ЕТИЧНИЙ ХАКІНГ ВЛАСНОГО ЗАСТОСУНКУ

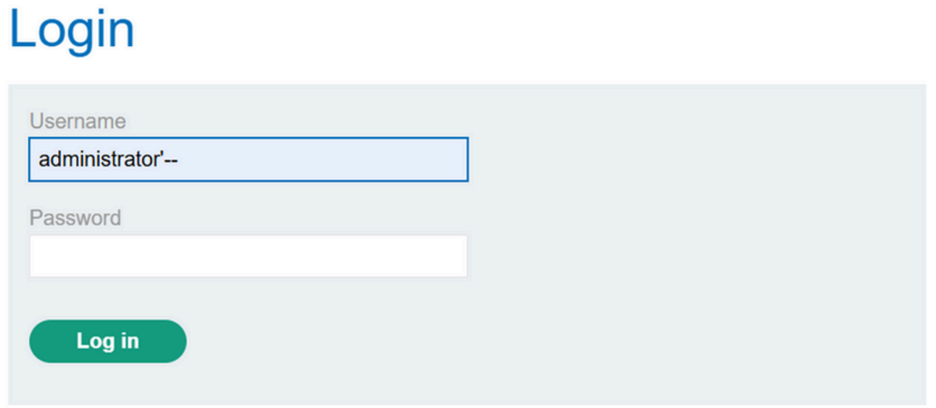
Виконав Полулях Андрій

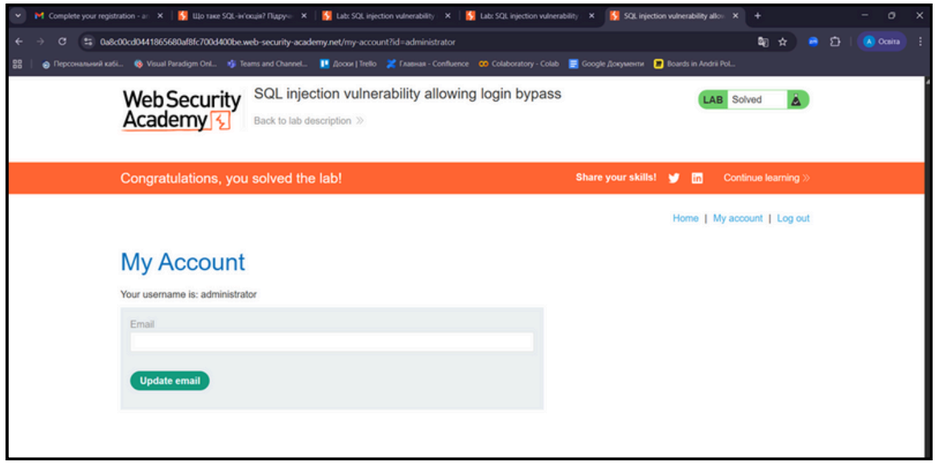
КРОК 1. ДОСЛІДЖЕННЯ SQL-ІН'ЄКЦІЙ НА ГОТОВИХ ПЛАТФОРМАХ

База даних читає цю умову як: «Покажи мені всі продукти, де категорія дорівнює 'Lifestyle' АБО де 1 дорівнює 1», а оскільки 1=1 завжди є істиною, результат умови WHERE стає TRUE для кожного рядка в таблиці й база даних повертає всі товари з таблиці, навіть приховані

КРОК 1. ДОСЛІДЖЕННЯ SQL-ІН’ЄКЦІЙ НА ГОТОВИХ ПЛАТФОРМАХ

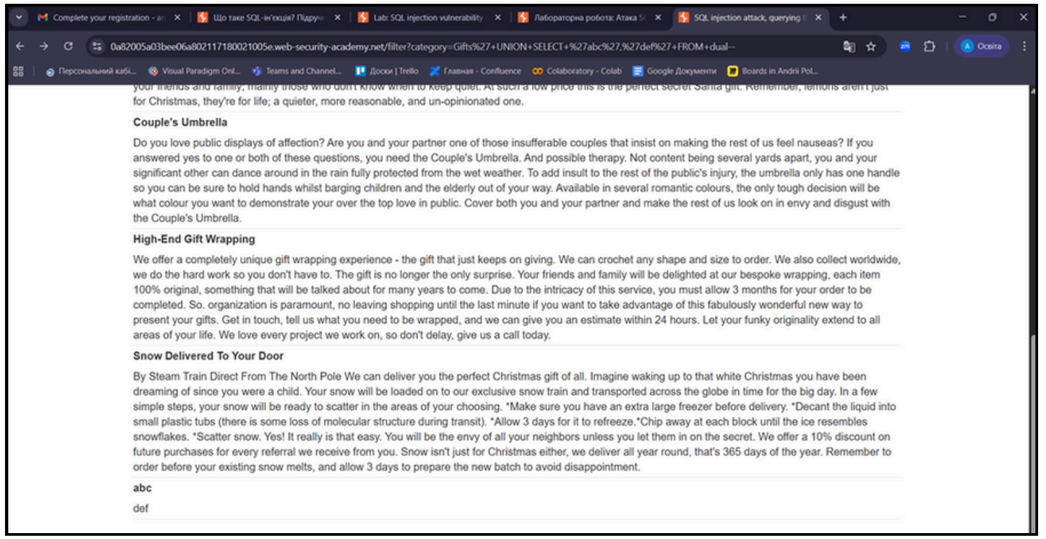
Мета ін’єкції змусити базу даних забути перевірити пароль і увійти в систему з чужим ім’ям





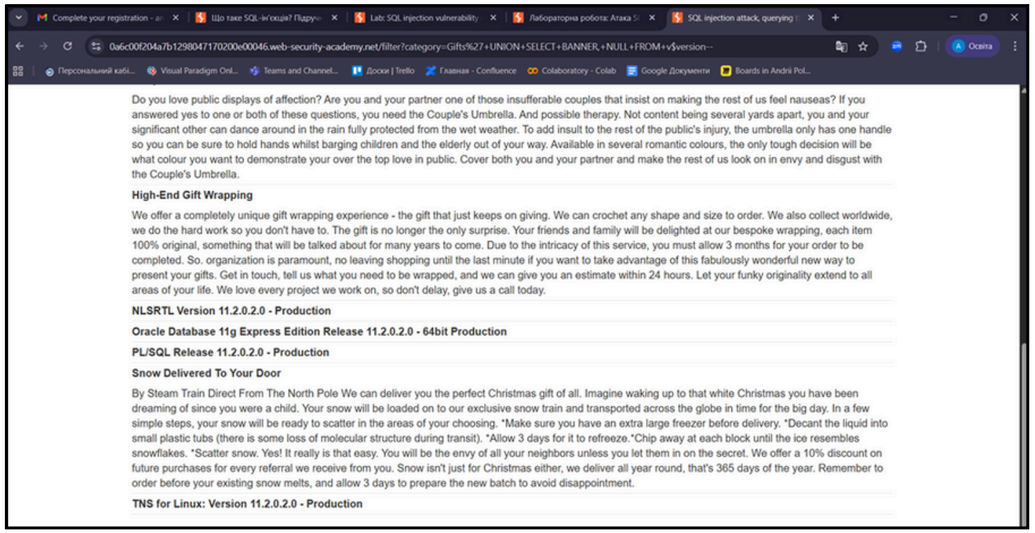
КРОК 1. ДОСЛІДЖЕННЯ SQL-ІН’ЄКЦІЙ НА ГОТОВИХ ПЛАТФОРМАХ

Запит '+UNION+SELECT+'abc','def'+FROM+dual-- допомагає визначити кількість стовпців, які повертає запит , і які стовпці містять текстові дані. Знання кількості стовпців і їхніх типів є необхідністю для атаки UNION, оскільки оператор UNION вимагає, щоб обидва запити мали абсолютно однакову кількість стовпців



КРОК 1. ДОСЛІДЖЕННЯ SQL-ІН’ЄКЦІЙ НА ГОТОВИХ ПЛАТФОРМАХ

Намагаємося дізнатися версію бази даних, використовуючи запит '+UNION+SELECT+BANNER,+NULL+FROM+v$version--, де BANNER назва стовпця в системній таблиці Oracle, який містить текст версії бази даних, а FROM v$version це системна таблиця в Oracle, яка містить інформацію про версію.



КРОК 2. АНАЛІЗ ПРИНЦИПІВ SQL-ІН’ЄКЦІЙ

Приклад 1.

До виправлення:

SELECT * FROM products WHERE category = '$category' AND released = 1

Після виправлення:

SELECT * FROM products WHERE category = ? AND released = 1

КРОК 2. АНАЛІЗ ПРИНЦИПІВ SQL-ІН’ЄКЦІЙ

Приклад 2.

До виправлення:

SELECT * FROM users WHERE username = '$username' AND password = '$password'

Після виправлення:

SELECT * FROM users WHERE username = ? AND password = ?

КРОК 2. АНАЛІЗ ПРИНЦИПІВ SQL-ІН'ЄКЦІЙ

Небезпечний варіант:

```php
$category = $_GET['category'];

$sql = "SELECT * FROM products WHERE category = '$category' AND released = 1";
```

Безпечний варіант:

```php
$category = $_GET['category'];

$stmt = $pdo->prepare('SELECT * FROM products WHERE category = ? AND released = 1');
$stmt->execute([$category]);
```

КРОК 3. ТЕСТУВАННЯ НА ПРАКТИЦІ

Критерій	Вразлива версія	Захищена версія
Вхідні дані	Lifestyle' OR 1=1--	Lifestyle' OR 1=1--
SQL-запит, що виконав сервер	SELECT ... WHERE category = 'Lifestyle' OR 1=1--'	SELECT ... WHERE category = ? (дані окремо)
Результат на екрані	Відображено всі товари з усіх категорій	Система повідомить про помилку, оскільки категорія з назвою «Lifestyle' OR 1=1--» не існує
Поведінка системи	Логіку запиту змінено. Умова OR спрацювала	Логіку збережено. Вхідні дані прийнято як текст

ДЯКУЮ ЗА УВАГУ