

ТЕМА 18 · ЗАВЕРШАЛЬНА

Безпека бекенду

Типові вразливості, захист від них — і підсумок усього курсу

Бекенд-розробка, сервіси та мікросервіси

Комп'ютерна інженерія · 3 курс · Лекція 18 з 18

7 питань завершальної лекції

01

Безпека — наскрізна
відповідальність

02

Ін'єкції: SQL, XSS

03

Автентифікація: типові
вразливості

04

Контроль доступу та
CSRF

05

Чутливі дані та секрети

06

Безпека залежностей

07

Підсумок курсу

Уже розглянуто протягом курсу

Категорія OWASP	Де вже розглядалося
Ін'єкції (SQL, XSS)	Теми 6, 7 — підготовлені запити, екранування
Порушена автентифікація	Тема 8 — хешування паролів, сесії, JWT
Порушений контроль доступу	Теми 8, 9 — ролі, права доступу
Розкриття чутливих даних	Теми 14, 15 — секрети, HTTPS
Вразливі компоненти	Теми 15, 16 — залежності, CI/CD

SQL-ін'єкція (тема 7)

НЕБЕЗПЕЧНО

```
$sql = "SELECT * FROM users  
WHERE login = '  
  . $_POST['login'] . "'";
```

БЕЗПЕЧНО

```
$stmt = $pdo->prepare(  
    'SELECT * FROM users  
    WHERE login = :login');  
$stmt->execute([  
    'login' => $_POST['login']  
]);
```

XSS (тема 6)

НЕБЕЗПЕЧНО

```
echo "<p>{$comment}</p>";  
  
// $comment може містити  
// <script>...</script>
```

БЕЗПЕЧНО

```
echo '<p>' . htmlspecialchars(  
    $comment,  
    ENT_QUOTES,  
    'UTF-8'  
) . '</p>';
```

Обидва захисти — прояв одного принципу: розділяти дані від коду (SQL чи HTML).

Вразливість → захист (тема 8)

Вразливість	Захист
Паролі у відкритому вигляді	password_hash() з bcrypt
Брутфорс-атака	Обмеження спроб входу
Enumeration-атака	Однакове повідомлення про помилку
Session fixation	session_regenerate_id() після входу
Перехоплення cookie	HttpOnly, Secure, тільки HTTPS

Порушень контроль доступу

```
// НЕБЕЗПЕЧНО: перевіряється лише факт автентифікації
public function show(int $orderId): void {
    requireLogin();
    $order = $this->repository->findById($orderId);
    echo json_encode($order); // будь-хто бачить БУДЬ-ЯКЕ замовлення
}

// БЕЗПЕЧНО: перевіряється власник ресурсу
public function show(int $orderId): void {
    requireLogin();
    $order = $this->repository->findById($orderId);
    if ($order['userId'] !== $_SESSION['user_id']) {
        http_response_code(403);
        exit;
    }
    echo json_encode($order);
}
```

CSRF: підроблений запит від жертви

Зловмисний сайт змушує браузер жертви (вже автентифікованої через cookie) непомітно надіслати запит на зміну даних від її імені.

Захист: CSRF-токен. REST API з токеном у заголовку Authorization (не cookie) природно стійкіший — сторонній сайт не може додати довільний заголовок.

Ризик → захист (теми 14-15)

Ризик	Захист
Паролі БД у Git-репозиторії	Змінні середовища, .env поза Git
Дані відкритим текстом	HTTPS для всіх з'єднань
Детальні помилки на production	Узагальнене повідомлення, деталі в лог
Застарілі залежності	Регулярне оновлення, перевірка в CI

Навіть видалений пізніше секрет залишається в історії Git-комітів — .env одразу в .gitignore.

composer audit у CI/CD

```
$ composer audit  
# Перевіряє залежності на відомі вразливості (CVE)  
  
$ composer outdated
```

Той самий принцип — базові Docker-образи (тема 15) теж оновлюються. Перевірку варто автоматизувати як крок CI/CD-пайплайна (тема 16).

Три фази курсу

Теми 1-6

Фундамент мови

Синтаксис, типи, умови, цикли,
функції, ООП

Теми 7-11

Повноцінний застосунок

PDO, авторизація, MVC, REST API,
тести

Теми 12-18

Розподілена система

Мікросервіси, Docker, CI/CD,
спостережуваність, безпека

Ключове запитання кожного блоку

Блок тем	Запитання
1-6: Фундамент мови	Як написати код, що коректно обробляє дані?
7-11: Повноцінний застосунок	Як структурувати й перевірити застосунок?
12-14: Архітектура системи	Коли й навіщо розділяти на сервіси?
15-17: Production	Як розгортати й спостерігати за системою?
18: Безпека	Як захистити все від типових атак?

Вісімнадцять тем — один шлях

1
PHP основи

2
Змінні й типи

3
Умови й цикли

4
Функції, ООП

5
JSON/файли/cURL

6
HTTP-запити

7
PDO, БД

8
Автентифікація

9
MVC

10
REST API

11
Тестування

12
Мікросервіси

13
Комунікація

14
Інфраструктура

15
Docker

16
CI/CD

17
Спостережуваність

18
Безпека

КУРС ЗАВЕРШЕНО

Від першого echo до production-мікросервісу

Дякуємо за увагу протягом усіх 18 лекцій курсу

Бекенд-розробка, сервіси та мікросервіси