

۱۰ سؤال (با جواب)

سؤال ۱:

فرق `$_SESSION = []` با `session_destroy()` چیست؟

✓جواب:

- `$_SESSION = []` فقط متغیرهای سشن در حافظه PHP رو پاک می‌کنه، ولی فایل سشن روی سرور و کوکی مرورگر باقی می‌مونه.
- `session_destroy()` فایل سشن روی سرور رو هم پاک می‌کنه، ولی کوکی مرورگر (PHPSESSID) رو دست نمی‌زنه.

سؤال ۲:

چرا بعد از `logout()` دوباره PHPSESSID جدید در Inspect ظاهر میشه؟

✓جواب:

چون بعد از حذف کوکی، اگر دوباره `session_start()` صدا زده بشه، PHP یک سشن جدید می‌سازه و کوکی جدید می‌فرسته.

سؤال ۳:

تابع `session_regenerate_id(true)` برای چه کاری استفاده میشه؟

✓جواب:

برای تغییر Session ID و جلوگیری از حمله Session Fixation. وقتی `true` باشه، Session ID قبلی کاملاً حذف میشه.

سؤال ۴:

اگر در `logout()` فقط `session_destroy()` رو صدا بزنیم، کاربر همچنان لاگین حساب میشه یا نه؟

✓ جواب:

خیر، اطلاعات سشن روی سرور پاک میشه ولی چون کوکی `PHPSESSID` هنوز تو مرورگر کاربر هست، ممکنه دوباره با همون ID سشن جدیدی ساخته بشه. پس باید کوکی هم حذف بشه.

سؤال ۵:

توی شرط منو `(if ($_SESSION['user'] ?? false) ?? false)`، چرا از `?? false` استفاده می‌کنیم؟

✓ جواب:

برای اینکه اگر کلید `user` داخل `$_SESSION` وجود نداشته `undefined` بود، خطای PHP رخ نده و مقدار پیش‌فرض `false` استفاده بشه.

سؤال ۶:

چرا لاگ‌اوت رو با `POST` یا حتی `DELETE` می‌فرستیم و نه با لینک ساده `GET`؟

✓ جواب:

چون عملیات تغییر وضعیت کاربر (`state-changing`) محسوب میشه و باید با متدهای امن `POST` یا `DELETE` انجام بشه، نه `GET` که قابل کلیک تصادفی یا کش شدن باشه.

سؤال ۷:

اگر `session_regenerate_id(false)` بز نیم چه اتفاقی می افتد؟

✓ جواب:

یک Session ID جدید ساخته میشه، ولی Session ID قبلی هم هنوز معتبر می مونه.

سؤال ۸:

تابع `session_get_cookie_params()` چه چیزی بر می گردونه و چرا استفاده می کنیم؟

✓ جواب:

آرایه ای از تنظیمات کوکی سشن مثل `lifetime, path, domain, secure, httponly`.
برای اینکه کوکی رو درست و دقیق با همون تنظیمات قبلی حذف کنیم.

سؤال ۹:

اگر کاربر با دو مرورگر مختلف لاگین کنه، آیا یک Session ID خواهند داشت؟

✓ جواب:

خیر. هر مرورگر برای خودش یک Session ID جداگانه دریافت می کنه و روی سرور دو فایل سشن ساخته میشه.

سؤال ۱۰:

اگر بخوایم کاربر فقط یک سشن فعال داشته باشه (یعنی لاگین از مرورگر جدید لاگین قبلی رو ببندد)، باید چه کار کنیم؟

✓جواب:

باید در دیتابیس یک ستون برای ذخیره Session ID داشته باشیم. وقتی کاربر لاگین کرد Session ID جدید ثبت میشه و قبلی نامعتبر میشه.

۳۰ تمرین (با جواب)

تمرین ۱:

یک شرط بنویس که اگر کاربر لاگین کرده بود پیام "Welcome, [email]" نشون بده، وگرنه پیام "Please log in".

✓جواب:

```
<?php if ($_SESSION['user'] ?? false): ?>
    <p>Welcome, <?= $_SESSION['user']['email'] ?></p>
<?php else: ?>
    <p>Please log in</p>
<?php endif; ?>
```

تمرین ۲:

منو "Profile" رو فقط وقتی کاربر لاگین کرده باشه نشون بده.

✓جواب:

```
<?php if ($_SESSION['user'] ?? false): ?>
    <a href="/profile">Profile</a>
<?php endif; ?>
```

تمرین ۳:

کدی بنویس که وقتی کاربر لاگین میکنه، علاوه بر ایمیل، IP کاربر رو هم توی سشن ذخیره کنه.

✓جواب:

```
function login($user) {  
    $_SESSION['user'] = [  
        'email' => $user['email'],  
        'ip' => $_SERVER['REMOTE_ADDR']  
    ];  
    session_regenerate_id(true);  
}
```

تمرین ۴:

یک شرط بنویس که اگر کاربر لاگین نبود، خودکار به صفحه لاگین ریダイرکت بشه.

✓جواب:

```
if (! ($_SESSION['user'] ?? false)) {  
    header("Location: /login");  
    exit;  
}
```

تمرین ۵:

توی منوها، اگر مسیر فعلی با لینک منو یکی بود، کلاس active اضافه کن.

✓جواب:

```
<a href="<?=$key?>" class="<?= ($current == $key) ?  
'active' : '' ?>">  
    <?=$value?>  
</a>
```

تمرین ۶:

کدی بنویس که همه داده‌های سشن (به جز ایمیل کاربر) پاک بشن.

✓جواب:

```
foreach ($_SESSION as $key => $value) {  
    if ($key !== 'user') {  
        unset($_SESSION[$key]);  
    }  
}
```

تمرین ۷:

یک دکمه "Log out" بساز که با کلیک، کاربر کامل خارج بشه.

✓جواب:

```
<form action="/logout" method="post">  
    <button type="submit">Log out</button>  
</form>
```

تمرین ۸:

تابعی بنویس که بررسی کنه آیا کاربر ادمین هست یا نه (با فرض اینکه توی
\$_SESSION['user']['role'] ذخیره شده).

✓جواب:

```
function isAdmin() {  
    return ($_SESSION['user']['role'] ?? '') ===  
    'admin';  
}
```

تمرین ۹:

کدی بنویس که فقط کاربرانی با role = "admin" بتوانن به صفحه notes دسترسی داشته باشن.

✓جواب:

```
if (! isAdmin()) {  
    header("Location: /");  
    exit;  
}
```

تمرین ۱۰:

تابعی بنویس به نام `isLoggedIn()` که اگر کاربر لاگین بود `true` بدهد، وگرنه `false`.

✓جواب:

```
function isLoggedIn() {  
    return isset($_SESSION['user']);  
}
```