

Web dynamique ...

Éric BERTHOMIER
eric.berthomier@free.fr

March 16, 2022

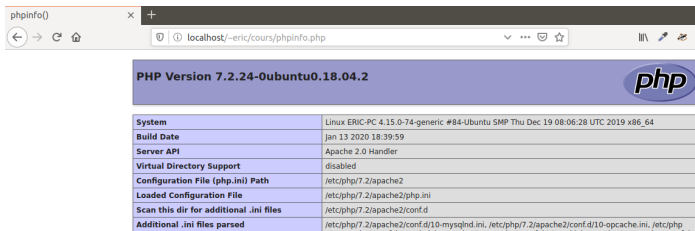


Version 1.0 - Version Stagiaire

Mon premier fichier PHP

firstphp.php

```
<?php  
    phpinfo();  
?>
```



System	Linux ERIC-PC 4.15.0-74-generic #84-Ubuntu SMP Thu Dec 19 08:06:28 UTC 2019 x86_64
Build Date	Jan 13 2020 18:39:59
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-mysqld.ini, /etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-openssl.ini, /etc/php/7.2/apache2/conf.d/10-zlib.ini

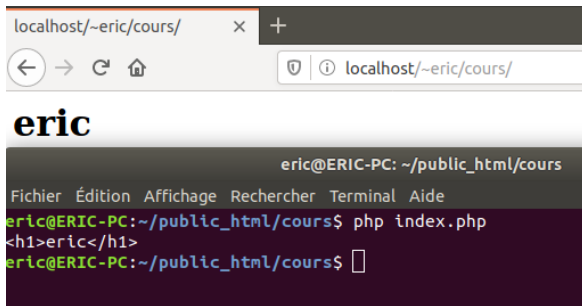
Web dynamique



Notion de variable

variable.php

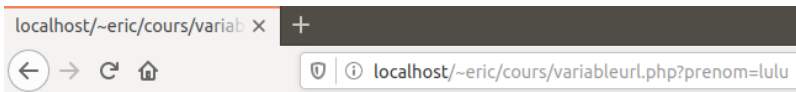
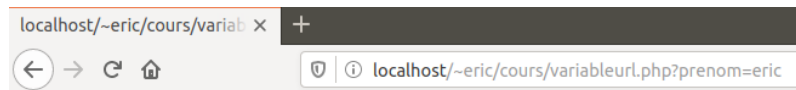
```
<?php
$variable="eric";
print("<h1>".$variable."</h1>");
?>
```



Passage de variable en URL

variableurl.php

```
<?php  
    print ("<h1>".$_GET['prenom']."</h1>");  
?>
```



Exercice

- Identifier des sites utilisant le passage de paramètre GET



Exercice

- Identifier des sites utilisant le passage de paramètre GET
- Trouver les éléments en lien avec ces derniers



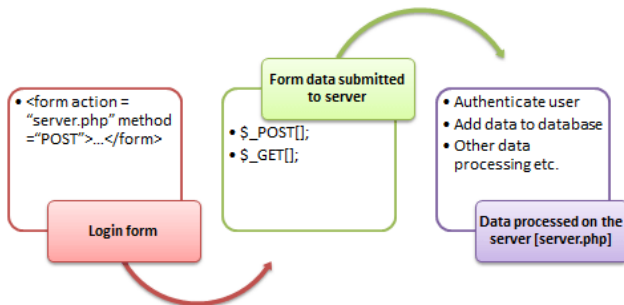
Mon premier formulaire

firstformulaire.html

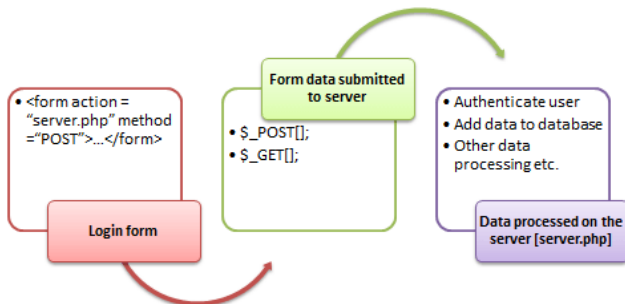
```
<!DOCTYPE html>
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <title>Mon 1er formulaire</title>
</head>
<body>
  <form method="post" action="infoatraitier.html">
    <fieldset>
      <legend>Information à donner</legend>
      <input type="text" name="login" />
    </fieldset>
    <br>
    <input type="submit" name="submit" value="Envoyer l'information" />
  </form>
</body>
</html>
```



Principe de fonctionnement d'un formulaire de saisie



Principe de fonctionnement d'un formulaire de saisie



Quel que soit la méthode utilisée, le formulaire va utiliser le protocole HTML GET ou POST pour envoyer ces informations au serveur.



Traitement des données - POST / GET

Il existe une seconde méthode pour transmettre les données au travers du Web. La méthode POST.



Traitement des données - POST / GET

Il existe une seconde méthode pour transmettre les données au travers du Web. La méthode POST.

Découverte et analyse :

`http://cours.ericberthomier.fr/mdp/index.html`



Sniff !!!

`http://cours.ericberthomier.fr/demo`



Retrouver le mot de passe !

Réflexion

Qui peut réaliser l' "*attaque*" précédente ?



Conclusion

