
PHPUnit 6.5.14 by Sebastian Bergmann and contributors.

.....                               25 / 25 (100%)

Time: 7.59 seconds, Memory: 42.00MB

OK (25 tests, 34 assertions)
```

Passage de Symfony 3.4 à 4.4

Une version de l'application a été ajoutée dans un Repository GitHub :

https://github.com/vbopenclass/Project8_4.4

En plus de tous les avantages de la dernière version stable de Symfony, nous avons légèrement accru la performance.

Dans le cas de la page de connexion :

The screenshot displays a performance comparison interface. At the top, a 'Comparison' header shows two metrics: a red circle with a plus sign indicating a +0.547% change, and a blue circle with a minus sign indicating a -3.35% change. Below this, a table-like structure compares two profiles:

- From: 2nd Profile S. 4.4**
200 GET <http://127.0.0.1:8001/login>
24 minutes ago
- To: 1st Profile S. 3.4**
200 GET <http://127.0.0.1:8002/login>
1 hour ago

Below the comparison, technical details are listed:

- Probe version: 1.31.0
- Agent version: 1.32.0
- Runtime: PHP 7.3.12 (cli-server)
- Probe OS: WINNT
- Agent OS: Windows 10 Pro 10.0
- Samples: 10
- Response size: 53.1 kB → 43.67 kB

At the bottom, there is a link to 'Switch comparison direction'.