Presentació: Sessions en PHP

Pàgina 1: Portada

Títol: Sessions en PHP
Subtítol: Gestió d'estat al servidor
Contingut:

- Logo o imatge relacionada amb sessions
- Curs/assignatura : ASIX2 / SM9-Implantació d’aplicacions web
- Data

Pàgina 2: Índex

Títol: Continguts **Contingut:**

1. Introducció a les sessions
2. Diferència galetes vs sessions
3. Gestió bàsica de sessions
4. Finalització de sessions
5. Configuració i seguretat
6. Exemple pràctic
7. Bones pràctiques

Pàgina 3: Què són les sessions?

Títol: Introducció a les Sessions **Contingut:**

- **Definició:** Mecanisme per emmagatzemar dades de l'usuari **al servidor**
- **Problema:** HTTP és *stateless* (sense estat)
- **Solució:** Mantenir informació entre pàgines/sol·licituds
- **Ubicació:** Servidor (no client)
- **Identificació:** ID únic de sessió (PHPSESSID)

Pàgina 4: Com Funcionen?

Títol: Funcionament de les Sessions **Contingut:**

```
1. Usuari accedeix → Servidor crea sessió (ID: abc123)
2. Servidor envia cookie PHPSESSID=abc123
3. Dades es desen AL SERVIDOR
4. Cada petició: client envia PHPSESSID
5. Servidor recupera dades associades a abc123
```

Diagrama:

```
Client --solicitud--> Servidor
       <--PHPSESSID-- (crea sessió, desa dades)
Client --PHPSESSID--> Servidor
       <--dades------ (recupera dades)
```

Pàgina 5: Galetes vs Sessions

Títol: Comparativa: Galetes vs Sessions

Característica	Galetes	Sessions
Emmagatzematge	Client	Servidor
Mida	~4KB	Il·limitada*
Seguretat	Menys	Més
Caducitat	Configurable	Navegador/timeout
Velocitat	Ràpid	Més lent
Dades sensibles	NO	SÍ

*Dins de límits del servidor

Pàgina 6: Usos de les Sessions

Títol: Per a què serveixen les sessions? **Contingut:**

- **Autenticació** d'usuaris (login/logout)
- **Carros de compra**
- Preferències temporals
- Formularis multipàgina
- Control d'accés
- Prevenció CSRF
- Dades temporals segures

Pàgina 7: Inici de Sessió

Títol: session_start() - Inici de Sessió **Contingut:**

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

Regles CRÍTIQUES:

- Crida a **TOTES** les pàgines que usin sessions
- **ABANS** de qualsevol HTML
- **UNA sola vegada** per pàgina

INCORRECTE:

```
<html>
```

```
<?php session_start(); // ERROR! ?>
```

Pàgina 8: Emmagatzemament de Dades

Títol: Array Superglobal $_SESSION **Contingut:**

```
<?php
session_start();

// Assignació de dades
$_SESSION['nom'] = 'Joan';
$_SESSION['edat'] = 25;
$_SESSION['regals'] = array('Llibre', 'Pilota');
?>
```

Tipus de dades:

- Strings, enters, floats
- Arrays
- Objectes (amb precaució)

Pàgina 9: Llegir Dades

Títol: Recuperació de Dades de Sessió **Contingut:**

```
<?php
session_start();

// Comprova existència
if (isset($_SESSION['nom'])) {
    echo "Hola, " . $_SESSION['nom'];
} else {
    echo "No heu iniciat sessió";
}
?>
```

Sempre emprar `isset()` abans d'accedir

Pàgina 10: Modificació de Dades

Títol: Actualització de Variables de Sessió **Contingut:**

```
<?php
session_start();

// Modificació de valor
$_SESSION['nom'] = 'Maria';

// Modificació d’array
$_SESSION['regals'][] = 'Joc';      // Afegeix
unset($_SESSION['regals'][0]);      // Elimina element

// Elimina variable específica
```

```
unset($_SESSION['edat']);
?>
```

Les dades estan disponibles **immediatament**

Pàgina 11: Esborrament de Variables

Títol: Eliminació de Dades de Sessió **Contingut: Una variable específica:**

```
unset($_SESSION['nom']);
```

Totes les variables:

```
$_SESSION = array();
```

Diferència amb session_destroy():

- `unset()` / `$_SESSION = array()`: Esborrament de dades, sessió continua
- `session_destroy()`: Destrucció completa de la sessió

Pàgina 12: Destrucció de Sessió

Títol: session_destroy() - Finalització de Sessió **Contingut: Destrucció bàsica:**

```
<?php
session_start();
session_destroy();
?>
```

Destrucció completa (recomanat):

```
<?php
session_start();

// 1. Esborra variables
$_SESSION = array();

// 2. Destrueix sessió
session_destroy();
?>
```

Pàgina 13: Logout Complet

Títol: Funció de Logout Segur **Contingut:**

```
<?php
session_start();

// 1. Esborra totes les variables
$_SESSION = array();

// 2. Elimina galeta de sessió
```

```
if (isset($_COOKIE[session_name()])) {
    setcookie(session_name(), '', time() - 3600, '/');
}

// 3. Destrucció de sessió
session_destroy();

// 4. Redirecció
header('Location: index.php');
exit;
?>
```

Pàgina 14: Configuració - Nom de Sessió

Títol: Personalització del Nom de Sessió **Contingut:**

```
<?php
// Abans de session_start()
session_name('MEU_SITE');
session_start();
?>
```

Per defecte: PHPSESSID
Personalitzat: MEU_SITE (o el que vulgueu)

Útil per diferenciar sessions de diferents aplicacions

Pàgina 15: Timeout de Sessió

Títol: Temps de Caducitat **Contingut: Configurar en php.ini:**

```
session.gc_maxlifetime = 3600  ; 1 hora
```

Configuració en temps d'execució:

```
<?php
ini_set('session.gc_maxlifetime', 1800); // 30 min
session_start();
?>
```

Típics:

- 1800 segons = 30 minuts
- 3600 segons = 1 hora
- 7200 segons = 2 hores

Pàgina 16: Timeout Personalitzat

Títol: Control Manual de Timeout **Contingut:**

```
<?php
session_start();
```

```
$temps_maxim = 1800; // 30 minuts

if (!isset($_SESSION['ultim_acces'])) {
    $_SESSION['ultim_acces'] = time();
}

// Comprovació de caducitat
if (time() - $_SESSION['ultim_acces'] > $temps_maxim) {
    session_unset();
    session_destroy();
    header('Location: login.php?timeout=1');
    exit;
}

// Actualització
$_SESSION['ultim_acces'] = time();
?>
```

Pàgina 17: Seguretat – Regeneració d'ID

Títol: Prevenció de Fixació de Sessió **Contingut:**

```
<?php
session_start();

// Després de login exitós
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    // Validar credencials...

    // REGENERAR ID de sessió
    session_regenerate_id(true);

    $_SESSION['usuari'] = $usuari;
}
?>
```

Sempre cal regenerar la ID després de canvis d'autenticació

Pàgina 18: Protecció de Pàgines

Títol: Control d'Accés amb Sessions **Contingut:**

```
<?php
session_start();

// Funció de validació
function esta_autenticat() {
    return isset($_SESSION['usuari_id'])
           && !empty($_SESSION['usuari_id']);
}

// Protecció de pàgina
if (!esta_autenticat()) {
    header('Location: login.php');
    exit;
}
```

```
// Codi de la pàgina protegida...
?>
```

Pàgina 19: Seguretat – Escapament de Sortides

Títol: Prevenció XSS amb Dades de Sessió **Contingut:**

```
<?php
session_start();

// MAI confieu cegament en les dades de sessió
if (isset($_SESSION['nom'])) {
    // ESCAPEU abans de mostrar
    echo htmlspecialchars($_SESSION['nom'], ENT_QUOTES, 'UTF-8');
}
?>
```

Encara que són del servidor, poden venir d'entrada d'usuari

Pàgina 20: Exemple Pràctic (1/3)

Títol: Sistema de Regals - Formulari **Contingut:**

```
<?php
// inici.php
session_start();

if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $_SESSION['nom'] = trim($_POST['nom']);
    $_SESSION['cognom'] = trim($_POST['cognom']);
    $_SESSION['regals'] = array();

    if (isset($_POST['regals']) && is_array($_POST['regals'])) {
        $_SESSION['regals'] = $_POST['regals'];
    }

    header('Location: cistell.php');
    exit;
}
?>
```

Pàgina 21: Exemple Pràctic (2/3)

Títol: Sistema de Regals - Cistell **Contingut:**

```
<?php
// cistell.php
session_start();

// Protecció de la pàgina
if (!isset($_SESSION['nom'])) {
    header('Location: inici.php');
    exit;
```

```
}

// Actualització de regals
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $_SESSION['regals'] = $_POST['regals'] ?? array();
}

$nom = htmlspecialchars($_SESSION['nom'] . ' ' . $_SESSION['cognom']);
$regals = $_SESSION['regals'] ?? array();
?>
```

Pàgina 22: Exemple Pràctic (3/3)

Títol: Sistema de Regals - Finalització **Contingut:**

```
<?php
// A cistell.php
if (isset($_GET['finalitzar'])) {
    session_unset();
    session_destroy();
    header('Location: inici.php');
    exit;
}
?>

<!-- HTML -->
<a href="?finalitzar=1">Finalitzar sessió</a>
```

Pàgina 23: Errors Comuns

Títol: Problemes Freqüents **Contingut: 1. Headers already sent**

```
// MALAMENT
<html>
<?php session_start(); ?>

// BÉ
<?php session_start(); ?>
<html>
```

2. No criddeu session_start()

- Cal a TOTES les pàgines que usin sessions

3. Oblideu isset()

- Sempre comproveu abans d'accedir

Pàgina 24: Funcions Útils

Títol: Funcions de Sessions **Contingut:**

```
// Obtenció d'ID
$id = session_id();
```

```
// Obtenció de nom
$nom = session_name();

// Comprovació d'estat
if (session_status() === PHP_SESSION_ACTIVE) {
    echo "Sessió activa";
}

// Visualització de totes les variables
print_r($_SESSION);
```

Pàgina 25: Bones Pràctiques

Títol: Bones Pràctiques **Contingut:**

1. ✓ session_start() a totes les pàgines
2. ✓ Regenereu ID després d'autenticar
3. ✓ Establiu timeout adequat
4. ✓ Valideu dades de sessió
5. ✓ Escapeu sortides (htmlspecialchars)
6. ✓ Destruïu sessió en logout
7. ✓ NO emmagatzemeu contrasenyes
8. ✓ Empreu HTTPS
9. ✓ Protegiu pàgines sensibles
10. ✓ Netegeu sessions antigues

Pàgina 26: Depuració

Títol: Depuració de Sessions **Contingut: Veure contingut:**

```
echo "<pre>";
print_r($_SESSION);
echo "</pre>";
```

Informació de configuració:

```
echo "Nom: " . session_name();
echo "ID: " . session_id();
echo "Timeout: " . ini_get('session.gc_maxlifetime');
```

Pàgina 27: Sessions vs Galetes

Títol: Sessions o Galetes? **Contingut: Emprar SESSIONS per:**

- Dades sensibles (usuaris, permisos)
- Dades temporals de la visita
- Informació que no cal persistir
- Autenticació

Usar GALETES per:

- Preferències persistents
- Petites quantitats de dades
- Recordar entre visites
- Dades no sensibles

Pàgina 28: Resum

Títol: Resum **Contingut:**

- Sessions emmagatzemen dades **al servidor**
- Empreu **session_start()** abans de HTML
- Accediu amb **$_SESSION**
- Destruïu amb **session_destroy()**
- Més **segures** que galetes per a dades sensibles
- Sempre **regenereu ID** després de login
- **Valideu i escapeu** dades
- Cal session_start() a **totes les pàgines**

Pàgina 29: Preguntes

Títol: Preguntes? **Contingut:**

- Espai per preguntes
- Contacte : jordi.binefa@fje.edu
- Referències
    - Manual oficial PHP: php.net/manual/es/book.session.php
    - Seguretat en sessions: OWASP Session Management
    - Cross-site request forgery: https://ca.wikipedia.org/wiki/Cross-site_request_forgery
    - Fixació de sessió: https://ca.wikipedia.org/wiki/Fixaci%C3%B3_de_sessi%C3%B3
    - XSS (Cross Site Scripting): https://ca.wikipedia.org/wiki/Cross_Site_Scripting