Outils de Qualimétrie Open Source pour PHP

Club Qualimétrie

15 janvier 2008

qualixo

Plan

- Les outils de qualimétrie
- Présentation des outils
  - Vérification de règles
  - Production de métriques
  - Sécurité
- Synthèse

Sélection d'outils abordés

- Vérification de règles
  - PHPCheckstyle
  - PHP-Sat
  - PHP_CodeSniffer
  - PHP_Beautifier
  - PHPUnit
- Production de métriques (statiques)
  - Lint_php
  - SLOCCOUNT
  - PHPUnit
- Production de métriques (dynamique)
  - PHPUnit
  - PHPCoverage
- Détection de vulnérabilités (sécurité)
  - Pixy

Vérification de règles

qualixo

Spike PHPCheckstyle

http://sourceforge.net/projects/phpcheckstyle

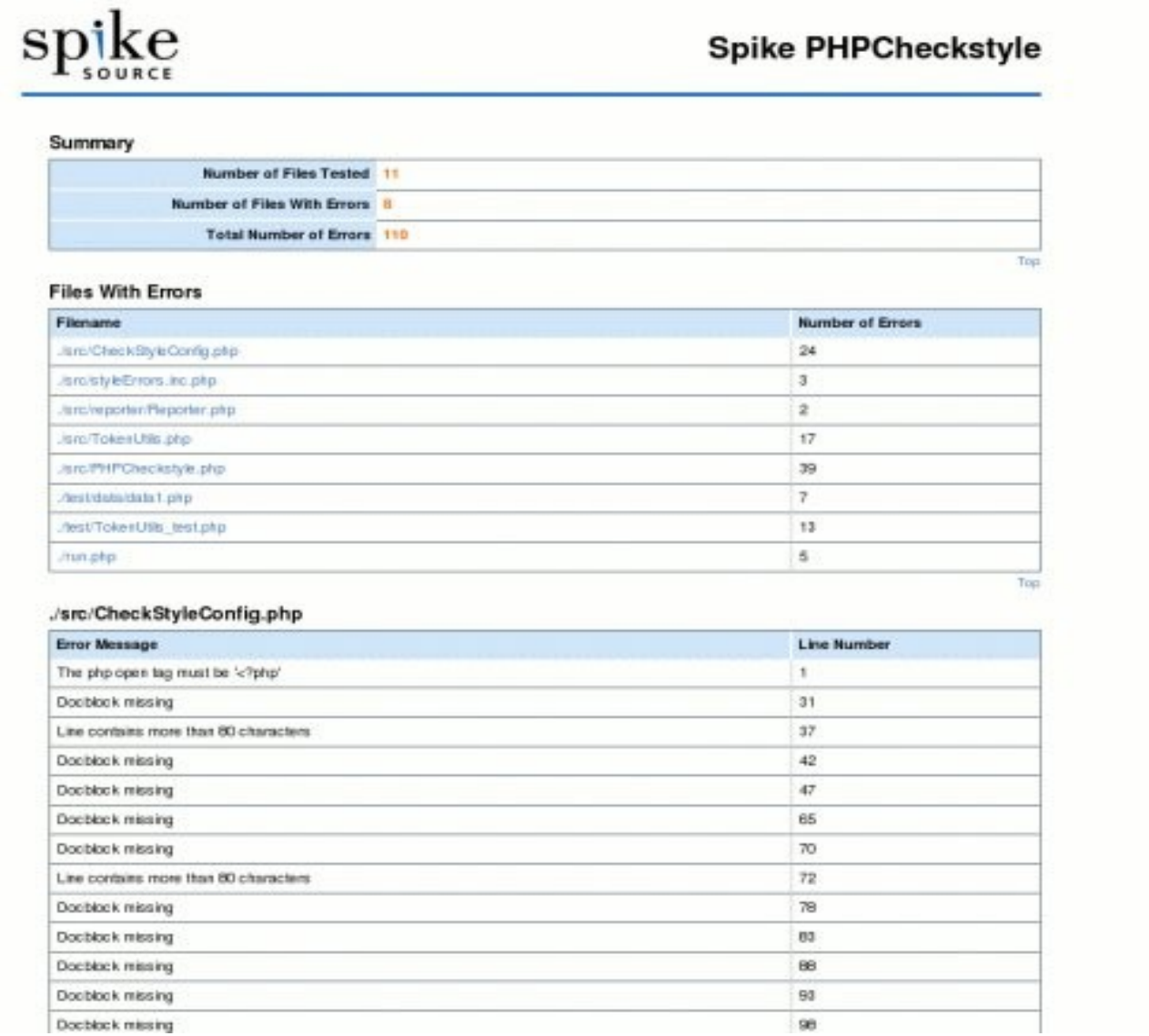
- Rules Checking PHP
  - Equivalent de l'outil CheckStyle pour Java
- Avantages

  - Facile à installer
  - Règles de mise en forme, nommage, programmation et PHPDoc
- Inconvénients

  - Outil récent (version initiale sortie en Juillet 2005)
  - Peu de feedback de la communauté Open Source

spike SOURCE

Spike PHPCheckstyle : illustration



spike SOURCE

Spike PHPCheckstyle

Summary

Number of Files Tested	11
Number of Files With Errors	8
Total Number of Errors	110

Top

Files With Errors

Filename	Number of Errors
./src/CheckStyleConfig.php	24
./src/styleErrors.inc.php	3
./src/reporter/Reporter.php	2
./src/TokenUtils.php	17
./src/PHPCheckstyle.php	39
./test/data/data1.php	7
./test/TokenUtils_test.php	13
./run.php	5

Top

./src/CheckStyleConfig.php

Error Message	Line Number
The php open tag must be '<?php'	1
Docblock missing	31
Line contains more than 80 characters	37
Docblock missing	42
Docblock missing	47
Docblock missing	65
Docblock missing	70
Line contains more than 80 characters	72
Docblock missing	78
Docblock missing	83
Docblock missing	88
Docblock missing	93
Docblock missing	98

PHP-sat

http://www.program-transformation.org/PHP/PhpSat

- Rules Checking PHP
  - Analyse statique du code pour détection de « bugs-patterns »
    - Correctness
    - Exposing Info
    - Optimization
    - Style
    - Malicious Code Vulnerability
  - Met en forme le code automatiquement
  - Permet également de détecter des failles de sécurité applicative
    - injections SQL et XSS
- Avantages
  - Couteau suisse
  - Sensibilisation à la sécurité applicative
- Inconvénients
  - Produit encore jeune (Google SoC 2006)

LGPL

PHP_CodeSniffer

http://pear.php.net/package/PHP_CodeSniffer

- Rules Checking PHP
  - Détecte les violations de convention de codage
  - Package du framework Pear

- Avantages

  - Intégré au framework Pear

- Inconvénients

  - Nombre de règle par défaut limité
  - Obligation de personnalisation
    - Plus un framwork qu'un outil

PHP_CodeSniffer : illustration

Exemple de Fichier résultat :

```
FILE: /chemin/du/code/myfile.php
----------------------------------------------------------------------
FOUND 5 ERROR(S) AND 1 WARNING(S) AFFECTING 5 LINE(S)
----------------------------------------------------------------------
2 | ERROR | Missing file doc comment
20 | ERROR | PHP keywords must be lowercase; expected "false" but found | | "FALSE"
47 | ERROR | Line not indented correctly; expected 4 spaces but found 1
47 | WARNING | Equals sign not aligned with surrounding assignments
51 | ERROR | Missing function doc comment
88 | ERROR | Line not indented correctly; expected 9 spaces but found 6
----------------------------------------------------------------------
```

PHP_Beautifier

http://pear.php.net/package/PHP_Beautifier

- Mise en forme du code source PHP
  - Met en forme le code source selon des conventions prédéfinies
  - Package du framework Pear

- Avantages

  - Intégré au framework Pear
  - Fonctionne en ligne de commande

- Inconvénients

  - Encore en version béta
    - Un certain nombre de bugs recensés

Production de métriques

qualixo

Lint_php

http://ars.altervista.org/lint_php/lint_php.php

- Calcul de métrique
  - Permet de calculer la complexité cyclomatique de McCabe
  - Outil utilisable en ligne

- Avantages

  - Calcul fiable, algorithme disponible et modifiable

- Inconvénients

  - N'analyse pas plusieurs fichiers en même temps
  - Obligation de copier/coller le code
  - Utilisation peu pratique

GPL

SLOCCount

http://www.dwheeler.com/sloccount/

- Calcul de métrique
  - Permet de calculer le nombre de lignes de code (SLOC)
  - Écrit à la base pour calculer le nombre de lignes de code du noyau Linux
  - Supporte bien plus que PHP
- Avantages
  - Fiabilité du calcul
  - Fonctionne sur de multiples langages en même temps
    - Répartition par technologie

- Inconvénients
  - Uniquement sur plate-forme Unix et apparentées
  - Une seule métrique

GPL

PHPUnit

- Calcul de métriques procédurales

http://www.phpunit.de/

  - Framework pour l'écriture de tests unitaires
  - Assure la mesure du taux de couverture des test
    - eq. PHPCoverage spike SOURCE
  - La version 3.2 permet le calcul de métriques à différents niveaux (projet, fichier, classe, méthode) tels que
    - Ligne de codes (LOC)
    - Ligne de commentaires (CLOC)
    - Complexité Cyclomatique
    - Et autres.
  - Vérifications de règles type « PMD »
- Avantages

  - Calcule un nombre important de métriques.
  - Un seul outil pour toutes les métriques (contrairement à Java où plusieurs outils sont nécessaires pour l'obtention des mêmes métriques)
- Inconvénients

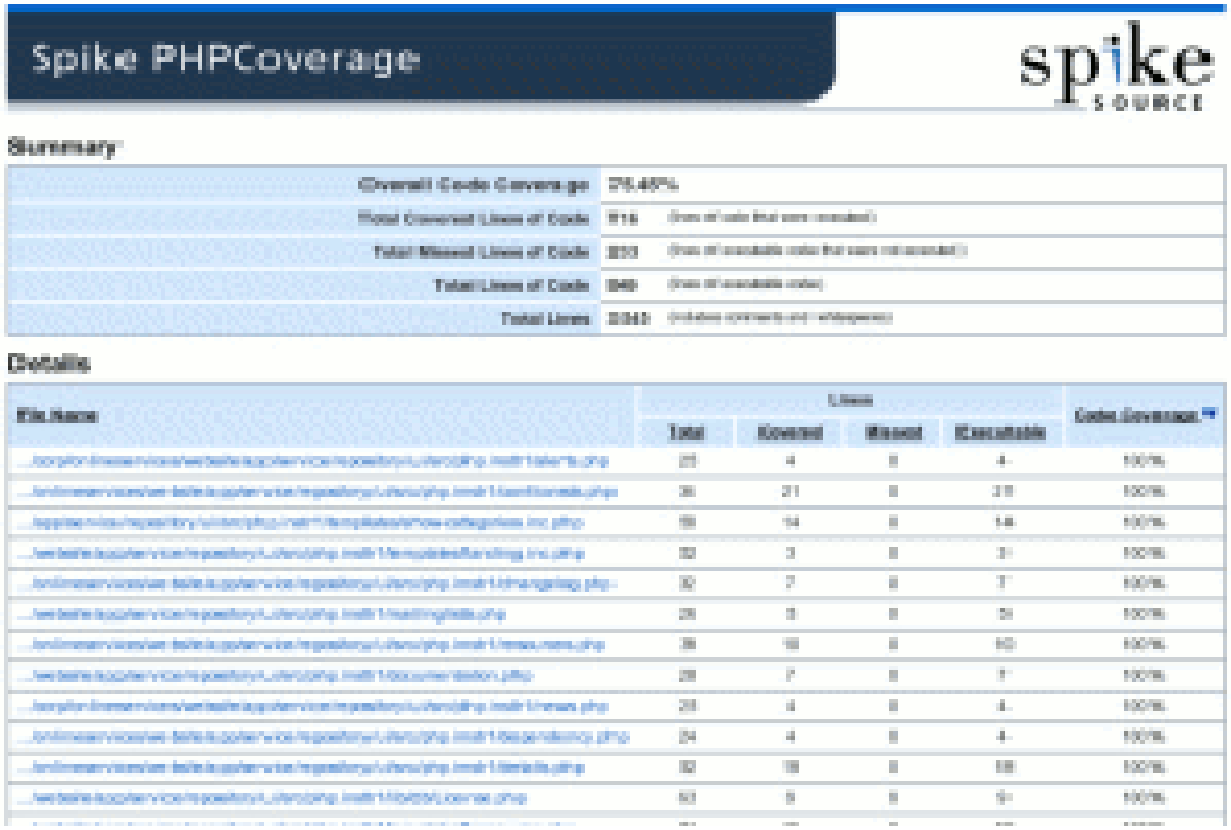
  - Calcule les métriques uniquement pour les programmes testés.
    - « Sans bonne couverture de code, les métriques ne seront pas représentatives»

PHPUnit : illustration

Exemple : code coverage

```
  82                :     /**
  83                :      * Sets the bank account's balance.
  84                :      *
  85                :      * @param  float $balance
  86                :      * @throws BankAccountException
  87                :      * @access protected
  88                :      */
  89                :     protected function setBalance($balance)
  90                :     {
  91              2 :         if ($balance >= 0) {
  92              0 :             $this->balance = $balance;
  93              0 :         } else {
  94              2 :             throw new BankAccountException;
  95                :         }
  96              0 :     }
```

Spike PHPCoverage : illustration



Détection de failles dans la sécurité

qualixo

pixy

http://pixybox.seclab.tuwien.ac.at/pixy/

- Rules Checking PHP
  - Permet de détecter des failles dans la sécurité de l'application (injections SQL et XSS)

- Avantages
  - Analyse le programme dans son ensemble
  - Rapport documenté fournit après l'analyse
- Inconvénients
  - N'analyse pas plusieurs fichiers en même temps.

  - Écrit en Java pour analyser du PHP

Résumé : outils pour Java/php

Domaine	Langage		Outil	
	Java	PHP	Java	PHP
Rules Checking	✔	✔	Checkstyle / PMD	PHP Checkstyle PHP Unit / PHP-sat
Respect architecture	✔	X	Macker	
Métriques procédurales	✔	✔	JavaNCSS / IDE	PHPUnit / Lint_php
Métriques OO	✔	X	CKJM / JDepend	
Tests	✔	✔	Junit	PHPUnit
Couverture de test	✔	✔	Cobertura/Emma	PHPUnit / PHPCoverage
Documentation	✔	✔	Javadoc ≈	PHPDocumentor
Sécurité Applicative	X	✔		PHP-sat / Pixy
Mise en forme automatique		✔	IDE	PHP-sat / PHP Beautifier