Contexte GSB

Normes de développement

Applications web écrites en PHP

Référence : GSB-STDWEBPHP

Version : 1.0

Sommaire

Table des matières

1 Introduction

Ce document s'appuie sur différentes sources de règles de codage, en particulier du projet communautaire PEAR - "PHP Extension and Application Repository"[1] et du cadre Zend Framework[2] qui fournissent entre autres des règles de codage pour les scripts PHP. Le document s'inspire aussi des règles de codage issues d'autres langages tels que Java.

Les règles énoncées par le présent document comportent au minimum :

- une **description** concise de la règle,

Si nécessaire :

- des **compléments** par rapport à la description,
- des **exemples** illustrant la règle, et éventuellement des **exceptions,**
- une partie **intérêts** en regard des critères qualité**.**

NB : La version actuelle des règles de codage ne comporte pas de règles sur les notions de POO (classe, niveau d'accès, membres d'instance ou de classe, etc.).

[1] http://pear.php.net/manual/fr/standards.php
[2] http://framework.zend.com/manual/fr/coding-standard.html

2 Fichiers

Ce paragraphe a pour but de décrire l'organisation et la présentation des fichiers mis en jeu dans un site Web dynamique écrit en PHP.

2.1 Extension des fichiers

Description

Les fichiers PHP doivent obligatoirement se terminer par l'extension **.php** pour une question de sécurité. En procédant ainsi, il n'est pas possible de visualiser le source des fichiers PHP (qui contiennent peut-être des mots de passe), le serveur web les fait interpréter par PHP.
Les fichiers qui ne constituent pas des pages autonomes (des fichiers destinés à être inclus dans d'autres pages web) se terminent par l'extension **.inc.php**.
Les fichiers contenant uniquement des définitions de fonctions se terminent par l'extension **.lib.php**.
Un fichier contenant une classe se nommera **class.<nom de la classe>.inc.php**
Les fichiers contenant des pages statiques (sans code PHP) doivent porter l'extension **.html**.

2.2 Nom des fichiers

Description

Seuls les caractères alphanumériques, tirets bas et tirets demi-cadratin ("-") sont autorisés. Les espaces et les caractères spéciaux sont interdits.

2.3 Format des fichiers

Description

Tout fichier .php ou page .html doit :
- Etre stocké comme du texte ASCII
- Utiliser le jeu de caractères UTF-8
- Etre formaté Dos

Compléments

Le << formatage Dos >> signifie que les lignes doivent finir par les combinaisons de retour chariot / retour à la ligne (CRLF), contrairement au << formatage Unix >> qui attend uniquement un retour à la ligne (LF). Un retour à la ligne est représenté par l'ordinal 10, l'octal 012 et l'hexa 0A. Un retour chariot est représenté par l'ordinal 13, l'octal 015 et l'hexa 0D.

3 Préambule XML

Description

Les pages Web doivent se conformer à une des normes HTML ou XHTML.
Toute page Web devra donc débuter par la directive <!DOCTYPE précisant quelle norme est suivie.
Elles seront validées à l'aide du validateur en ligne http://validator.w3.org

Exemple

Pour exemple, voici l'en-tête d'un fichier XHTML 1.0 :

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
       "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
```

3.1 Inclusion de scripts

L'inclusion de scripts peut être réalisée par plusieurs instructions prédéfinies en PHP : include, require, include_once, require_once. Toutes ont pour objectif de provoquer leur propre remplacement par le fichier spécifié, un peu comme les commandes de préprocesseur C `#include`.

Les instructions include et require sont identiques, hormis dans leur gestion des erreurs. include produit une alerte (warning) tandis que require génère une erreur fatale . En d'autres termes, lorsque le fichier à inclure n'existe pas, le script est interrompu. include ne se comporte pas de cette façon, et le script continuera son exécution.

La différence entre require et require_once (idem entre include et include_once) est qu'avec **require_once()**, on est assuré que le code du fichier inclus ne sera ajouté qu'une seule fois, évitant de ce fait les redéfinitions de variables ou de fonctions, génératrices d'alertes.

Description

L'inclusion de scripts sera réalisée à l'aide de l'instruction require_once lorsque les fichiers inclus contiennent des bibliothèques, require sinon.

Exemple

Script prem.inc.php

```
<?php
function uneFonction () {
      echo "Fonction définie dans prem.inc.php <br />";
}
?>
```

Script second.inc.php

```
<?php
require_once("prem.inc.php");
uneFonction();
echo "Pas de problème : uneFonction n'a pas été redéfinie 2 fois. Merci
require_once ! <br />";
?>
```

Script monscript.php

```
<?php
require_once(prem.inc.php);
require_once(second.inc.php);
echo "Tout va bien ! <br />";
?>
```

4 Présentation du code

4.1 Tag PHP

Description

Toujours utiliser `<?php ?>` pour délimiter du code PHP, et non la version abrégée `<? ?>`. C'est la méthode la plus portable pour inclure du code PHP sur les différents systèmes d'exploitation et les différentes configurations.

Intérêts

Portabilité

4.2 Séparation PHP/ HTML

Description

Les balises HTML doivent se situer au maximum dans les sections HTML et non incluses à l'intérieur du texte des messages de l'instruction d'affichage echo.

Exemples

Ne pas écrire

```
<?php
    echo "<select id=\"lstAnnee\" name=\"lstAnnee\">";
    $anCours = date("Y");
    for ( $an = $anCours – 5 ; $an <= $anCours + 5 ; $an++ ) {
        echo "<option value=\"" . $an ."\">" . $an . "</option>";
    }
    echo "</select>";
?>
</select>
```

Mais écrire

```
<select id="lstAnnee" name="lstAnnee">
<?php
    $anCours = date("Y");
    for ( $an = $anCours – 5 ; $an <= $anCours + 5 ; $an++ ) {
?>
       <option value="<?php echo $an ; ?>">echo $an; ?></option>
<?php
    }
?>
</select>
```

Intérêts :

Dans les sections HTML, l'éditeur de l'outil de développement applique la coloration syntaxique sur les balises et attributs HTML. Ceci accroît donc la lisibilité et la localisation des erreurs de syntaxe au niveau du langage HTML. Il est aussi plus aisé d'intervenir uniquement sur la présentation, sans effet de bord sur la partie dynamique.

Maintenabilité : lisibilité

Portabilité : indépendance

4.3 Caractères et lignes

Description

Chaque ligne doit comporter au plus une instruction.
Les caractères accentués ne doivent pas être utilisés dans le code source, excepté dans les commentaires et les messages texte.
Un fichier source ne devrait pas dépasser plus de **500 lignes**.

Exemples

Ne pas écrire

```
$i-- ; $j++ ;
```

Mais écrire

```
$i-- ;
$j++ ;
```

Intérêts

Maintenabilité : lisibilité et clarté du code.

4.4 Indentation et longueur des lignes

Description

Le pas d'indentation doit être **fixe** et correspondre à **4 caractères.** Ce pas d'indentation doit être paramétré dans l'éditeur de l'environnement de développement. L'indentation est stockée dans le fichier sous forme de 4 caractères espace (sans tabulation réelle).

Il est recommandé que la longueur des lignes ne dépasse pas 75 à 85 caractères.
Lorsqu'une ligne d'instruction est trop longue, elle doit être coupée après une virgule ou avant un opérateur. On alignera la nouvelle ligne avec le début de l'expression de même niveau de la ligne précédente.

Exemples

Exemple 1 : découpage d'un appel de fonction

On découpe la ligne après une virgule :

```
$maVar = fonctionA(expressionLongue1, expressionLongue2,
                   fonctionB(expressionLongue3,
                             expressionLongue4));
```

Exemple 2 : découpage d'une expression arithmétique

La ligne est découpée avant un opérateur :

```
$maVar = expressionLongue1 * expressionLongue2
         + expressionLongue3 - expressionLongue4
```

Exemple 3 : découpage d'une expression conditionnelle

La ligne est découpée avant un opérateur :

```
if(((condition1 && condition2) || (condition3 && condition4))
        && !(condition5 && condition6)) {
    doSomething();
}
```

Intérêts

Maintenabilité : lisibilité.

4.5 Espacement dans les instructions

Description

- Un mot-clé suivi d'une parenthèse ouvrante doit être séparé de celle-ci par un espace. Ce n'est pas le cas entre un identificateur de fonction et la parenthèse ouvrante.
- Tous les opérateurs binaires, sauf l'opérateur « -> » doivent être séparés de leurs opérandes par un espace.
- Les opérateurs unaires doivent être accolés à leur opérande.

Exemples :

```
. while (true) {
      ...
  }

. $totalTTC = $totalHT + ($totalHT * ($tauxTVA / 100));
  $totalTTC = round($totalTTC, 2);
  $existe = $unElt->hasAttribute();

. $nb = 0;
  $fin = false;
  while (!$fin) {

  ...  $nb++;
  }

. for ($nbLignes = 1; $nbLignes < 4; $nbLignes++) {

  }
```

Intérêts

Maintenabilité : lisibilité

4.6 Présentation des blocs logiques

Description

1. Chaque bloc logique doit être délimité par des accolades, même s'il ne comporte qu' une seule instruction (cf. exemple 1),

2. Dans une instruction avec bloc, l'accolade ouvrante doit se trouver sur la fin de la ligne de l'instruction ; l'accolade fermante doit débuter une ligne, et se situer au même niveau d'indentation que l'instruction dont elle ferme le bloc (cf. exemple 2),

3. Les instructions contenues dans un bloc ont un niveau supérieur d'indentation.

Exemples

Exemple 1 :

Ne pas écrire

```
if ($prime > 2000)
    $prime = 2000;
```

Mais écrire

```
if ($prime > 2000) {
    $prime = 2000;
}
```

Exemple 2 : écriture des instructions avec blocs :

Structures de contrôle conditionnelles

```
if (...) {
    ...
} elseif (...) {
    ...
} else {
    ...
}
switch (...) {
    case ... :
        ...
    case ... :
        ...
    default :
        ...
}
```

Définition de fonction

```
function uneFonction() {
    ...
}
```

Structures de contrôle itératives

```
for (...; ...; ...) {
    ...
}
while (...) {
    ...
}
do {
    …
}while (...);
```

Intérêts

La présence d'accolades ainsi que l'indentation facilitent la localisation des débuts et fins de blocs et réduit le risque d'erreur logique lors de l'ajout de nouvelles lignes de code.

Maintenabilité : lisibilité.

4.7 Appels de fonctions / méthodes

Description

Les fonctions doivent être appelées sans espace entre le nom de la fonction, la parenthèse ouvrante, et le premier paramètre ; avec un espace entre la virgule et chaque paramètre et aucun espace entre le dernier paramètre, la parenthèse fermante et le point virgule.
Il doit y avoir un espace de chaque côté du signe égal utilisé pour affecter la valeur de retour de la fonction à une variable. Dans le cas d'un bloc d'instructions similaires, des espaces supplémentaires peuvent être ajoutés pour améliorer la lisibilité.

Exemples

```
<?php
$total = round($total, 2);
?>

<?php
$courte         = abs($courte);
$longueVariable = abs($longueVariable);
?>
```

Intérêts

Maintenabilité : lisibilité

4.8 Définition de fonctions

Description

Les fonctions définies à usage exclusif d'un script seront définies en début du script.
La déclaration des fonctions respecte l'indentation classique des accolades.
Les arguments possédant des valeurs par défaut vont à la fin de la liste des arguments.

Exemples

```
<?php
function maFonction($arg1, $arg2 = '') {
    if (condition) {
        statement;
    }
    return $val;
}
?>
```

5 Documentations et commentaires

5.1 Introduction

La documentation est essentielle à la compréhension des fonctionnalités du code . Elle peut être intégrée directement au code source, tout en restant aisément extractible dans un format de sortie tel que HTML ou PDF. Cette intégration favorise la cohérence entre documentation et code source, facilite l'accès à la documentation, permet la distribution d'un code source auto-documenté. Elle rend donc plus aisée la maintenance du projet.

L'intégration de la documentation se fait à travers une extension des commentaires autorisés par le langage PHP. Nous utiliserons celle proposée par l'outil PHPDocumentor, dont les spécifications sont disponibles à l'URL http://www.phpdoc.org/.

Pour rappel, les commentaires autorisés par le langage PHP adoptent une syntaxe similaire aux langages C et C++ (`/* ... */` et `//`). Ils servent à décrire en langage naturel tout élément du code source.

L'extension de l'outil PHPDocumentor est la suivante `/** ... */`. Leur utilisation permettra de produire une documentation dans un ou plusieurs formats de sortie tels que HTML, XML, PDF ou CHM.

La syntaxe spécifique à l'outil PHPDocumentor sera utilisée au minimum pour les entêtes de fichiers source et les entêtes de fonctions. Des éléments sur l'installation, les spécifications et l'utilisation de l'outil PHPDocumentor sont fournis en annexe 1.

5.2 Entêtes de fichier source

Description

Chaque fichier qui contient du code PHP doit avoir un bloc d'entête en haut du fichier qui contient au minimum les balises phpDocumentor ci-dessous.

Compléments

Format d'entête de fichier source :

```
<?php
/**
 * Description courte des fonctionnalités du fichier

 * Description longue des fonctionnalités du fichier  si nécessaire
 * @author nom de l'auteur
 * @package default
 */
```

5.3 Entêtes de fonction

Description

Toute définition de fonction doit être précédée du bloc de documentation contenant au minimum :

- Une description de la fonction
- Tous les arguments
- Toutes les valeurs de retour possibles

Compléments

Format d'entête de fonction :

```
/**
 * Description courte de la fonction.

 * Description longue de la fonction (si besoin)
 * @param type nomParam1 description
 * ...
 * @param type nomParamn description
 * @return type description
 */
function uneFonction($nomParam1, ...) {
```

Exemple

```
/**
 * Fournit le compte utilisateur d'une adresse email.

 * Retourne le compte utilisateur (partie identifiant de la personne) de
 * l'adresse email $email, càd la partie de l'adresse située avant le
 * caractère @ rencontré dans la chaîne $email. Retourne l'adresse complète
 * si pas de @ dans $email.
 * @email string adresse email
 * @return string compte utilisateur
 */
function extraitCompteDeEmail ($email) {
  ...
}
```

5.4 Commentaires des instructions du code

Description

Il existe deux types de commentaires :
1. les commentaires mono ligne qui inactivent tout ce qui apparaît à la suite, sur la même ligne : //
2. les commentaires multi-lignes qui inactivent tout ce qui se trouve entre les deux délimiteurs, que ce soit sur une seule ligne ou sur plusieurs /* */

Il est important de ne réserver les commentaires multi-lignes qu'aux blocs utiles à PHPDocumentor et à l'inactivation de portions de code.
Les commentaires mono-ligne permettant de commenter le reste, à savoir, toute information de documentation interne relative aux lignes de code. Ceci afin d'éviter des erreurs de compilation dues aux imbrications des commentaires multi-lignes.

Exemples

- Insertion d'un commentaire mono-ligne pour expliquer le comportement d'un code

Exemple 1 :

```
function extraitCompteDeEmail ($email) {
    // le traitement se fait en 2 temps : recherche de la position $pos dans
    // l'adresse de l'occurrence du caractère @, puis si @ présent,
    // extraction du morceau de chaîne du 1er caractère sur $pos caractères
    $pos = strpos($email, "@");
    if ( is_integer($pos) ) {
        $res = substr($email, 0, $pos);
    }
    else {
        $res = $email;
    }
    return $res;
}
```

Exemple 2 :

```
// page inaccessible si visiteur non connecté
if (!estVisiteurConnecte()) {
    header("Location: cSeConnecter.php");
}

// acquisition des données reçues par la méthode post
$mois = lireDonneePost("lstMois", "");
$etape = lireDonneePost("etape","");
```

- Inactivation d'une portion de code pour débogage

```
/*
// page inaccessible si visiteur non connecté
if (!estVisiteurConnecte()) {
    header("Location: cSeConnecter.php");
}
*/
```

6 Nommage des identificateurs

Cette convention concerne les éléments suivants du langage :

- les fonctions,
- les paramètres formels de fonctions,
- les constantes,
- les variables globales à un script,
- les variables locales,
- les variables de session.

Pour l'ensemble de ces éléments, la clarté des identificateurs est conseillée. Le nom attribué aux différents éléments doit être aussi explicite que possible, c'est un gage de compréhension du code.

6.1 Nommage des fonctions

Description

L'identificateur d'une fonction est un verbe, ou groupe verbal.
Les noms de fonctions ne peuvent contenir que des caractères alphanumériques. Les tirets bas ("_") ne sont pas permis. Les nombres sont autorisés mais déconseillés.
Les noms de fonctions doivent toujours commencer avec une lettre en minuscule. Quand un nom de fonction est composé de plus d'un seul mot, la première lettre de chaque mot doit être mise en majuscule. C'est ce que l'on appelle communément la "notationCamel".

Exemples :
`filtrerChaineBD(), verifierInfosConnexion(),estEntier()`

Intérêts

Maintenabilité : lisibilité.

6.2 Nommage des constantes

Description

Les constantes doivent être déclarées grâce à la commande **define()** en utilisant un nom réellement significatif. Les constantes peuvent contenir des caractères alphanumériques et des tirets bas. Les nombres sont autorisés.
Les constantes doivent toujours être en majuscules, les mots séparés par des '_'.

On limitera l'utilisation des constantes littérales (nombre ou chaîne de caractères) dans les traitements.

Exemples

```
define("TYPE_USER_ADMIN", "ADM")
// définit la constante de nom TYPE_USER_ADMIN et de valeur ADM
```

Exceptions

Les constantes numériques -1, 0, 1 peuvent toutefois être utilisées dans le code.

Intérêts

Maintenabilité : lisibilité.

6.3 Nommage des variables et paramètres

Description

L'identificateur d'une variable ou paramètre indique le rôle joué dans le code ; c'est en général un nom, ou groupe nominal. Il faut éviter de faire jouer à une variable plusieurs rôles.
Les noms de variables et paramètres ne peuvent contenir que des caractères alphanumériques. Les tirets bas sont autorisés uniquement pour les membres privés d'une classe. Les nombres sont autorisés mais déconseillés.

Comme les identificateurs de fonctions, les noms de variables et paramètres adoptent la notation Camel.

Exemples :
`$nomEtud, $login`

Intérêts

Maintenabilité : lisibilité.

7 Algorithmique

7.1 Fonctions/méthodes

7.1.1 Modularité

Description

Le codage doit être réalisé en recherchant le plus possible la modularité :
- chaque fonction doit réaliser un et un seul traitement,
- chaque fonction doit être construite de manière à posséder la plus forte cohésion et la plus grande indépendance possible par rapport à son environnement.

Intérêts

Maintenabilité et fiabilité : modularité.

7.1.2 Nombre de paramètres des fonctions

Description

Les fonctions ne doivent pas comporter un trop grand nombre de paramètres. La limite de 5 à 6 paramètres est recommandée. Tout dépassement de cette limite doit être justifié.

Compléments

Cette règle s'applique, tout spécialement, dans le cadre de la programmation par objets qui permet justement de réduire le nombre de paramètres des fonctions.

Intérêts

Maintenabilité : lisibilité.

7.2 Instructions

7.2.1 Écriture des instructions d'affectation

Description

Il faut utiliser dès que possible les formes abrégées des instructions d'affectation.

Compléments

Les instructions d'affectation du type :

```
A = A <op> <exp> ;
```

peuvent être notées sous leur forme abrégée :

```
A <op>= <exp> ;
```

Exemples

Écrire

```
$total *= 0.90;
```

au lieu de

```
$total = $total * 0.90;
```

7.2.2 Parenthésage des expressions

Description

Il est recommandé d'utiliser les parenthèses à chaque fois qu'une expression peut prêter à confusion.

Exemples

Il ne faut pas écrire ...

```
if ($nbLignes == 0 && $nbMots == 0)
```

...mais plutôt écrire

```
if (($nbLignes == 0) && ($nbMots == 0))
```

Intérêts

L'ajout de parenthèses dans les expressions comportant plusieurs opérateurs permet d'éviter des confusions sur leur priorité.

Maintenabilité : lisibilité.

7.2.3 Interdiction des instructions imbriquées

Description

Les instructions imbriquées doivent être évitées quand cela est possible. En particulier, les types d'instructions imbriquées suivantes sont à bannir :

- affectations dans les conditions, dans les appels de fonctions et dans les expressions ;
- affectations multiples.

Compléments

Une expression ne doit donc contenir que :

- des variables,
- des constantes,
- des appels de fonctions dont les arguments ne sont pas eux-mêmes des éléments variables.

Exemples

Éviter les affectations dans les conditions :

```
while ($ligne = mysql_fetch_assoc($idJeu))
if ($nb++ != 20)
```

Éviter les affectations dans les appels de fonctions :

```
uneFonction($nb = rand(10,20), $qte);
```

Éviter les affectations dans les expressions :

```
$a = ($b = $c--) + $d;
```

Éviter les affectations multiples :

```
$a = $b = $c = $i++;
```

Intérêts

La complexité des expressions peut donner lieu à des erreurs d'interprétation. Par exemple, l'affectation dans une condition peut être lue comme un test d'égalité.

Maintenabilité : lisibilité.

7.2.4 Limitation de l'utilisation des *break* et *continue* dans les itératives

Description

Utilisation modérée
Les ruptures de séquence `break` et `continue` doivent être utilisées avec modération dans les itératives.

Compléments

L'abus de ce type d'instructions peut rendre le code difficile à comprendre. Elles pourront toutefois être utilisées ponctuellement. Dans ce cas, un commentaire devra le signaler.

Intérêts

Limiter les instructions `break` et `continue` améliore la structuration du code. Ces instructions (qui sont des "goto" déguisés), lorsqu'elles sont utilisées fréquemment, peuvent en effet dénoter une mauvaise analyse des conditions d'itérations dans certains cas.

7.2.5 Écriture des *switch*

Description

- Tout le contenu à l'intérieur de l'instruction "switch" doit être indenté avec 4 espaces. Le contenu sous chaque "case" doit être indenté avec encore 4 espaces supplémentaires.
- Les structures `switch` doivent obligatoirement comporter une clause `default`.
- Le niveau d'imbrication des `switch` ne doit pas dépasser 2.
- Chaque cas ou groupe de cas doit se terminer normalement par une instruction break. Les cas ne se terminant par un saut **break** doivent spécifier un commentaire rappelant que l'exécution se poursuit.
- L'instruction break est obligatoire à la fin du cas par défaut. Cela est redondant mais protège d'une erreur en cas de rajout d'autres cas par la suite.

Compléments

```
switch (choix) {
    case expression1 :
        instructions
        /* pas de break */
    case expression2 :
    case expression3 :
        instructions
        break;
    default :
        instructions;
        break;
}
```

Intérêts

Fiabilité : robustesse, clarté.

7.2.6 Utilisation de l'opérateur ternaire conditionnel

Description

1. Il faut éviter d'utiliser l'abréviation « `? :` » du « `if ... else` », sauf si les conditions suivantes sont réunies (cf. exemple) :
   - la valeur de l'expression conditionnelle est effectivement utilisée (dans un retour ou un appel de fonction, une affectation, etc.),
   - les 3 opérandes ne sont pas trop complexes.
2. Si toutefois on utilise cet opérateur, il faut mettre la condition (placée avant le « ? ») entre parenthèses.

Compléments

Exemple

Le cas suivant...

```
if ($a > $b) {
    $maxi = $a;
} else {
    $maxi = $b;
}
```

...se prête bien à l'utilisation de l'opérateur conditionnel ternaire

```
$maxi = ($a > $b) ? $a : $b;
```

En effet, on utilise la valeur de l'expression conditionnelle et les opérandes ne sont pas trop complexes.

Intérêts

Maintenabilité : lisibilité.

8 Gestion des formulaires HTML

8.1 Nommage des formulaires et des champs de formulaires

Description

Les noms des éléments HTML débuteront par un préfixe rappelant leur type.
Les préfixes retenus concernent les formulaires et les champs contenus dans les formulaires.

Type d'élément	Préfixe
Formulaire	`frm`
Zone de texte mono_ligne (text, password) / multi_lignes	`txt`
Champ caché	`hd`
Bouton d'option (bouton radio)	`opt`
Case à cocher	`chk`
Zone de liste	`lst`
Bouton de type reset	`br`
Bouton de type button	`bt`
Bouton de type submit	`cmd`

8.2 Méthodes de soumission des formulaires

Les méthodes de soumission d'un formulaire sont au nombre de 2 : GET et POST. La première véhicule les noms et valeurs des champs dans l'URL de la requête HTTP, la seconde dans le corps de la requête HTTP.

Description

La méthode POST est à préférer pour des raisons de taille de données et de confidentialité. A noter que la confidentialité se résume ici à ne pas voir apparaître les noms et valeurs de champs dans la zone d'adresse du navigateur : les données sont, dans les 2 cas, transmises en clair sur le réseau dans le cas où le protocole applicatif utilisé reste HTTP.

Le choix de la méthode GET peut cependant se justifier s'il est souhaitable de pouvoir conserver les différentes soumissions d'un formulaire en favoris.

8.3 Variables superglobales $_GET, $_POST

Les valeurs saisies dans un formulaire sont mises à disposition des scripts PHP dans les tableaux associatifs superglobaux $_GET et $_POST. Le tableau $_GET contient également les valeurs transmises via la constitution d'un lien.

Description

Au cours de la mise au point des scripts, il est recommandé d'appeler la fonction var_dump sur ces tableaux $_GET et $_POST afin d'apprécier réellement les données (nom et valeur) reçues.
De plus, pour éviter de se référer dans tout le script soit au tableau $_GET, soit au tableau $_POST, tout script PHP affectera initialement les éléments des deux tableaux dans des variables. Ceci permettra également de migrer facilement d'une méthode de soumission POST vers GET ou vice-versa.

On pourra définir des fonctions spécialisées afin de récupérer les valeurs des éléments à partir d'un tableau ou d'un autre, en prévoyant des valeurs par défaut en cas d'inexistence d'un élément.

Exemples

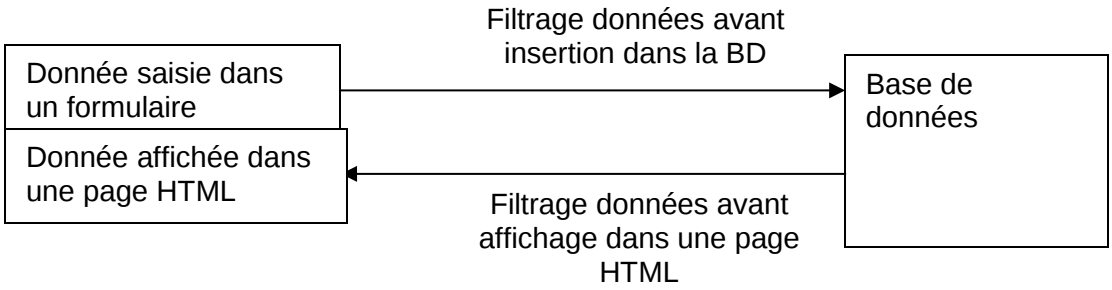
```
// acquisition des données reçues par la méthode post
$mois = $_POST["lstMois"];
$etape = $_POST["etape"];
// à commenter après débogage
var_dump($_GET, $_POST);
```

9 Eléments de sécurité sur la protection des données

9.1 Introduction

Toute donnée saisie à l'aide d'un formulaire peut engendrer des dysfonctionnements, que ce soit lors de l'enregistrement dans la base de données ou lors de son affichage ultérieur dans une page HTML.

Ces dysfonctionnements sont dus à l'interprétation de certains caractères dits spéciaux, soit par le SGBDR, soit par le navigateur. Il est donc nécessaire d'annuler les effets de ces caractères spéciaux en traitant les données d'une part avant de les insérer dans la base de données et d'autre part, avant de les restituer dans une page HTML.



9.2 Protection des données avant insertion dans la base de données

9.2.1 Comment protéger les données ?

Certains caractères spéciaux ont une signification précise pour le SGBDR. Il en est ainsi du guillemet simple ' qui a pour rôle de délimiter une valeur chaîne au sein d'une requête SQL.

Il n'est pourtant pas exclu que ce caractère se trouve dans une valeur chaîne, en particulier dans les noms de famille et surtout dans des champs commentaires. Le rôle du guillemet simple doit donc être annulé avant d'être inclus dans une requête SQL, sous peine de provoquer un refus d'exécution de la part du moteur SGBDR.

D'autre part, l'absence de traitement de ce caractère spécial laisse la porte ouverte à des attaques par injection SQL.

Toute valeur alphanumérique à enregistrer dans la base doit faire l'objet d'un traitement des caractères spéciaux. Ce traitement consiste à ajouter le caractère d'échappement \ devant chaque caractère spécial pour imposer que le caractère doit être interprété comme un caractère normal.

Certaines fonctions PHP prédéfinies tq *addslashes* ou *mysql_real_escape_string* prennent en charge ce traitement.

Il faut aussi noter que la directive PHP *magic_quotes_gpc* présente dans le fichier php.ini peut prendre les valeurs On ou Off : elle permet de gérer automatiquement ou non l'appel à la fonction *addslashes* sur toutes les données GET, POST et COOKIE. Il ne faut donc pas appeler la fonction *addslashes* sur des données déjà protégées avec la directive *magic_quotes_gpc* sinon les protections seront doublées.

La fonction *get_magic_quotes_gpc* est utile pour vérifier la valeur de la directive magic_quotes_gpc.

Afin d'être indépendant de cette directive de configuration (dont la valeur peut varier suivant les environnements), il est recommandé de définir une fonction utilitaire *filtrerChainePourBD* testant cette directive et échappant une chaîne si besoin.

9.2.2 Fabrication d'une requête SQL sécurisée

Description

La fonction utilitaire filtrerChainePourBD doit être appelée sur toute valeur alphanumérique avant d'être insérée dans la base de données.

Exemple de fabrication d'une requête sécurisée :

```
<?php
$query = "SELECT * FROM users";
$query .= " WHERE user='" . filtrerChainePourBD($user) . "'";
$query .= " AND password = " . filtrerChainePourBD($password) . "'";
?>
```

9.3 Protection des données d'une page HTML

9.3.1 Comment protéger les données d'une page HTML ?

Le langage HTML est fondé sur la notion de balises marquées par les caractères < et >. La valeur des attributs d'une balise est délimitée par des guillemets simples ou doubles.

C'est le rôle du navigateur d'interpréter ces balises pour générer la présentation attendue de la page. Les données elles-mêmes doivent donc être exemptes de ces caractères réservés pour éviter une interprétation erronée de la page.

Exemple 1 : La valeur du champ txtComment suivant :

<input type="text" name="txtComment" value="Bonjour "Dupont"">

sera tronquée par le navigateur : la valeur initiale du champ txtComment sera Bonjour.

Exemple 2 : La valeur du champ txtComment suivant.

<input type="text" name="txtComment" value="<script> while (true) alert('Erreur'); </script>">

sera interprétée comme une séquence de script et provoquera indéfiniment l'affichage d'une boîte message. Le navigateur lui-même devra être arrêté.

Pour éviter ces effets néfastes, ces caractères réservés doivent être traduits en symboles nommés HTML (aussi appelés entités HTML). Ainsi, le caractère < doit être transformé en <, > en > , etc.

La fonction PHP prédéfinie *htmlspecialchars* prend en charge ce traitement.

`string` **htmlspecialchars** (`string string` , *`int quote_style`* , *`string charset`*)

Les remplacements effectués sont :

- " & " (et commercial) devient " `&` "
- " " " (guillemets doubles) devient " `&quot;` " lorsque `ENT_NOQUOTES` n'est pas utilisé.
- " ' " (single quote) devient " `&#039;` " uniquement lorsque `ENT_QUOTES` est utilisé.
- " < " (supérieur à) devient " `<` "
- " > " (inférieur à) devient " `>` "

Les guillemets simples et doubles ne sont pas systématiquement traduits : cela dépend de la valeur du paramètre optionnel quote_style.
`ENT_COMPAT` , la constante par défaut, va convertir les guillemets doubles, et ignorer les guillemets simples; `ENT_QUOTES` va convertir les guillemets doubles et les guillemets simples; `ENT_NOQUOTES` va ignorer les guillemets doubles et les guillemets simples.

Exemple :

```
<?php
$new = htmlspecialchars("<a href='test'>Test</a>", ENT_QUOTES);
echo $new;
// <a href=&#039;test&#039;>Test</a>
?>
```

9.3.2 Fabrication d'une page HTML sécurisée

Description

La fonction *htmlspecialchars* doit être appelée sur toute valeur en provenance de la base de données avant d'être affichée dans une page HTML. On l'appellera avec pour second argument la constante ENT_QUOTES pour convertir à la fois les guillemets doubles et simples.

10 Configuration du fichier php.ini

Description

Afin de favoriser la détection des erreurs, ainsi que la portabilité d'une configuration PHP à une autre, il est obligatoire de réaliser le développement d'une application Web avec certaines directives de configuration PHP affectées aux valeurs recommandées suivantes.

Nom de la directive	**Description**	**Valeur imposée**
short_open_tag	Définit si les balises courtes d'ouverture de PHP (<? ?>) sont autorisées ou non.	Off
output_buffering	Définit l'activation ou non de la bufferisation de sortie. L'activation de la buffferisation peut être autorisée moyennant d'être dûment justifiée.	Off
error_reporting	Fixe le niveau d'erreur. Ce paramètre est un entier, représentant un champ de bits. Cette directive est renseignée en utilisant les types d'erreurs définis sous forme de constantes et en utilisant les opérateurs bits à bits & (ET), | (OU), ~ (SAUF), de même que l'opérateur booléen ! (SAUF). Le rapport d'erreur de niveau **E_NOTICE** (inclus dans **E_ALL)** durant le développement a des avantages. En terme de déboguage, les message d'alertes signalent des bogues potentiels dans le code. Par exemple, l'utilisation de valeurs non initialisées est signalée. Comme **E_STRICT,** nouveau niveau d'erreur introduit en PHP5, n'est pas inclus sans **E_ALL,** il faut explicitement l'ajouter. Il permet d'être alerté de l'utilisation de fonctions non recommandées.	E_ALL | E_STRICT

Compléments

Les directives de configuration PHP peuvent être appliquées à 3 niveaux :

- à l'ensemble des applications Web d'un serveur Web par le biais du fichier php.ini,
- à l'ensemble des scripts PHP d'un répertoire par le biais d'un fichier caché situé dans ce répertoire et analysé par le serveur Web (directive php_flag du fichier .htaccess analysé par Apache),
- à un seul script PHP par le biais de l'appel de la fonction ini_set.

Intérêts

Portabilité : indépendance du logiciel par rapport à son environnement

Fiabilité : robustesse

Annexe 1 – Eléments sur l'outil PHPDocumentor[3]

PHP Documentor est un outil de génération automatique de documentation à partir des commentaires inclus dans les programmes PHP.
PHPDocumentor eut être utilisé soit via la ligne de commande, soit via une interface web.

Le téléchargement de l'archive de l'outil PHP Documentor se fait là :
http://sourceforge.net/projects/phpdocu/files/

Pour installer phpDocumentor, il faut décompresser l'archive dans un répertoire en respectant la structure interne des dossiers. L'utilisation de l'interface web implique de décompresser l'archive dans un dossier accessible par le serveur Web. Dans la suite du document, nous considérons que ce dossier se nomme *phpdoc*.

Les blocs de commentaires

Format d'un bloc de commentaires

La documentation exploitée par PHPDocumentor doit se trouver dans un bloc de commentaires respectant le format suivant :

```
/**
 * Mes explications ...
 */
```

Ce bloc de commentaires est un bloc de commentaires étendu qui commence par un "/**" et présente un "*" au début de chaque ligne. Les blocs de commentaires précèdent les éléments qu'ils documentent.

Toute ligne dans un bloc de commentaires qui ne commence pas par un « * » sera ignorée.

Contenu d'un bloc de commentaires

Un bloc de commentaires contient trois segments de base dans l'ordre suivant :

- une **description courte** : débute sur la première ligne, et peut se terminer par un point ou une ligne blanche.
- une **description longue** : peut occuper autant de lignes que nécessaire.
- des **marqueurs** : des mots préfixés par le caractère @. Ils informent phpDocumentor sur la façon d'afficher la documentation. Tous les marqueurs sont optionnels, mais ils doivent respecter une syntaxe spécifique pour être interprétés correctement.

Voici quelques marqueurs à utiliser :

- @**author** : nom de l'auteur
- @**param** : type, nom et description d'un paramètre
- @**return** : type et description du résultat retourné par une fonction
- @**see** : nom d'un autre élément documenté, produisant un lien vers celui-ci
- @**link** : url
- @**todo** : changements à faire dans le futur

3 Référence site officiel : www.phpdoc.org

Eléments de code à documenter

Plusieurs éléments de code peuvent être documentés : des fichiers, des fonctions, des classes, des méthodes, des propriétés, des variables globales, des constantes.

Nous présentons ci-après un exemple concernant les fonctions.

Une fonction est caractérisée par :

- son nom
- son type et sa valeur de retour (@return)
- ses paramètres (@param)
- sa description

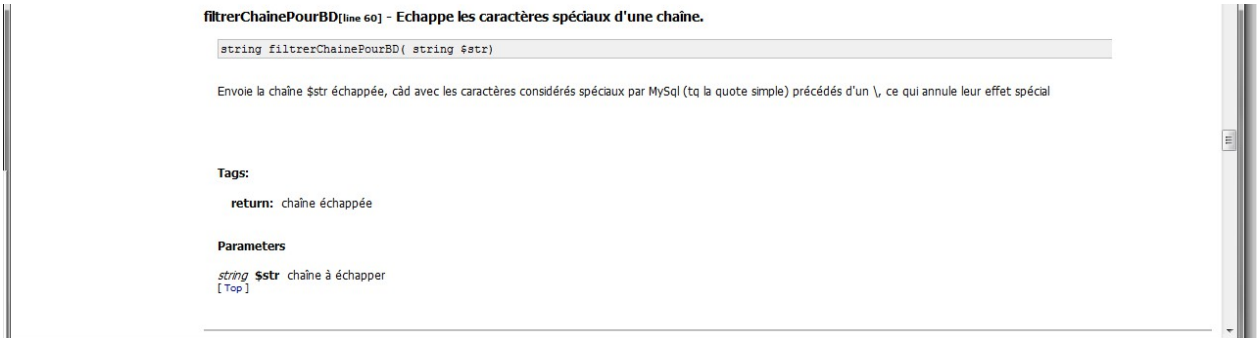
Il est donc possible de la documenter ainsi :

```
/**
 * Echappe les caractères spéciaux d'une chaîne.

 * Envoie la chaîne $str échappée, càd avec les caractères considérés
 * spéciaux par MySql (tq la quote simple) précédés d'un \, ce qui annule
 * leur effet spécial

 * @param string $str chaîne à échapper
 * @return string
 */
function filtrerChainePourBD($str) {
  if ( ! get_magic_quotes_gpc() ) {
      $str = mysql_real_escape_string($str);
  }
  return $str;
}
```

On peut ajouter autant de lignes @param qu'il y a de paramètres.
En utilisant le template HTML:Smarty:PHP, on obtient l'extrait suivant dans la page HTML produite par l'outil phpDocumentor :

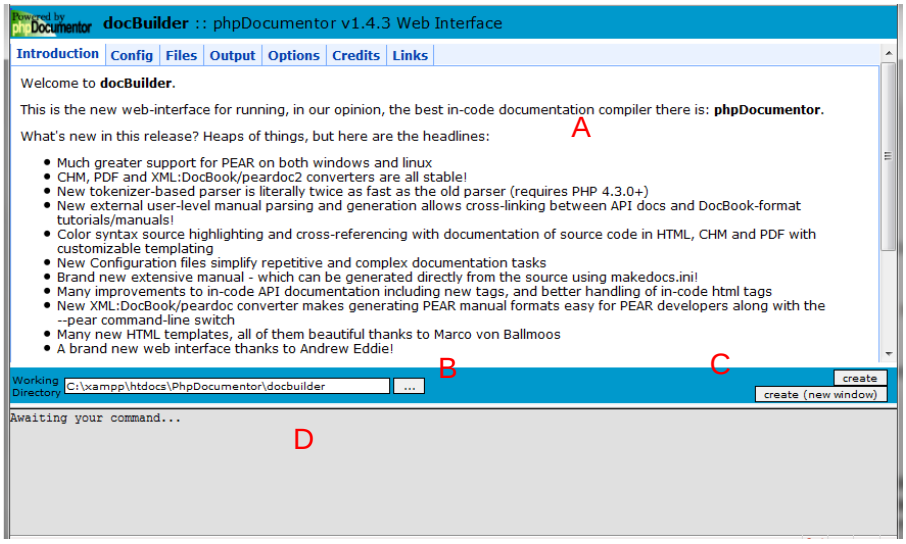


Génération de la documentation

La génération portera d'une part, sur les fichiers source à interpréter et d'autre part, sur le choix des formats de sortie.

Génération par l'interface web

Via un navigateur, il faut accéder au sous-dossier `/dobuilder` du dossier `/phpdoc` accessible du serveur web sur lequel il est installé. Dans le cas où navigateur et serveur web sont sur le même poste, on saisira l'url suivante : http://localhost/phpdoc/docbuilder. La page d'accueil suivante sera alors affichée :



Zone A – Menu horizontal permettant de choisir toutes les options

Zone B – Répertoire de travail, c'est-à-dire le répertoire utilisé par PHP Documentor pour créer ses fichiers temporaires.

Zone C – Boutons permettant de lancer la création de la documentation, soit dans la même page, soit dans une nouvelle page.

Zone D – Console, espace dans lequel les informations d'exécution seront affichées dans le cas où la création sera réalisée dans la même page.

Onglet "Config"

Dans l'onglet *Config*, on peut choisir une configuration spéciale (fichier .ini) déjà préparée. Cette configuration inclut le répertoire source, le répertoire cible, les fichiers à interpréter, ceux à ne pas interpréter, etc… Il suffit donc de créer ce fichier ini, de le sélectionner et de lancer la création de la documentation. Des fichiers .ini exemple se trouvent dans le sous-dossier user du dossier d'installation de PHP Documentor.

Onglet “Files”

Cet onglet permet de définir les fichiers/dossiers à interpréter ou à ne pas interpréter. Trois zones de texte sont donc disponibles pour préciser la liste des fichiers à analyser, la liste des dossiers à analyser et la liste des fichiers à ne pas analyser.

Chaque liste attend des chemins d'accès locaux (ex: /var/http/www/appli/fichier.php ou d:/xampp/htdocs/appli/fichier.php) séparés par des virgules. Les caractères spéciaux “*” et “?” sont autorisés.

Onglet “Output”

Cet onglet permet de définir dans quel dossier et sous quelle forme les documentations sont à générer. La zone de texte “Target” désigne l’emplacement de la documentation qui sera générée et la zone de texte “Output format” le(s) modèle(s) de sortie qu'elle adoptera. Un format de sortie se compose du format (HTML, XML, PDF, CHM), d'un convertisseur disponible en fonction du format, et d'un modèle proposé par le convertisseur choisi.

Quelques exemples, parmi les nombreux formats disponibles :

- **HTML:frames:default**, le modèle par défault
- **HTML:Smarty:PHP**, le modèle proche de celui adopté par la documentation sur PHP
- **XML:DocBook/peardoc2:default**
- **PDF:default:default**
- **CHM:default:default**

NB1 : Concernant le format HTML[4], dans le cas où les pages PHP suivent l'encodage de caractères utf-8, les templates de phpdocumentor pour les entêtes html doivent être modifiés : ce sont les fichiers header.tpl dans le sous-dossier phpDocumentor\Converters\frames ou Smarty. Il faut alors remplacer l'encodage iso-8859-1 par UTF-8 dans la balise *meta* de l'entête html.

NB2: Le menu déroulant sous le champ “Output format” permet de sélectionner un modèle et d'en avoir un aperçu via une petite icône.

Onglet “Options”

Dans cet onglet, il est possible de changer le nom de la documentation (Generated Documentation Title), les noms par défaut des packages et catégories.

Génération par l'interface ligne de commande sous Windows

En premier lieu, il faut ajouter dans la variable d'environnement système path le chemin d'accès qui contient l'interpréteur PHP.

Puis, le générateur de la documentation est appelé comme suit :

```
php répertoire_installation_phpdocumentor\phpdoc [options ligne de commande]
```

Par exemple, la ligne de commande suivante :

```
php c:\xampp\htdocs\phpdoc\phpdoc -f c:\xampp\htdocs\appli\monFichier.php -t c:\docAppli -o HTML:Smarty:PHP
```

interprétera le fichier c:\xampp\htdocs\appli\monFichier.php pour en générer la documentation sous le dossier c:\docAppli au format HTML:Smarty:PHP.

4 Concernant les formats autres que HTML, l'encodage utf-8 des pages PHP pose problème pour les pages de documentation générées.

La ligne de commande `php c:\xampp\htdocs\phpdoc\phpdoc -h` fournit la liste des options proposées par la commande phpdoc.