

Bezpieczne zapytania w aplikacji

Czas: 2 × 45 min

praca indywidualna

Cel: Poprawienie aplikacji PHP tak, aby dane od użytkownika nigdy nie stawały się częścią polecenia SQL, a aplikacja łączyła się z bazą kontem o minimalnych uprawnieniach i nie ujawniała szczegółów błędów.

Po zajęciach potrafisz:

- wyjaśnia, dlaczego sklepanie zapytania z danymi z formularza jest błędem
- stosuje zapytania przygotowane PDO (prepare, execute, parametry ? i :nazwa)
- zabezpiecza nazwy kolumn w ORDER BY białą listą
- tworzy konto aplikacji z minimalnymi uprawnieniami i sprawdza ich działanie
- obsługuje błędy bazy bez pokazywania ich użytkownikowi i stosuje htmlspecialchars

Sprzęt i materiały

- komputer z XAMPP (Apache, PHP 8, MariaDB 10.4)
- plik `r2_19_klienci_start.php` z folderu Pliki_do_zadan
- świeżo zaimportowana baza `sklep`

Oprogramowanie

- **XAMPP** — pliki PHP w `C:\xampp\htdocs`, dziennik błędów `C:\xampp\apache\logs\error.log`
apachefriends.org/download.html
- **VS Code** — edycja PHP
code.visualstudio.com
- **Dokumentacja PHP — PDO** — prepare, execute, PDOException
php.net/manual/pl/book.pdo.php
- **OWASP — SQL Injection Prevention Cheat Sheet** — lista zasad obrony
cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Przygotowanie przed zajęciami

- Przypomnij sobie z prezentacji 2.12 zasadę „dane to nie kod” i budowę zapytania przygotowanego w PDO.

Bezpieczeństwo

- Testuj wyłącznie własną aplikację na `localhost`. Sprawdzanie zabezpieczeń cudzych stron i serwerów bez pisemnej zgody właściciela jest niezgodne z prawem.
- W zadaniu używamy tylko zwykłych danych (nazwiska z apostrofem, polskie znaki). Nie szukaj i nie wpisuj „ataków” — celem jest poprawny kod, a nie łamanie zabezpieczeń.
- Hasło konta aplikacji wymyśl sam (min. 12 znaków) i nie wpisuj go do sprawozdania — w sprawozdaniu zastąp je gwiazdkami.
- Nie wystawiaj XAMPP do sieci (domyślnie nasłuchuje lokalnie) i na koniec usuń konto testowe, jeśli nauczyciel tak poleci.

Przebieg zadania

1 Diagnostyka kodu startowego

Skopiuj `r2_19_klienci_start.php` do `C:\xampp\htdocs` i otwórz `http://localhost/r2_19_klienci_start.php`.

1. Z1. Wyszukaj klientów, których nazwisko zaczyna się od „Now”. Działa?
2. Z2. Dodaj klienta: Liam O'Connor, liam.oconnor@example.ie, Kraków. Zapisz komunikat. Wyszukaj nazwisko zaczynające się od „O”.
3. Z3. W kodzie zaznacz (komentarzem `// PROBLEM`) każde miejsce, w którym dane od użytkownika trafiają do SQL lub do HTML bez zabezpieczenia, oraz miejsca ujawniające szczegóły błędów. Wypisz je w sprawozdaniu (powinno być co najmniej 6).

2 Konto aplikacji z minimalnymi uprawnieniami

Wykonaj w konsoli `mysql -u root`.

1. Z4. Utwórz użytkownika `sklep_www@localhost` z własnym hasłem i nadaj mu tylko SELECT i INSERT na tabeli `sklep.klienci`. Wyświetl `SHOW GRANTS`.
2. Z5. Zaloguj się jako `sklep_www` (`mysql -u sklep_www -p sklep`) i sprawdź: SELECT z `klienci`, DELETE z `klienci`, SELECT z `zamowienia`, DROP TABLE `klienci`, SHOW DATABASES. Zapisz, które polecenia zostały odrzucone i jakim błędem.

3 Nowa wersja: PDO i zapytania przygotowane

Utwórz plik `klienci.php` (nie zmieniaj pliku startowego — porównasz oba).

```
$pdo = new PDO('mysql:host=localhost;dbname=sklep;charset=utf8mb4', 'sklep_www', '...', [
    PDO::ATTR_ERRMODE            => PDO::ERRMODE_EXCEPTION,
    PDO::ATTR_DEFAULT_FETCH_MODE => PDO::FETCH_ASSOC,
    PDO::ATTR_EMULATE_PREPARES  => false,
]);
// dalej: prepare(...) z ? lub :nazwa, execute([...]) – bez sklejanego danych
```

1. Z6. Połącz się kontem `sklep_www` w bloku try/catch. Przy błędzie połączenia zapisz szczegóły funkcją `error_log()`, a użytkownikowi pokaż tylko „Serwis chwilowo niedostępny”. Ustaw `display_errors` na 0.
2. Z7. Napisz wyszukiwanie przez `prepare` z warunkiem `nazwisko LIKE ?` — znak `%` dodaj do wartości parametru, nie do treści SQL.
3. Z8. Napisz dodawanie klienta przez `prepare` z parametrami nazwanymi. Przed zapisem sprawdź: imię i nazwisko niepuste, e-mail poprawny (`filter_var(..., FILTER_VALIDATE_EMAIL)`). Puste miasto zapisz jako NULL.
4. Z9. Obsłuż powtórzony e-mail (błąd 1062, `$e->errorInfo[1]`) komunikatem „Ten e-mail jest już zarejestrowany.”, a inne błędy — ogólnym komunikatem i wpisem w dzienniku.
5. Z10. Sortowanie: nazwy kolumn nie da się przekazać parametrem — zastosuj białą listę (tablica dozwolonych kolumn, domyślnie `nazwisko`) i kierunek tylko ASC albo DESC.
6. Z11. Wszystkie dane wypisywane w HTML (wyniki i wartość pola wyszukiwania) przepuść przez `htmlspecialchars(..., ENT_QUOTES, 'UTF-8')`.

4 Testy i lista kontrolna

1. Z12. Przetestuj nową wersję: dodaj Liama O'Connora i Giulie D'Angelo, wyszukaj „O'”, dodaj drugi raz ten sam e-mail, wpisz niepoprawny e-mail, podaj w adresie `?sort=cena` i `?sort=miasto&kier=desc`. Zapisz wyniki w tabeli testów.
2. Z13. Sprawdź w `C:\xampp\apache\logs\error.log`, że szczegóły błędu 1062 trafiły do dziennika, a nie na stronę.
3. Z14. Wypełnij w sprawozdaniu listę kontrolną bezpiecznej aplikacji i porównaj obie wersje kodu.

W sprawozdaniu umieść

- ☐ lista problemów znalezionych w kodzie startowym (Z3)
- ☐ polecenia tworzenia konta aplikacji i wyniki testu uprawnień (Z4–Z5, hasło zamaskowane)
- ☐ kod `klienci.php` z komentarzami
- ☐ tabela testów Z12 i fragment dziennika błędów z Z13
- ☐ wypełniona lista kontrolna
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego nazwisko O'Connor zepsuło zapytanie w wersji startowej i dlaczego w wersji z PDO działa bez żadnego „escapowania”?
2. Dlaczego nazwy kolumny w ORDER BY nie można przekazać jako parametru zapytania przygotowanego i jak sobie z tym radzimy?
3. Jakie korzyści daje konto aplikacji z uprawnieniami tylko SELECT i INSERT zamiast konta root?
4. Dlaczego pokazywanie użytkownikowi treści błędu SQL jest złą praktyką? Gdzie powinny trafiać szczegóły błędów?

Kryteria oceny

Kryterium	Punkty
Diagnoza kodu startowego (Z1–Z3)	3
Konto aplikacji i test uprawnień (Z4–Z5)	3
Zapytania przygotowane, walidacja i obsługa błędów (Z6–Z9)	6
Biała lista sortowania i htmlspecialchars (Z10–Z11)	3
Testy, dziennik i lista kontrolna (Z12–Z14)	3
Odpowiedzi na pytania kontrolne	2
Razem	20

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