Programmation Web côté serveur

CM2 : PHP « intermédiaire »

Mickaël Martin Nevot

V2.2.0

Cette œuvre de Mickaël Martin Nevot est mise à disposition sous licence Creative Commons Attribution - Utilisation non commerciale - Partage dans les mêmes conditions.

BY-NC-SA

Programmation Web côté serveur

I. Présentation du cours
II. PHP
III. PHP « intermédiaire »
IV. POO
V. PHP « avancé »

 (cc) BY-NC-SA

Structure de langage

- **Structures de langage** :
  - echo, return, include, require, etc.

≠ fonction

- Utilisation de parenthèses non conseillée (même avec plusieurs arguments) :
  - Gain de performances :

```
echo $a; // Plutôt que echo ($a);
echo '1, ', '2'; // Plutôt que echo '1, ' . '2';
```

  - Erreur en cas de plusieurs arguments :

```
// Cause une erreur.
echo ($a, $b);
```

  - Conversion en expression :

```
// Erreur vous voulez retourner une référence !
return ($a);
```

BY-NC-SA

Retour sur return !

- Depuis une fonction : termine et retourne l'argument
- Depuis un script inclus : retourne par la fonction d'inclusion au script appelant
- Depuis le script principal : arrêt du script

(cc) BY-NC-SA

Quelques fonctions

- Teste la **définition d'une variable** :
  - `isset($var_1, $var_2, …)`
- Teste si une variable est vide : `empty($var)`
- Crée un **MD5** : `md5($str, …)`
- Génère un **identifiant unique** : `uniqid($prefix = …, …)`
- Génère un **nombre aléatoire** : `mt_rand(…)`
- Envoie un **en-tête HTTP** : `header($str, …)`
  - Redirection du navigateur :
    - `$str = 'Location: ' . $url`
- Initialise une **session** : `session_start()`

`!isset($var) || $var == false`

Pas d'affichage avant

Important !

Avant d'utiliser un header

(cc) BY-NC-SA

GET et POST

- HTTP (*hypertext transfer protocol*) :
  - Protocole de communication (client-serveur)
  - Méthodes (commandes) :
    - **GET** : construction d'URL dynamique
    - **POST** : passage « caché » des valeurs

URL (*uniform resource locator*) : littéralement « localisateur uniforme de ressource », est une chaîne de caractères utilisée pour adresser les ressources du Web, aussi appelée **adresse Web**

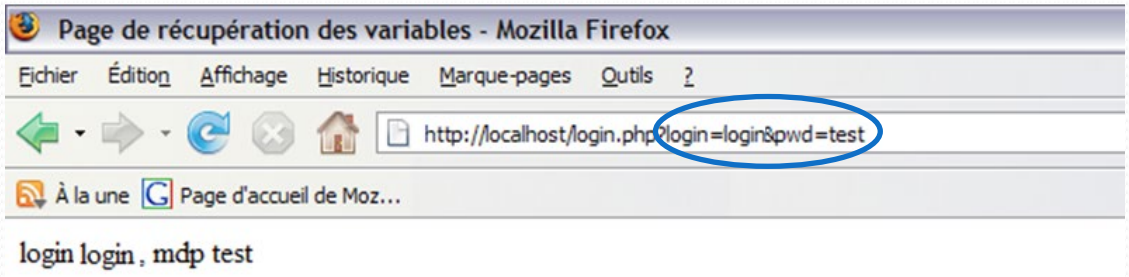
- Variables « superglobales » : `$_GET`, `$_POST`
  - Récupération de valeurs passées via le protocole HTTP et les méthodes **GET** et **POST**

(cc) BY-NC-SA

GET et POST

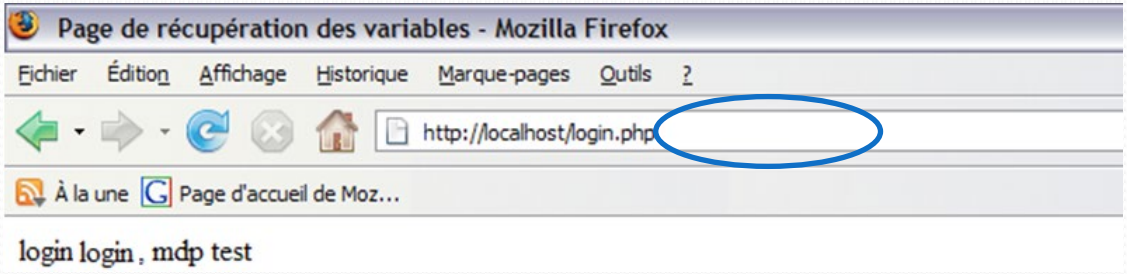
- **GET :**

```
if (isset($_GET['login'], $_GET['pwd']))
{
    echo 'login ', $_GET['login'], ', mdp ', $_GET['pwd'];
}
```



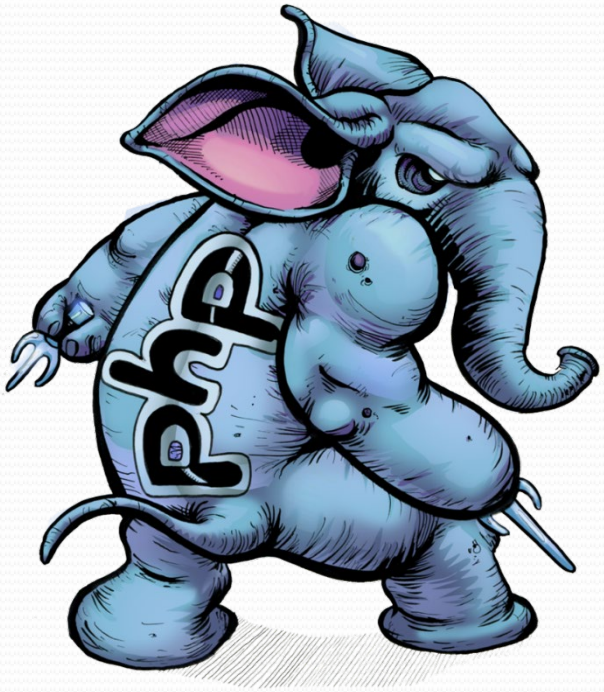
- **POST :**

```
if (isset($_POST['login'], $_POST['pwd']))
{
    echo 'login ', $_POST['login'], ', mdp ', $_POST['pwd'];
}
```



(cc) BY-NC-SA

GET et POST



- Passage de valeurs par tableaux

```
<input type="text" name="arr[foo]" value="1">
<input type="text" name="arr[bar]" value="2">
…
$arr = $_POST['arr'];
// array ('foo' => '1', 'bar' => '2');
```

- Filtrage

```
// if (!isset($_GET['a'])) { $a = null;
// } elseif (!is_string($_GET['a'])) { $a = false;
// } else { $a = $_GET['a']; }
$a = filter_input(INPUT_GET, 'a');
// $b = isset($_GET['b']) && is_string($_GET['b']) ? $_GET['b'] : '';
$b = (string) filter_input(INPUT_GET, 'b');
```

Attention aux *gotchas* ! Certains caractères spéciaux dans l'index seront convertis afin de pouvoir être transmis selon la méthode choisie

 (cc) BY-NC-SA

E-mail

- Fonction :
  - `mail($to, $subject, $message, $headers = …, …)`
- Envoi d'un *e-mail* :
  - Destinataire(s) : `$to`
  - Sujet du mail : `$subject`
  - Message à envoyer : `$message`
    - Texte simple
    - HTML
    - Texte simple et HTML (multi-format)
  - En-têtes : `$headers`

 (cc) BY-NC-SA

E-mail multi-format

- *E-mail* en texte **simple** :
  - Toujours lisible : compatibilité totale
  - Très léger
- *E-mail* en **HTML** :
  - Mise en forme complexe (police, image, lien, etc.)
- *E-mail* **multi-format** (**meilleure solution**) :
  - Affichage en texte simple en cas d'incompatibilité HTML
  - Affichage en HTML autrement

 (cc) BY-NC-SA

En-tête et frontière

- En-tête :
  - Adresse de l'expéditeur : `'From: exp1@fai.fr'`
  - Adresse de réponse : `'Reply-To: exp2@fai.fr'`
  - Destinataire(s) en copie : `'Cc: email_1, email_2'`
  - Destinataire(s) en copie cachée : `'Bcc: email_1, email_2'`
  - *Internet media type* : `'Content-type: type; sous-type'`
- Frontière (*boundary*) :
  - Permet de faire la séparation texte simple / HTML
  - *Content-type* de l'entête :
    `'Content-type: multipart/alternative; boundary=frontière'`
  - Au début de chaque type de message :
    - Frontière préfixée de deux tirets accolés
    - Après la frontière, modification des *headers* appliqués localement (au moins le *content-type* du message)

Peut être fausse

(cc) BY-NC-SA

Exemple d'e-mail

```
$to = 'to_mail@fai.org';
$from = 'my_mail@fai.org';
$reply = 'reply_mail@fai.org';
$subject = 'Test mail';

$bndary = md5(uniqid(mt_rand()));
$headers = 'From: Name <' . $from . '>' . "\n";
$headers .= 'Return-Path: <' . $reply . '>' . "\n";
$headers .= 'Content-type: multipart/alternative; boundary="' . $bndary. '"';

$message_text = 'Hello world!';
$message_html = '<html><body><strong>Hello world!</strong></body></html>';
$message = '--' . $bndary . "\n";
$message .= 'Content-Type: text/plain; charset=utf-8' . "\n\n";
$message .= $message_text . "\n\n";
$message .= '--' . $bndary . "\n";
$message .= 'Content-Type: text/html; charset=utf-8' . "\n\n";
$message .= $message_html . "\n\n";

mail($to, $subject, $message, $headers);
```

PHPMAILER
The PHP email class https://github.com/PHPMailer/PHPMailer

Utilisation (analogue) recommandée : plus sécurisée et fiable

 (cc) BY-NC-SA

Fichier

- **Ouverture** : `fopen($file, $mode, …)`
  - Fichier à ouvrir : `$file`
  - Spécifie le type d'accès désiré au fichier : `$mode`
    - Ouvre un fichier à son début : `'r'`, `'r+'`
    - Ouvre un fichier à sa fin : `'a'`, `'a+'`
    - Crée/écrase et ouvre un fichier : `'w'`, `'w+'`
    - Crée et ouvre un fichier : `'x'`, `'x+'`
- **Fermeture** : `fclose($handle)`

renvoie un pointeur sur le fichier

Ouvre en lecture dans tous les cas et en plus en écriture en cas de présence de + dans le mode

 (cc) BY-NC-SA

Fichier

- **Lecture** (jusqu'à `$length` octets du fichier `$handle`, ou jusqu'à la fin de la ligne courante par défaut pour `fgets(...)`) :
  - `fread($handle, $length)`
  - `fgets($handle, $length = ...)`
- **Écriture** :
  - `fwrite($handle, $str, ...)`
  - `fputs($handle, $str, ...)`
- Test si fichier/répertoire existe : `file_exists($filename)`
- Copie du fichier : `copy($source, $dest, ...)`
- Renomme un fichier/répertoire : `rename($old, $new, ...)`
- Efface un fichier : `unlink($filename)`

Nombre de caractères à lire

Valeur retournée par `fopen()`

`fputs(...)` est un alias de `fwrite(...)`

Chaine de caractères à écrire

 (cc) BY-NC-SA

Chargement HTML d'un fichier

- Le nom original du fichier (sur la machine du client) :
  `$_FILES['variable']['name']`
- Le nom temporaire du fichier (sur le serveur) :
  `$_FILES['variable']['tmp_name']`
- *L'Internet media type* du fichier :
  `$_FILES['variable']['type']`
- La taille du fichier (en octets) :
  `$_FILES['variable']['size']`
- L'éventuel code d'erreur :
  `$_FILES['variable']['error']`

```
<form action="send_fichier.php" method="post" enctype="multipart/form-data">
    <p>
        Votre fichier : <input type="file" name="mon_fichier"></input>
        <input type="hidden" name="MAX_FILE_SIZE" value="20000"></input>
    </p>
</form>
// …
move_uploaded_file($_FILES['variable']['tmp_name'],
                   $uploads_dir . '/' . $_FILES['variable']['name']);
```

 BY-NC-SA

Variables dynamiques

- Nom de variable affecté et utilisé dynamiquement :

```
$var = 'hello';
$hello = 'world';
echo ${$var}; // Affiche : world.

…

$champ_cache = $_POST['champ_cache'];

function insert() { // Code. }
function delete() { // Code. }
function update() { // Code. }
function select() { // Code. }

if ('insert' === $champ_cache
 || 'delete' === $champ_cache
 || 'update' === $champ_cache
 || 'select' === $champ_cache)
{
    $champ_cache();
}
```

 (cc) BY-NC-SA

Rappel : expressions rationnelles

- **Chaîne de caractères appelé motif (ou *pattern*) qui décrit un ensemble de chaînes de caractères possibles**
- Pas de standardisation
- Symboles spéciaux communs :
  - `.` : n'importe quel caractère
  - \ : échapper (banaliser) un caractère
  - `[ ]` : un des caractères au choix parmi ceux entre crochets
  - `^`, `$` : début/fin (`^a`, `a$`)
  - Quantifieurs :
    - `?` : zéro ou une fois
    - `*` : zéro, une ou plusieurs fois
    - `+` : une ou plusieurs fois

 (cc) BY-NC-SA

Rappel : expressions rationnelles

http://www.debuggex.com

- Exemple :
  - `a.b`
  - `[0-9][0-9]aaa.*`
  - `^r.*[0-9]$`
  - `^[a-z0-9._-]+@[a-z0-9._-]{2,}\.[a-z]{2,4}$`
- En PHP :
  - POSIX : `eregx` (`ereg_replace(...)`)
  - PCRE : `preg_x` (`preg_replace(...)`, `preg_match(...)`, etc.)

Utilise les symboles standards

Plus puissant et plus rapide

```
if(preg_match('/^[a-z0-9._-]+@[a-z0-9._-]{2,}\.[a-z]{2,4}$/', $email)) {
    echo 'syntaxe de l\'e-mail : ok';
}
```

 (cc) BY-NC-SA

PHP et MySQL

BD : base de données

- **Connexion** à un serveur MySQL :

```
mysqli_connect($host = …, $username = …, $passwd = …, …)
```

- Sélectionne une **BD** :

```
mysqli_select_db($link, $dbname)
```

- Ferme la connexion MySQL :

```
mysqli_close($link)
```

Une connexion est fermée par défaut à la fin du script l'ayant ouverte

- Envoie un message en cas d'erreur : `die($str)`

```
$link = mysqli_connect($host, $username, $passwd) or die('Erreur : ' . $host);
```

Important : l'activation de l'extension MySQLi est obligatoire (par défaut à partir de PHP 5.3.0) !

(cc) BY-NC-SA

PHP et MySQL

- Envoie une **requête** au serveur :
  `mysqli_query($link, $query)`
- Retourne un **enregistrement** :
  - Tableau indexé :
    `mysqli_fetch_row($result)`
  - Tableau associatif :
    `mysqli_fetch_assoc($result)`
- Nombre d'enregistrements d'un résultat :
  `mysqli_num_rows($result)`
- Libère la mémoire du résultat :
  `mysqli_free_result($result)`

(cc) BY-NC-SA

Exemple PHP et MySQL

```
$link = mysqli_connect('localhost', 'mysql_username', 'mysql_passwd')
    or die('Pb de connexion au serveur: ' . mysqli_connect_error());
mysqli_select_db($link, 'my_dbname') or die ('Pb de sélection BD : ' . mysqli_error($link));

$query = 'SELECT name AS username FROM table WHERE id = 1';
$result = mysqli_query($link, $query);
if (!$result)
{
    echo 'Impossible d\'exécuter la requête ', $query, ' : ', mysqli_error($link);
}
else
{
    if (mysqli_num_rows($result) != 0)
    {
        while ($row = mysqli_fetch_assoc($result))
        {
            echo $row['username'];
        }
    }
}
```

 BY-NC-SA

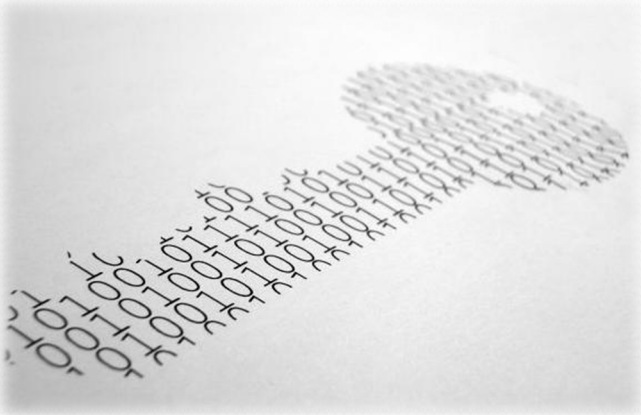
Utilité des pages sécurisées

- Restreindre une partie d'un site Web
- **Protéger des données**
- Utilisations courantes :
  - Partie d'un site accessible qu'à certains utilisateurs
  - Partie d'un site qui comporte des **données personnelles** (compte bancaire, adresse postale, etc.)
  - Compte ***e-mail***
  - Compte pour un site *d'**e-commerce***

BY-NC-SA

Moyens de sécurisation

- Niveau **réseau** : (par exemple HTTPS)
  - On utilise SSL (*secure socket layer*) pour chiffrer le canal de communication :
    - Utilise un certificat pour l'identification
    - Certificat hébergé chez un tiers
- Niveau **applicatif** :
  - Authentification
  - Pages sécurisées



 BY-NC-SA

Authentification

- Table **utilisateur** dans la base de données :
  - Un identifiant (*e-mail*, pseudonyme, etc.)
  - Un mot de passe encodé
- Lors de l'**authentification** :
  - On vérifie le couple identifiant / mot de passe encodé avec les informations en base de données
  - On met les informations dans la variable `$_SESSION`
- **Vérification de l'authentification à chaque page** :
  - L'utilisateur ne retape pas ses identifiants
  - Vérification faite grâce à la variable `$_SESSION`

(cc) BY-NC-SA

Exemple d'authentification

```
// Page d'authentification.
if (filter_input(INPUT_POST, 'login') && filter_input(INPUT_POST, 'pwd'))
{
    // Connexion au serveur de la base de données, à la base de données et
    // récupération dans la table utilisateur du login dans la variable $login
    // et du mot de passe dans la variable $pwd.
    // …
    if ($login === $_POST['login'] && password_verify($_POST['pwd'], $pwd))
    {
        session_start();
        $_SESSION['suid'] = session_id();
        header('Location: page.php');
    }
    else
    {
        header('Location: file.html');
    }
    exit();
}
```

(cc) BY-NC-SA

Exemple d'authentification

```
// page.php.
session_start();
if (isset($_SESSION['suid']))
{
    // L'authentification est validée.
}
```

 (cc) BY-NC-SA

Post-Redirect-Get (PRG)

- Page Web du formulaire :

```php
<?php
require 'path_to_file/validate.php';
validate();
?>
<html>…<form action="validate.php" method="post">…</form>…</html>
```

- Traitement :

```php
<?php
function validate(): void {
    // Aucun affichage dans cette fonction.
    if ($_POST) {
        // Valider les données d'entrée.
        if (/* Données d'entrée ok */) {
            // Traitement (requêtes à la base de données, données en session, etc.).
            // Redirection.
            header('Location: ' . $_SERVER['REQUEST_URI'], true, 303);
            exit();
        }
    }
}
```

(cc) BY-NC-SA

Aller plus loin

- Pièces jointes dans un *e-mail*
- Flux d'entrée/sortie
- Utiliser la librairie GD (traitement des images)

(cc) BY-NC-SA

Liens

- Documents électroniques :
  - Manuels :
    - http://php.net/manual
    - http://fr.php.net/manual/fr/ref.mysql.php
  - *Framework* :
    - http://framework.zend.com
    - http://www.symfony-project.org
  - Génération de données :
    - http://www.generatedata.com/#generator
  - Fonctions images :
    - http://www.manuelphp.com/php/ref.image.php

Crédits

Auteur

Mickaël Martin Nevot
mmartin.nevot@gmail.com

Carte de visite électronique

Relecteur

- Christophe Delagarde (christophe.delagarde@univ-amu.fr)
- Pierre-Alexis de Solminihac (pa@solminihac.fr)

Cours en ligne sur : www.mickael-martin-nevot.com