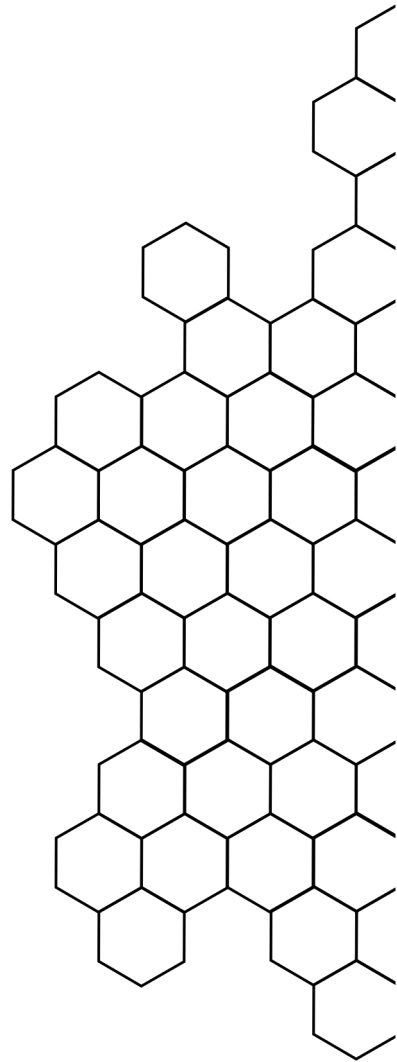
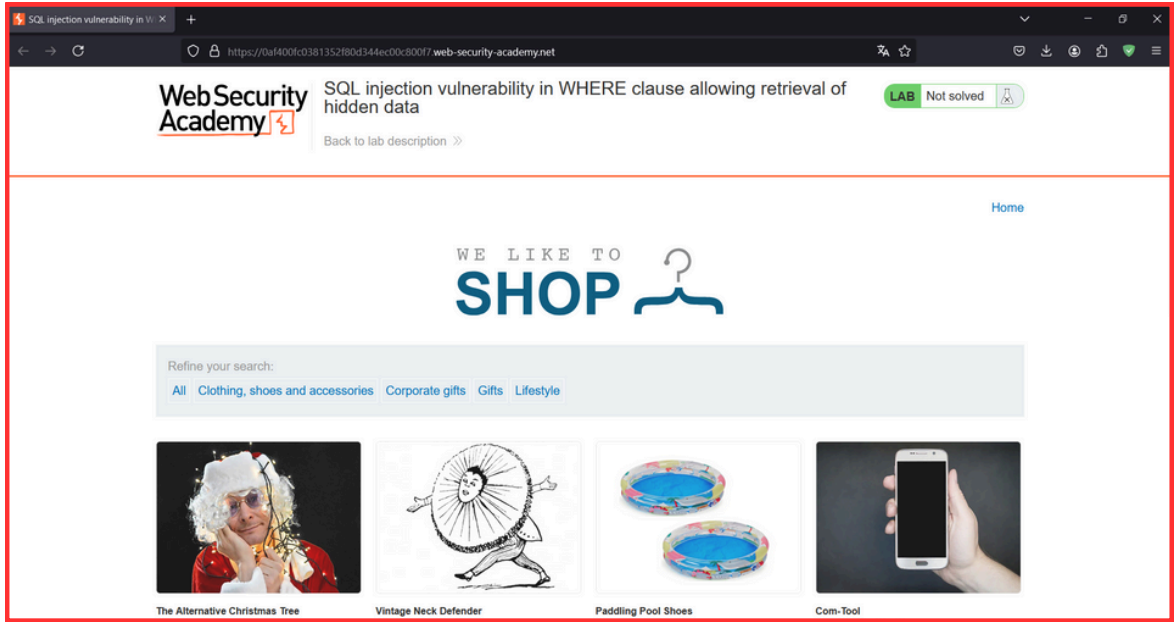


INJECTION

LAB 1

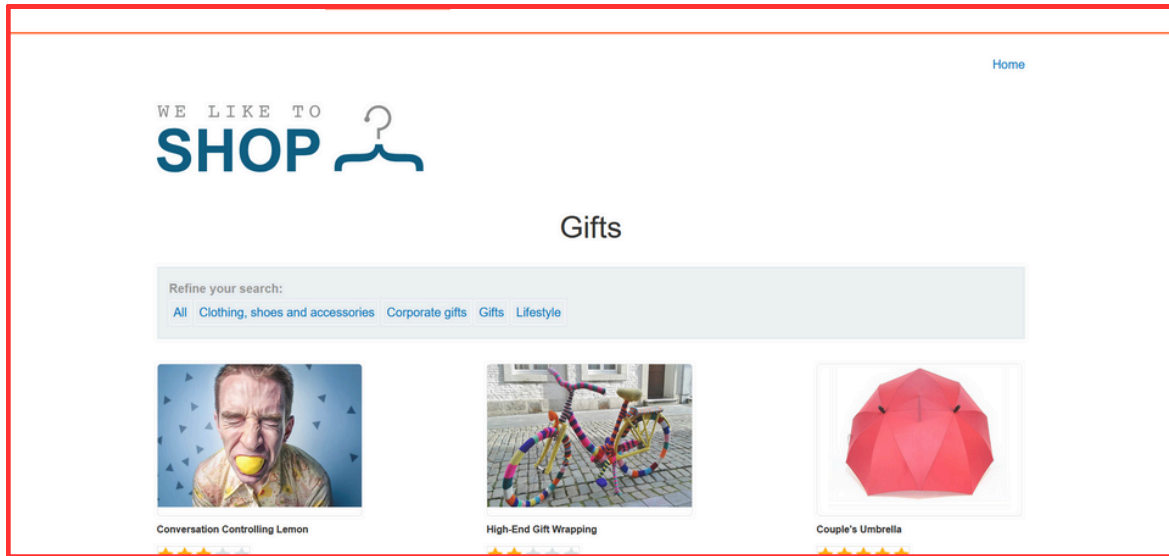
TARİH: 29.08.2024





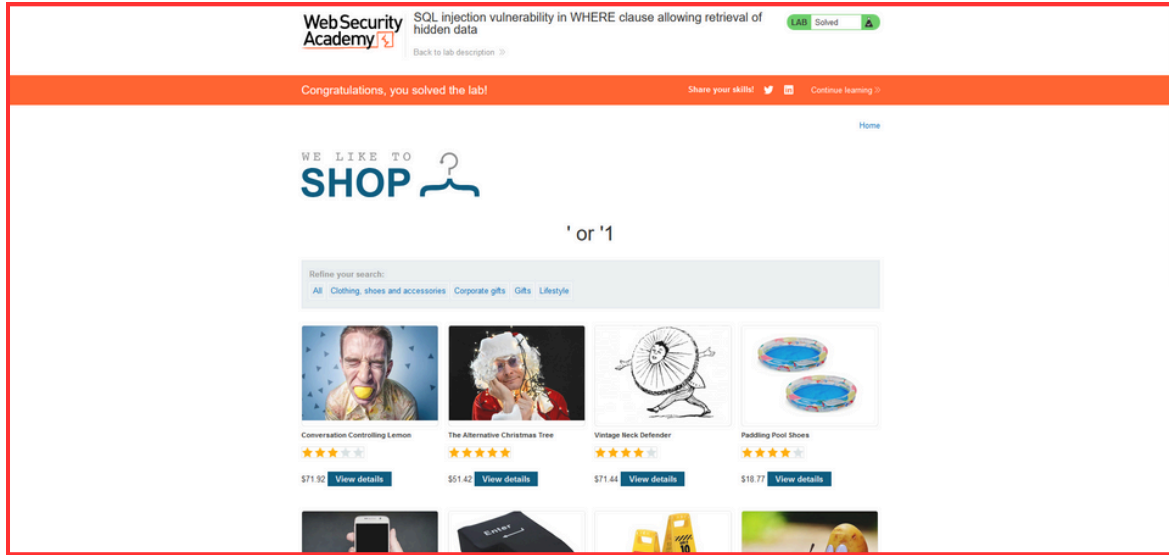
Sayfaya giriş yaptık ve WHERE parametresi kullanıldığı için ortaya çıkan zafiyeti bulmamız gerek. Diğer lablardan farklı olan ortadaki kategori kısmı dikkatimi çekti. İncelemek için bir kategoriye tıkladım.

<https://0af400fc0381352f80d344ec00c800f7.web-security-academy.net/filter?category=Gifts>



Kategori seçtiğimde URL kısmında da category adında bir parametreyle beraber seçtiğim kategoriyi gördüm. Burada SQL Injection zafiyeti olma ihtimali var o yüzden payload deneyebilirim.

https://0af400fc0381352f80d344ec00c800f7.web-security-academy.net/filter?category=' or '1



SQL Injection zafiyeti olup olmadığını anlamak için kısaca ' or '1 payloadını denedim. Ardından tüm ürünler ekrana geldi böylece SQL Injection zafiyetini tespit ederek labı tamamladık.