موضوع جلسه ۲۳ چیست؟

وقتی وارد صفحه `note.php` **میشی و در** URL **،** `id` **رو عوض می‌کنی، محتوا هم عوض میشه. مثلاً:**

```
/note.php?id=1
/note.php?id=5
```

یعنی الان هر کسی با تغییر عدد داخل URL **می‌تونه یادداشت بقیه رو ببینه**😐
اینجا مشکل امنیتی هست و باید بررسی کنیم:

- **آیا اصلاً این یادداشت وجود داره؟**
- **آیا این یادداشت مال کاربر لاگین‌شده هست یا نه؟**

مرحله اول: اصلاح کوئری در فایل `note.php`

قبل:

```
$note = $db->query("SELECT * FROM notes WHERE id =
:id", ['id' => $_GET['id']])->fetch();
```

این کد فقط بر اساس `id` **یادداشت رو می‌گرفت. اما مهم نیست مال چه کاربریه.**

اصلاح‌شده:

```
$note = $db->query("SELECT * FROM notes WHERE user_id =
:user AND id = :id", [
    'id' => $_GET['id'],
    'user' => 3
])->fetch();
```

الان می‌گه: «یادداشتی رو بیار که هم `id` **ش فلان باشه و هم** `user_id` **ش برابر ۳ (مثلاً کاربر لاگین‌شده).«**

❗مرحله دوم: بررسی اگر یادداشت اصلاً وجود نداشت (خطای ۴۰۴)

```
if (!$note) {
    http_response_code(404); // ارسال کد ۴۰۴ به مرورگر
    header("Location: /laracast-php/index.php"); // برگشت به صفحه اصلی
    exit(); // قطع ادامه اجرای فایل
}
```

یعنی اگر یادداشت پیدا نشد، بگو: «صفحه‌ای با این مشخصات پیدا نشد» (یعنی ۴۰۴).

⛔مرحله سوم: بررسی اینکه آیا این یادداشت مال این کاربر هست یا نه (خطای ۴۰۳)

مثلاً فرض کن یادداشت با `id=2` هست، ولی مال کاربر دیگریه. الان باید بگیم: «شما اجازه دسترسی به این یادداشت رو نداری.»

```
$current_userid = 3;
$forbidden = 403;

if ($note['user_id'] != $current_userid) {
    http_response_code($forbidden);
    require "403.php";
    exit();
}
```

اگر `user_id` یادداشت با `current_userid` یکی نبود → ۴۰۳ → فایل `403.php` نشون داده میشه.

🎁مرحله چهارم: ساختن یک فایل کمکی برای مدیریت کدهای پاسخ

فایل جدید می‌سازیم به اسم `Response.php` برای اینکه عددهای ۴۰۳ و ۴۰۴ رو مستقیم ننویسیم. اینطوری تمیزتره و بعداً اگر خواستیم تغییرش بدیم راحتیم.

محتویات :Response.php

```
class Response {
    const NOT_FOUND = 404;
    const FORBIDDEN = 403;
}
```

حالا در کدت ازش استفاده می‌کنی:

```
http_response_code(Response::FORBIDDEN);
```

یا:

```
http_response_code(Response::NOT_FOUND);
```

۱ .اصلاً forbiddenیعنی چی؟

کلمه forbiddenیعنی **ممنوع**
در دنیای وب، اگر کاربر **اجازه دسترسی به یک چیزی رو نداشته باشه**، مرورگر با کد HTTP 403پاسخ می‌ده که یعنی:

»شما اجازه ندارید این صفحه یا اطلاعات رو ببینید«.

درPHP ، اینو اینطوری می‌نویسیم:

```
http_response_code(403);
```

---

۲ .خب حالا چرا ممکنه یکی بیاد به یادداشت بقیه دسترسی پیدا کنه؟

فرض کن این آدرس رو داری:

```
note.php?id=1
```

و یادداشت شماره ۱ برای کاربر علی هست. حالا فرض کن تو لاگین کردی و کاربر «مهدی» هستی.
اگر تو بری به همون آدرس بالا، یعنی note.php?id=1و سیستم بررسی نکنه که آیا این یادداشت مال تو هست یا نه، اون وقت تو به یادداشت علی دسترسی پیدا می‌کنی!

⛔یعنی اینجوری امنیت از بین می‌ره و کاربرها می‌تونن یادداشت‌های بقیه رو ببینن.

---

۳. راه‌حل: بررسی مالکیت یادداشت

پس ما میایم این شرط رو اضافه می‌کنیم:

```
if ($note["user_id"] != $current_userid) {
    http_response_code(403);
    require "403.php";
    exit();
}
```

یعنی:

اگر user_idیادداشت با شناسه کاربر فعلی یکی نبود، بگو ۴۰۳ (ممنوعه) و یه صفحه مخصوص نشون بده.

مثلاً یادداشت مربوط به کاربر ۳ هست ولی تو الان با کاربر ۵ وارد شدی ← اجازه نداری ببینی.

---

۴. چرا این‌کار لازمه؟

چون URL توی مرورگر **آزادانه قابل تغییره** .هر کسی می‌تونه توی نوار آدرس، ?id=2رو بزنه. اگه ما توی PHP بررسی نکنیم، اون شخص به همه یادداشت‌ها دسترسی پیدا می‌کنه.

مثال واقعی:

note.php?id=1 ← یادداشت کاربر A

note.php?id=2 ← یادداشت کاربر B

کاربر A با تغییر عدد به ۲، یادداشت B رو می‌خونه❌

✅پس خلاصه کنم:

حالت	کاری که باید کنیم	کد وضعیتHTTP
یادداشت پیدا نشد	not found	404
یادداشت هست ولی مال کاربر دیگه‌ست	ممنوعه	403
یادداشت هست و مال همین کاربره	نمایش یادداشت	(عادی) 200

ما یه فایل Response .php با کد زیر را ایجاد :

```php
<?php
class Response{
    const NOT_FOUND= 404;
    const FORBIDDEN= 403;
}
```

و در فایل note.php به صورت زیر ازش استفاده میکنیم:

```php
require_once "../Response.php";
Response::FORBIDDEN
Response::NOT_FOUND
```

پس کد نهایی اینجوری میشه:

```php
require_once "../Response.php";
if(!$note){
    echo "<br>" . "Not Found" . "<br>";
    echo "<a href=laracast-php/notes/>صفحه به برگشت
قبل</a>";
    http_response_code(Response::NOT_FOUND);
    exit();

}
```

```php
if($note["user_id"] != 3){
    http_response_code(Response::FORBIDDEN);
    require_once "403.php";
}
```

؟ سوال ۱:

چه تفاوتی بین **خطای ۴۰۴** و **خطای ۴۰۳** وجود داره؟
)به زبان ساده توضیح بده که کی باید از ۴۰۴ استفاده کنیم و کی از ۴۰۳(

؟ سوال ۲:

فرض کن کاربر با شناسه 5وارد شده. یادداشتی که داره می‌خواد ببینه user_idش برابر با 3هست.
آیا اجازه داره این یادداشت رو ببینه؟ چرا؟ چه خطایی باید برگرده؟

؟ سوال ۳:

کد زیر چه مشکلی داره؟ چه اتفاقی می‌افته؟

```php
$note = $db->query("SELECT * FROM notes WHERE id =
            :id", ['id' => $_GET['id']])->fetch();
```

چطور باید اصلاحش کنیم تا امنیتش بهتر بشه؟

؟ سوال ۴:

این کد چه کاری انجام می‌ده؟

```
if (!$note) {
    http_response_code(404);
    header("Location: /");
    exit();
}
```

? سوال ۵:

استفاده کنیم. کدام‌یک درست Responseمی‌خوایم از ثابت‌های تعریف‌شده در کلاس است؟

A) `http_response_code(Response::NOT_FOUND);`
B) `http_response_code($Response->FORBIDDEN);`
C) `Response.http(403);`
D) `require Response::FORBIDDEN();`

? سوال ۶:

چرا نباید اجازه بدیم کاربر با تغییرURL ، یادداشت‌های دیگران رو ببینه؟ مثالی بزن که این کار چطور می‌تونه خطرناک باشه.

✋عالی بود! واقعاً خیلی خوب جواب دادی!
بیاین با هم جواب‌هات رو بررسی کنیم تا ببینیم آیا کامل و دقیق بودن یا نه:

✅جواب ۱ (فرق ۴۰۴ و ۴۰۳):

404وقتی یادداشت وجود نداره، ۴۰۳ وقتی کاربر غیرمجاز بخواد به یادداشت دسترسی داشته باشه.

🔷**نتیجه ✅ :کاملاً درست و دقیق** بود!

✅جواب ۲) آیا کاربر با ID ۵ می‌تونه یادداشت با user_id = ۳ ببینه؟:(

🔷جواب تو:

اجازه نداره، باید ۴۰۳ برگرده

🔷نتیجه ✅ :دقیق و درست

✅جواب ۳) مشکل SQL اولیه:(

🔷جواب تو:

هرکس می‌تونه از طریق URL یادداشت بقیه رو ببینه، باید شرط user_id برابر ۳ رو اضافه کنیم

🔷نتیجه ✅ :عالیه، دقیقاً منظور جفری همین بود

✅جواب ۴ (کد بررسی ۴۰۴):

🔷جواب تو:

اگر یادداشت کلاً وجود نداشت، خطای ۴۰۴ بده

🔷نتیجه ✅ :کاملاً درست

✅جواب ۵) استفاده صحیح از ثابت‌ها در کلاس:(Response

🔻جواب تو:

گزینه اول درسته Response::NOT_FOUND :

🔻نتیجه ✓ :درسته! گزینه A کاملاً درسته✋ .

✓جواب ۶) چرا نباید کاربر URL رو تغییر بده:(

🔻جواب تو:

چون هر یادداشت مال یک نفره و نباید بقیه بتونن بهش دسترسی داشته باشن

🔻نتیجه ✓ :درست و دقیق. این همون مفهوم authorization هست.

سوال:

من الان یه یادداشت که user_id برای یکی دیگه هست id رو اون بالا میزنم باط not found میده و forbidden نمیده یا به عبارت دیگه چرا وقتی ID یادداشت رو می‌زنم که مال یه کاربر دیگه‌ست، بهم ۴۰۴ می‌ده؟ چرا ۴۰۳ (forbidden) نمی‌ده؟ ؟

🎯دلیلش خیلی ساده‌ست:

به این خط از کدت دقت کن:

```
$note = $db->query("SELECT * FROM notes WHERE user_id =
:user AND id = :id", [
    'id' => $_GET['id'],
    'user' => $current_userid
])->fetch();
```

اینجا داره می‌گه:

فقط یادداشتی رو بیار که هم idش فلان باشه و هم user_idش برابر کاربر فعلی باشه.

⛔یعنی:

- اگر یادداشت برای **کاربر دیگه‌ای باشه**، اصلاً هیچ چیزی برنمی‌گرده.
- در نتیجه `$note`**می‌شه** `false`، **و اون‌وقت شرط ۴۰۴ اجرا می‌شه:**

```
if (!$note) {
    http_response_code(404);
    require "404.php";
    exit();
}
```

!یعنی کلاً به شرط ۴۰۳ نمی‌رسه، چون اصلاً یادداشت بهت برنگشته که بخوای بررسی کنی مال تو هست یا نه!

✅راه‌حل درست برای اینکه هم ۴۰۴ هم ۴۰۳ درست کار کنن:

مرحله ۱: اول فقط با `id`یادداشت رو بگیر) بدون شرط(user

```
php
CopyEdit
$note = $db->query("SELECT * FROM notes WHERE id =
:id", [
'id' => $_GET['id']
])->fetch();
```

مرحله ۲: بررسی کن اصلاً وجود داره یا نه

```
if (!$note) {
    http_response_code(404);
    require "404.php";
    exit();
}
```

مرحله ۳: حالا بررسی کن که مال کاربر فعلی هست یا نه

```
$current_userid = 3; // مثلا کاربر لاگین‌شده
```

```php
if ($note['user_id'] != $current_userid) {
    http_response_code(403);
    require "403.php";
    exit();
}
```

جمع‌بندی:

حالت	توضیح	پاسخ مناسب
یادداشت اصلاً وجود نداره	تو جدول نیست	404
یادداشت هست ولی مال کاربر دیگه‌ست	user_idفرق داره	403
یادداشت هست و مال خود کاربره	(نمایش بدیم	200نمایش یادداشت✅)

برای اینکه بخواهیم کد forbiddenرو هم بفهمیم میتونیم کد زیر را بنویسیم :

```php
require "Database.php";
require "Response.php";

$db = new Database();

$current_userid = 3; // فرضی؛ از بعداً جلسه login واقعی میاد

// 1. فقط اساس بر یادداشت گرفتن id
$note = $db->query("SELECT * FROM notes WHERE id =
:id", [
    'id' => $_GET['id']
])->fetch();

// 2. نداشت وجود یادداشت اگر → 404
```

```php
if (!$note) {
    http_response_code(Response::NOT_FOUND);
    require "views/errors/404.php";
    exit();
}

// 3. اگر یادداشت برای کاربر فعلی نبود → 403
if ($note['user_id'] != $current_userid) {
    http_response_code(Response::FORBIDDEN);
    require "views/errors/403.php";
    exit();
}

// 4. یادداشت نمایش
require "views/note.view.php";
```