

Sesje i ciasteczka

Czas: 2 × 45 min

praca indywidualna

Cel: Zapamiętywanie stanu w bezstanowym protokole HTTP: licznik odwiedzin i preferencja motywu w ciasteczkach z właściwymi atrybutami oraz koszyk zakupów w sesji PHP, sprawdzane w narzędziach F12.

Po zajęciach potrafisz:

- ustawia, odczytuje i usuwa ciasteczka funkcją `setcookie` z atrybutami `expires`, `path`, `HttpOnly`, `SameSite`
- wyjaśnia znaczenie atrybutu `Secure` i powód jego pominięcia na `http://localhost`
- korzysta z sesji (`session_start`, `$_SESSION`) do przechowywania koszyka
- obsługuje dodawanie, zmniejszanie i czyszczenie koszyka metodą POST z wzorcem PRG
- odczytuje ciasteczka i nagłówki `Set-Cookie` w narzędziach F12

Sprzęt i materiały

- komputer z Windows 11 i XAMPP
- folder `r2_11_start` z Pliki_do_zadan (`produkty.php`, `styl.css`)

Oprogramowanie

- **XAMPP (Apache, PHP 8, MariaDB, phpMyAdmin)** — projekt w folderze `C:\xampp\htdocs`
[apachefriends.org/download.html](https://httpd.apache.org/download.html)
- **Visual Studio Code**
code.visualstudio.com
- **Przeglądarka Chrome, Edge lub Firefox** — narzędzia deweloperskie F12 (Elementy, Konsola, Sieć, Aplikacja)

Przygotowanie przed zajęciami

- Przeglądnij wykład 2.09 (cookies, sesje, atrybuty ciasteczek, RODO).

Bezpieczeństwo

- Wartość ciasteczka pochodzi od przeglądarki i może być dowolna — przed użyciem sprawdzaj ją (lista dozwolonych wartości, `filter_var`).
- Nie wyświetlaj identyfikatora sesji na stronie i nie przekazuj go w adresie URL — kto go zna, może przejąć sesję.
- Ciasteczka preferencji (inne niż niezbędne) na prawdziwej stronie wymagają zgody użytkownika; w ćwiczeniu wystarczy informacja na stronie.

Przebieg zadania

1 Wspólny plik i sesja

Skopiuj pliki do `C:\xampp\htdocs\nazwisko_z11`. Utwórz `wspolne.php` dołączany na początku każdej strony — przed jakimkolwiek HTML (ciasteczka i sesja wysyłają nagłówki).

```
session_set_cookie_params(['lifetime' => 0, 'path' => '/', 'httponly' => true, 'samesite' => 'Lax']);
session_start();
require __DIR__ . '/produkty.php';
```

- W `wspolne.php` uruchom sesję jak wyżej, odczytaj motyw z ciasteczka `motyw` (dozwolone tylko `jasny` / `ciemny`, domyślnie `jasny`), koszyk z `$_SESSION['koszyk']` (tablica id → ilość) i liczbę sztuk (`array_sum`).
- Napisz funkcję `naglowek($tytul, $motyw, $sztuk)`, która wypisuje początek strony: `body` z klasą `ciemny` przy motywie ciemnym oraz menu Start, Sklep, „Koszyk (N)”.

2 Ciasteczka: licznik i motyw (index.php)

- Licznik odwiedzin: odczytaj `$_COOKIE['odwiedziny']` (liczba całkowita ≥ 0 , w przeciwnym razie 0), zwiększ o 1 i zapisz `setcookie('odwiedziny', ..., [opcje])` na 30 dni z `path`, `httponly` i `samesite = Lax`. Pierwsza wizyta: „Jesteś u nas pierwszy raz”, kolejne: „Odwiedzasz nas po raz N.”.
- Formularz POST z przyciskami „Jasny” i „Ciemny” zapisuje ciasteczko `motyw` na 365 dni, a następnie przekierowuje na `index.php` (PRG). Sprawdź, że motyw działa na obu podstronach i po zamknięciu przeglądarki.
- Przycisk „Usuń moje ciasteczka” usuwa `motyw` i `odwiedziny` (ta sama nazwa i ścieżka, data wygaśnięcia w przeszłości).
- Dodaj w opcjach `'secure' => true`, odśwież stronę kilka razy i zapisz, co dzieje się z licznikiem na `http://localhost` (w Chrome i w Firefoksie, jeśli masz). Wyłącz opcję i dopisz komentarz, kiedy należy ją włączyć.

3 Koszyk w sesji (sklep.php)

Wszystkie zmiany koszyka wykonuj metodą POST (formularz z ukrytym polem `id` i przyciskiem `name="akcja"`), a po obsłudze przekieruj na `sklep.php`.

- Wyświetl produkty z ceną i przyciskiem „Do koszyka” (akcja `dodaj`). Dodawaj tylko id istniejące w `$produkty`.
- Pod listą pokaż koszyk: produkt, ilość, wartość, przycisk „-1” (akcja `usun`, przy zerze pozycja znika), wiersz „Razem” z liczbą sztuk i kwotą oraz przycisk „Wyczyść koszyk” (akcja `wyczysc`, `unset`). Pusty koszyk: „Koszyk jest pusty.”.
- Test: 2 × Bazylia, 1 × Doniczka, -1 Bazylia, 1 × Pomidor. Zapisz kwotę. Otwórz stronę w oknie prywatnym (incognito) — co jest w koszyku i dlaczego?

4 Analiza w F12

- F12 → Aplikacja (Firefox: Dane) → Ciasteczka: zapisz w tabeli nazwę, wartość, datę wygaśnięcia, HttpOnly i SameSite dla `PHPSESSID`, `motyw`, `odwiedziny`.
- W konsoli F12 wpisz `document.cookie` i porównaj z tabelą. W zakładce Sieć znajdź odpowiedź z nagłówkiem `Set-Cookie`. Zrób zrzuty, spakuj folder.

W sprawozdaniu umieść

- ☐ tabela ciasteczek z F12 (nazwa, wartość, wygaśnięcie, HttpOnly, SameSite)
- ☐ wynik `document.cookie` i zrzut nagłówka `Set-Cookie` z zakładki Sieć
- ☐ wynik testu koszyka i obserwacja w oknie prywatnym

- ☐ obserwacja licznika z włączonym `secure` na `http://localhost`
- ☐ kod obsługi koszyka (akcje dodaj, usun, wyczysc)
- ☐ spakowany folder `nazwisko_z11`

Pytania kontrolne

1. Czym różni się przechowywanie danych w ciasteczku od przechowywania w sesji? Gdzie fizycznie leży koszyk?
2. Co dają atrybuty `HttpOnly`, `Secure` i `SameSite=Lax`?
3. Dlaczego `setcookie` i `session_start` muszą być wywołane przed wysłaniem jakiegokolwiek HTML?
4. Po co wywołuje się `session_regenerate_id(true)` po zalogowaniu użytkownika?

Kryteria oceny

Kryterium	Punkty
wspolne.php: parametry ciasteczka sesji, walidacja motywu, funkcja nagłówka z licznikiem koszyka	3
Licznik odwiedzin z walidacją i atrybutami, komunikat pierwszej i kolejnej wizyty	3
Motyw w ciasteczku (POST + PRG) na obu podstronach, usuwanie ciasteczek, test Secure	4
Koszyk w sesji: dodaj, -1, wyczyść, suma, pusty koszyk, PRG, kontrola id	5
Analiza F12 (tabela ciasteczek, document.cookie, Set-Cookie) i test okna prywatnego	3
Odpowiedzi na pytania	2
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).