# AstroGate5 Web – Datei verstehen: session.php (Zeile für Zeile)

Datei: app/session.php | Lernmodus: Mittelweg

## 1) Ziel

Du verstehst, wie PHP-Sessions funktionieren, warum sie vor HTML gestartet werden müssen und wie Flash-Meldungen technisch umgesetzt sind.

## 2) Kompletter Code

```
<?php
// app/session.php
declare(strict_types=1);

function session_start_sicher(): void
{
    if (session_status() === PHP_SESSION_ACTIVE) {
        return;
    }

    $secure = (!empty($_SERVER['HTTPS']) && $_SERVER['HTTPS'] !== 'off');

    session_set_cookie_params([
        'lifetime' => 0,
        'path' => '/',
        'domain' => '',
        'secure' => $secure,
        'httponly' => true,
        'samesite' => 'Lax',
    ]);

    session_start();
}

function flash_set(string $key, string $msg): void
{
    $_SESSION['flash'][$key] = $msg;
}

function flash_get(string $key): ?string
{
    if (!isset($_SESSION['flash'][$key])) return null;
    $msg = (string)$_SESSION['flash'][$key];
    unset($_SESSION['flash'][$key]);
    return $msg;
}
```

## 3) Zeile-für-Zeile Erklärung

**Zeile 1**

```
<?php
```

Start von PHP.

**Zeile 2**

```
// app/session.php
```

Kommentar: Diese Datei kümmert sich nur um Sessions & Flash-Meldungen.

**Zeile 3**

```
declare(strict_types=1);
```

Strikte Typen: sorgt für sauberes Verhalten.

**Zeile 4**

Diese Zeile ist Teil der Session-/Flash-Logik.

**Zeile 5**

```
function session_start_sicher(): void
```

Definition einer Funktion. Sie startet die Session sicher.

**Zeile 6**

```
{
```

Funktionsblock beginnt.

**Zeile 7**

```
    if (session_status() === PHP_SESSION_ACTIVE) {
```

Prüft: Läuft bereits eine Session?

**Zeile 8**

```
        return;
```

Wenn ja: Funktion sofort verlassen (kein doppeltes session_start).

**Zeile 9**

```
    }
```

Diese Zeile ist Teil der Session-/Flash-Logik.

**Zeile 10**

Diese Zeile ist Teil der Session-/Flash-Logik.

**Zeile 11**

```
    $secure = (!empty($_SERVER['HTTPS']) && $_SERVER['HTTPS'] !== 'off');
```

Ermittelt, ob HTTPS aktiv ist (wichtig für sichere Cookies).

**Zeile 12**

Diese Zeile ist Teil der Session-/Flash-Logik.

**Zeile 13**

```
    session_set_cookie_params([
```

session_set_cookie_params legt fest, wie das Session-Cookie aussieht.

**Zeile 14**

```
        'lifetime' => 0,
```

lifetime=0: Cookie gilt nur bis Browser geschlossen wird.

**Zeile 15**

```
        'path' => '/',
```

path='/' : Cookie gilt für die ganze Webseite.

**Zeile 16**

```
        'domain' => '',
```

domain leer: aktueller Host.

**Zeile 17**

```
        'secure' => $secure,
```

secure: Cookie nur über HTTPS senden (wenn verfügbar).

**Zeile 18**

```
        'httponly' => true,
```

httponly: JavaScript darf NICHT auf das Cookie zugreifen (XSS-Schutz).

**Zeile 19**

```
        'samesite' => 'Lax',
```

samesite=Lax: Schutz vor CSRF-Angriffen (Standardwert).

**Zeile 20**

```
    ]);
```

Diese Zeile ist Teil der Session-/Flash-Logik.

**Zeile 21**

Diese Zeile ist Teil der Session-/Flash-Logik.

**Zeile 22**

```
    session_start();
```

Startet die Session endgültig.

**Zeile 23**

```
}
```

Ende der Funktion.

**Zeile 24**

Diese Zeile ist Teil der Session-/Flash-Logik.

**Zeile 25**

```
function flash_set(string $key, string $msg): void
```

Funktion zum Setzen einer Flash-Meldung.

**Zeile 26**

```
{
```

Diese Zeile ist Teil der Session-/Flash-Logik.

**Zeile 27**

```
    $_SESSION['flash'][$key] = $msg;
```

Speichert Nachricht in der Session unter 'flash'.

**Zeile 28**

```
}
```

Diese Zeile ist Teil der Session-/Flash-Logik.

**Zeile 29**

Diese Zeile ist Teil der Session-/Flash-Logik.

**Zeile 30**

```
function flash_get(string $key): ?string
```

Funktion zum einmaligen Auslesen einer Flash-Meldung.

**Zeile 31**

```
{
```

Diese Zeile ist Teil der Session-/Flash-Logik.

**Zeile 32**

```
    if (!isset($_SESSION['flash'][$key])) return null;
```

Wenn keine Meldung existiert: null zurückgeben.

**Zeile 33**

```
    $msg = (string)$_SESSION['flash'][$key];
```

Speichert Meldung in Variable.

**Zeile 34**

```
    unset($_SESSION['flash'][$key]);
```

Löscht Meldung sofort aus der Session (nur einmal anzeigen).

**Zeile 35**

```
    return $msg;
```

Gibt die Meldung zurück.

**Zeile 36**

```
}
```

Diese Zeile ist Teil der Session-/Flash-Logik.

## 4) Mini-Übungen

Übung A: Entferne testweise session_status()-Prüfung und beobachte die Fehlermeldung.
Übung B: Setze eine Flash-Meldung auf einer Seite und lies sie auf einer anderen aus.
Übung C: Kommentiere httponly aus und lies nach, warum das gefährlich ist.