



The Bearded Bear

Bear Scan — Audit de code PHP / Symfony

Sachez où en est votre code.

En 10 jours.

Un audit de code PHP/Symfony — sécurité, architecture, dette technique — livré et priorisé par un CTO. Pas de rapport générique : des recommandations concrètes et actionnables.

Plaquette Bear Scan

Édition octobre 2026

the-bearded-bear.com

POUR QUI

À qui s'adresse Bear Scan

CTO & DSI

Vous héritez d'une codebase et voulez un état des lieux objectif avant d'investir.

Fondateurs SaaS

Le produit a grossi vite : vous voulez savoir ce qui tiendra la charge et ce qui va casser.

Repreneurs / M&A

Due diligence technique avant rachat : risques, dette et coût de remise à niveau chiffrés.

Équipes Symfony

Un legacy PHP/Symfony à moderniser : vous cherchez par où commencer, sans y passer trois semaines.

PÉRIMÈTRE

Ce que j'audite

Architecture

Patterns utilisés, couplage, séparation des responsabilités, scalabilité. Identification des points de friction.

Qualité de code

Analyse statique (PHPStan, Rector), conventions, complexité cyclomatique, couverture de tests.

Sécurité

Vulnérabilités OWASP, mais aussi autorisation applicative (IDOR, mass assignment), JWT et uploads — au-delà des dépendances obsolètes et des headers HTTP.

Performance

Requêtes SQL, cache, temps de réponse, profiling. Identification des goulots d'étranglement.

CI/CD

Pipeline de déploiement, tests automatisés, environnements, processus de release et rollback.

Dette technique

Cartographie de la dette, estimation du coût de remédiation, priorisation des chantiers.

SÉCURITÉ

Ce qu'un linter PHP ne voit pas

~36 analyseurs, scoring pondéré sur 6 axes · Rapports PDF / HTML / SARIF · Historique & diff entre scans · agrégation multi-dépôts

IDOR / BOLA

Accès à une ressource sans contrôle d'appartenance : lire ou modifier les données d'un autre utilisateur via un ID deviné. Invisible pour un linter, détecté ici.

Mass assignment Symfony

Formulaires et désérialisation qui laissent écrire des champs non prévus (rôle, statut, propriétaire). On repère les entités surexposées.

Uploads non validés

Fichiers acceptés sans contrôle de type, de taille ou de chemin : porte d'entrée classique vers l'exécution de code ou le stockage empoisonné.

JWT faibles

alg:none, secret HMAC trop court, LexikJWT sans passphrase : jetons forgeables. On audite la configuration réelle, pas la théorie.

Migrations Doctrine

Migrations destructrices ou divergentes du schéma, index manquants : risques de perte de données et de lenteurs en production.

Serializer & RGPD

Groupes de sérialisation trop larges qui exposent des données personnelles dans les réponses API. Surface RGPD cartographiée.

LIVRABLES

Ce que vous recevez

Rapport d'audit détaillé

Relu, priorisé et contextualisé par un CTO — pas du HTML brut. Scoring par discipline, problèmes avec sévérité, extraits de code. PDF, HTML ou SARIF. Annexe « devis de migration » incluse quand le projet tourne hors LTS.

Plan d'action priorisé

Chaque recommandation classée par urgence (critique, important, mineur) avec estimation d'effort et impact attendu.

Call de restitution

Session pour parcourir les résultats, répondre aux questions et affiner les priorités ensemble.

TARIFS

Une grille, pas un tarif fourre-tout

Le prix suit la taille et la complexité réelles de votre codebase. Rapport livré en 10 jours ouvrés.

Essentiel

990 € HT

< 15 000 lignes, mono-dépôt

- Scan complet (~36 analyseurs, 6 axes)
- Rapport PDF priorisé par un CTO
- Call de restitution 30 min

Standard

1 900 € HT

15 000 – 60 000 lignes

- Tout Essentiel, plus :
- Plan d'action priorisé (effort × impact)
- Call de restitution 1 h
- Ré-audit à 3 mois offert

Approfondi

3 200 € HT

> 60 000 lignes / multi-bundle

- Tout Standard, plus :
- Revue d'architecture détaillée
- Synthèse exécutive (pour le board)
- 2 calls de restitution

Portfolio

5 000–15 000 € HT

DSI / due diligence M&A, N dépôts

- Vue portefeuille multi-dépôts
- Santé pondérée par dépôt
- Roadmap transverse priorisée

OPTIONS

Pour aller plus loin

Annexe devis de migration

Incluse dans chaque rapport concerné : chiffrage de la migration Symfony/PHP hors LTS, prête à budgéter.

Ré-audit / suivi trimestriel

À 50 % du prix de l'audit initial, ou inclus dans la maintenance Bear Upgrade. L'historique et le diff entre scans montrent noir sur blanc ce qui progresse et ce qui dérive.

Montant crédité sur Bear Upgrade

Signez un Bear Upgrade dans les 30 jours suivant la restitution : le prix de l'audit est déduit de la migration.

Urgence (< 48 h)

Livraison accélérée du rapport quand la deadline l'exige : +30 % sur le palier concerné.

Questions fréquentes

Combien de temps dure un audit ?

Comptez 10 jours ouvrés entre le début de l'analyse et la livraison du rapport. Le call de restitution est planifié dans la foulée.

De quoi avez-vous besoin pour réaliser l'audit ?

Un accès en lecture à votre repository (GitLab, GitHub, Bitbucket) et un call de cadrage de 30 min pour comprendre le contexte et les priorités.

En quoi est-ce différent d'un scan automatique ?

Le rapport n'est pas du HTML brut craché par un outil. Chaque finding est relu, priorisé et contextualisé par un CTO : ce qui compte pour votre projet remonte en premier, le bruit est écarté.

Détectez-vous des failles qu'un linter PHP ignore ?

Oui. Au-delà de l'analyse statique (PHPStan, Rector), Bear Scan détecte les failles d'autorisation applicative — IDOR/BOLA, mass assignment Symfony, uploads non validés, JWT faibles — que les linters ne voient pas.

Quel palier choisir ?

L'Essentiel couvre un projet mono-dépôt de moins de 15 000 lignes ; le Standard, un projet de taille moyenne ; l'Approfondi, les grosses codebases multi-bundles ; le Portfolio, une DSI ou une due diligence M&A sur plusieurs dépôts. Le calculateur affine l'estimation selon votre projet.

L'audit couvre-t-il uniquement les projets Symfony ?

Non. L'expertise approfondie porte sur Symfony/PHP, mais j'audite aussi les aspects transversaux (architecture, CI/CD, sécurité, dette technique) quel que soit le framework.

Que se passe-t-il après l'audit ?

Vous êtes autonomes pour exécuter le plan d'action avec votre équipe. Si vous souhaitez être accompagnés pour la mise en œuvre, je la prends en charge avec Bear Upgrade (migration et modernisation du socle).

Prêt à connaître l'état réel de votre codebase ?

Un appel pour cadrer le périmètre de l'audit et choisir le palier adapté.

Cadrer mon audit en 30 min

Appel de 30 min, sans engagement :
réserver un créneau

flavien@the-bearded-bear.com
the-bearded-bear.com

The Bearded Bear est le nom commercial de THE BEAR AND THE SHRIMP SAS, société par actions simplifiée au capital de 2 000 EUR, 5 Rue Conchette, 63300 Thiers. SIRET 900 562 604 00026 · RCS Clermont-Ferrand 900 562 604 · TVA FR 48 900 562 604. Prix hors taxes ; conditions générales de vente : the-bearded-bear.com/cgv.