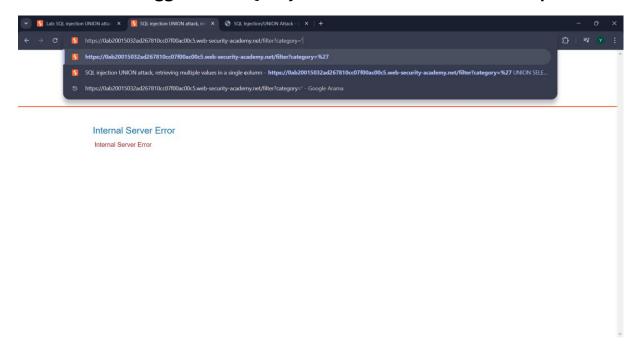
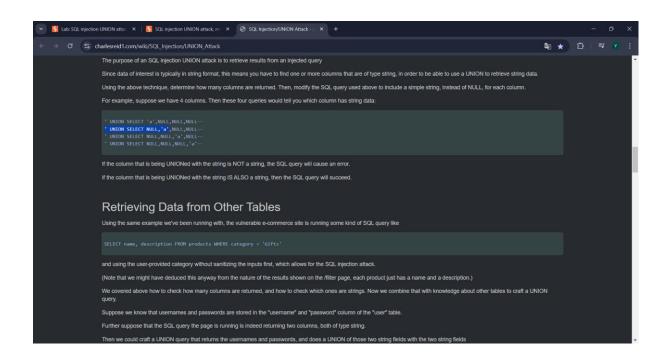
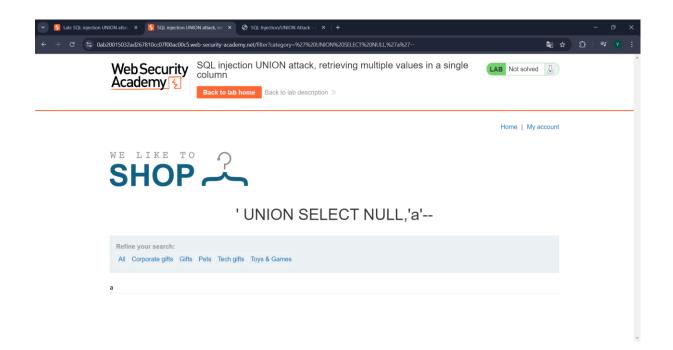
## Portswigger Lab: SQL Injection UNION Attack Write-Up

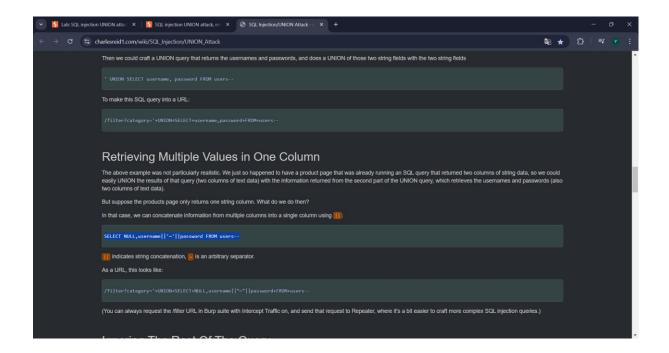


İlk adımda categoryler kısmına bakarken injection olduğunu farkettim ve bunu (ʻ,\) kullanarak doğruladım.

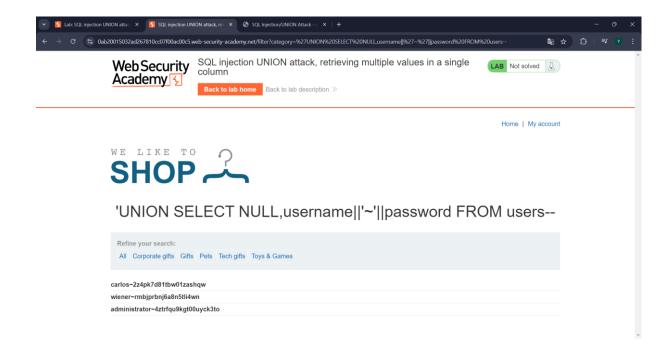


Sonrasında bulduğum bir sitedeki union sorgularını denedim ve veri tabanında komut çalıştırmayı başardım. Bu sorgu veri tabanında ilk sütunu null girip ikinci sütun için a değerini işledi ve çalıştığını gözlemledim. Tablonun 2 sütunlu olduğunu anladım. Bu sorguda a değerinin yerinin ikinci sütunda olma sebebi veri tabanı asıl sorguya göre hareket etmesiydi. Ben de veri tabanına uyum sağlamak için ikinci sütunda işlem yapmaya çalıştım.

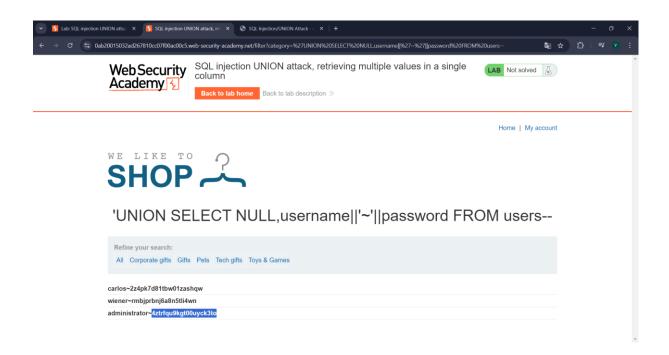




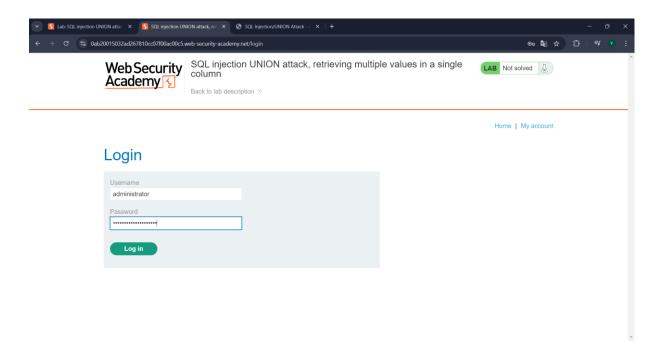
Buradaki sorguda da ikinci sütunda 2 sütun birden çekmeyi deniyorum tam benim ihtiyacım olan sorgu buydu. Çünkü benden username ve password isteniliyordu ve bu sorgunun başına union ekleyip gönderdiğimizde istediğime ulaşıyorum.



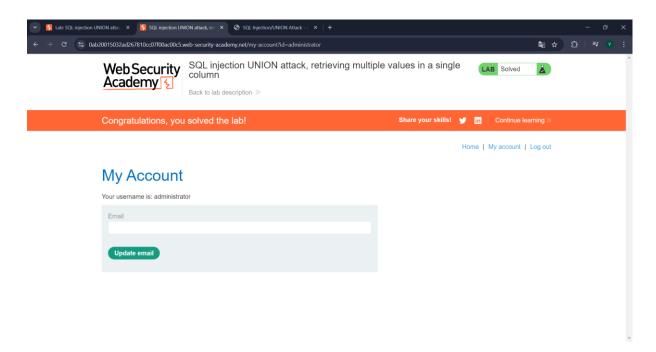
Burada sadece başına 'union ekledim ve böylelikle yukarıdaki çıktıyı aldım.



Sonrasında benden administrator kullanıcına giriş yapmam isteniliyor



Bulduğum bilgileri kullanarak giriş yaptım.



Giriş işlemi başarıyla gerçekleşti.