

PortSwigger Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data


Herkese selamlar ben Mansur Derda. Bugün PortSwigger üzerinde bulunan SQL injection zafiyetinin 1. laboratuvarını anlatacağım

Soru metninde de verildiği üzere WHERE ifadesindeki SQL enjeksiyonu güvenlik açığı gizli verilerin alınmasına izin veriyor. Yani bizden istenen aşağıda verilen sorguyu kullanarak listelenmesine izin verilmeyen ürünlere erişim sağlamak.

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

Öncelikle yukarıdaki sorgunun nasıl çalıştığına bir göz atalım;

"SELECT *" ile products tablosundaki tüm sütunları seçiyoruz. "WHERE" ile filtreleme yapıp category sütununda Gifts değeri ile tutulan tüm verileri sonuca ekliyoruz. "AND" ile yeni işlem ekleyip relased sütununda değeri 1 yani piyasaya sürülmüş ürünleri de listeliyoruz.



web-security-academy.net/filter?category=Gifts

Görselde görüldüğü üzere şuan category'nin altında bulunan Gifts kısmındayız. Burada bulunan Gifts kısmı yerine başka bir değer girersek ne olur bunun

sonucuna bakmamız lazım. SQL injection aramanın şanındandır diyerek " ' " işareti koyuyoruz. Tırnak işareti koymamızın sebebi ise arkada çalışan SQL sorgusuna müdahale etmek. Eğer biz bu girdi sonucunda bilinmeyen bir hata vb. alırsak yaptığımız işlemin herhangi bir filtreleme işleminden geçmeden başarıyla SQL sorgusu üzerinde çalıştığını farketmiş olacağız.

Amacımızı tekrar hatırlıyoruz. Satışa sürülmemiş ürünleri görmemiz isteniyordu

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```


ve bize de böyle bir sorgu verilmişti. Ben bu sorgudaki "released = 1" kısmını sorguya göndermemeyi başarırısam aşağıdaki Gifts ekranında satışa sürülmemiş ürünleri de görmüş olacağım.

SHOP 

Gifts

Refine your search:


[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Gifts](#) [Pets](#)



Couple's Umbrella

★★★★☆


\$16.23 [View details](#)



High-End Gift Wrapping

★★★★☆

\$23.29 [View details](#)



Snow Delivered To Your Door

★★★★★

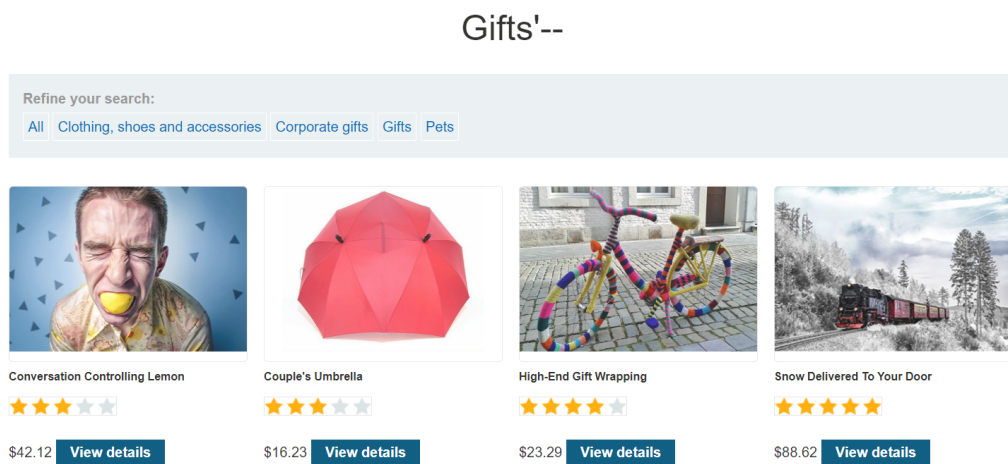
\$88.62 [View details](#)

Peki bunu nasıl yapacağım??

Yazılımda farklı amaçlarla kullanılan bir işlem vardır. Bu işlem seçilen kısımlarda ya da yorum satırı kullanılan yerden sonraki tüm kodları işleme almaz. İşte yorum satırı kullanarak "released = 1" kısmını işleme almayabilirim.

```
SELECT * FROM products WHERE category = 'Gifts'--' AND released = 1
```

Yukarıda yaptığım işlemde gifts kısmının sonuna " --' " kısmını ekleyer sorgunun sonuna yorum satırı "--" ekledim. Bu sayede "released = 1" kısmını sorguya eklememiş oldum ve satışa sürülmemiş diğer ürünü de aşağıdaki gibi görüntülemiş oldum



Umarım bu yazı sizler için faydalı olmuştur.