Portswigger Academy - SQLi APPRENTICE

SQL injection Challenges

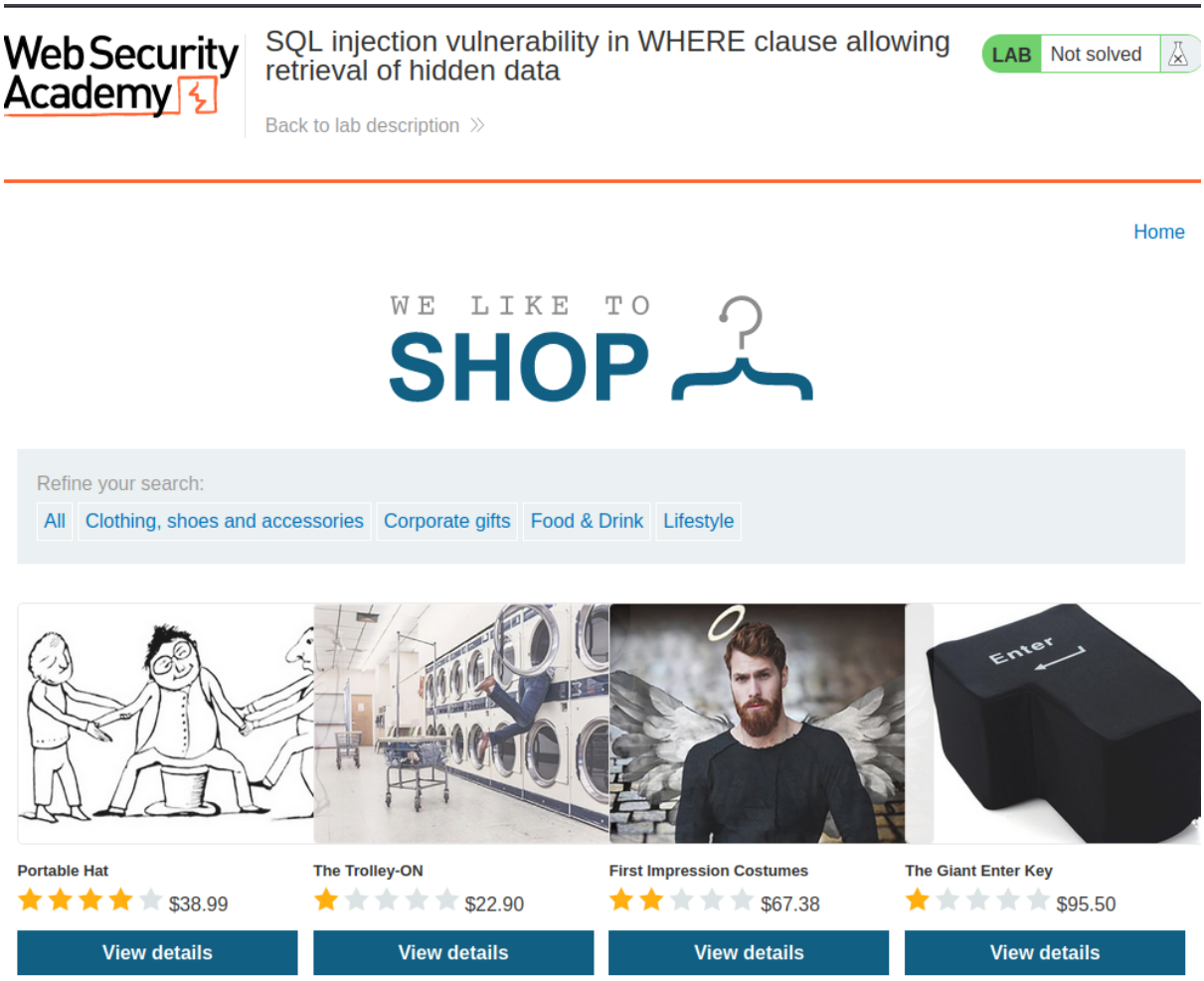
Challange 1 “SQL injection vulnerability in WHERE clause allowing retrieval of hidden data”

1) Lab’da bizden istenen şey bütün ürünleri göstermemiz. Bunun için sorgu bize verilmiş durumda.

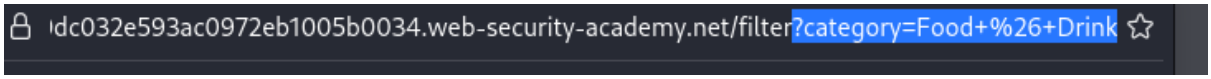
Sorguda, “category” kısmı girdi kabul eden kısım olacaktır. Bu nedenle “category” parametresi üzerinden SQL enjeksiyonu yapmamız gerekiyor. İstenen şey, bütün ürünlerin gösterilmesi olacağı için basitçe “or true -- ” değeri yeterli olacaktır.

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

2) Lab a giriş yaptığımızda aşağıdaki gibi bir arayüz karşılıyor:



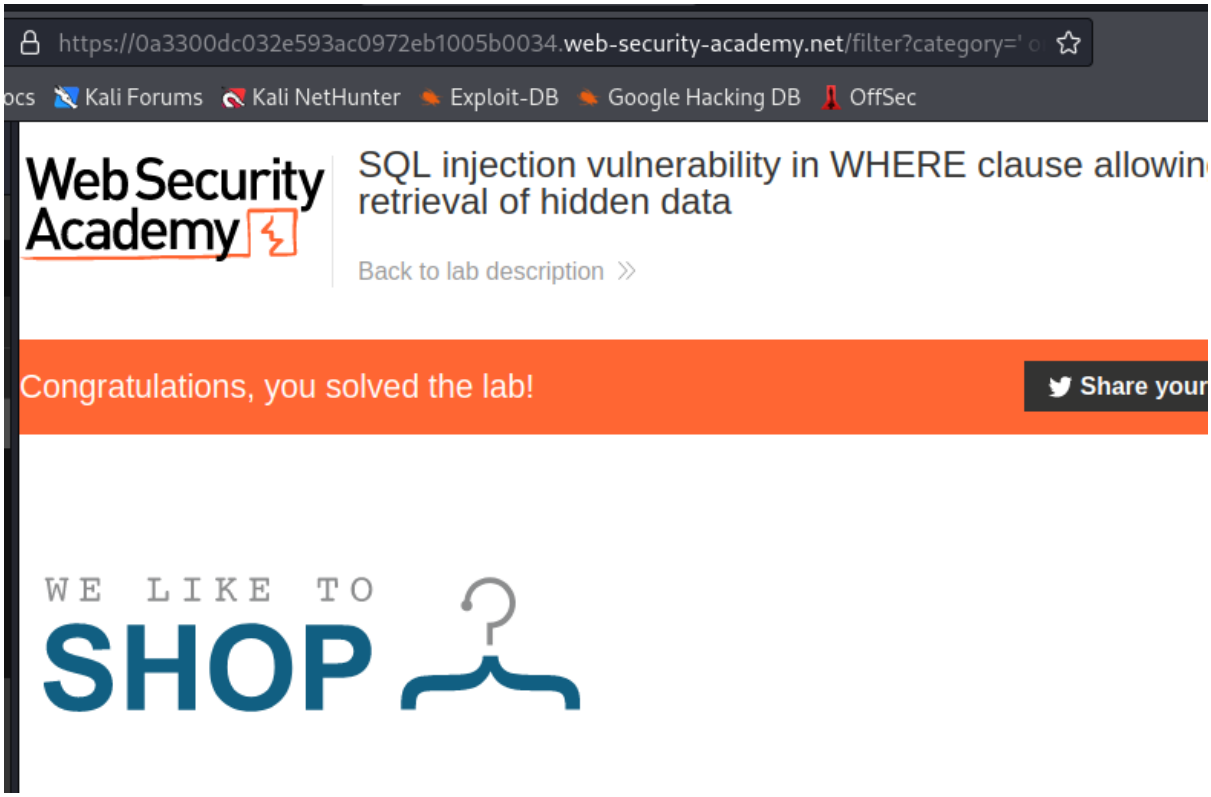
3) Herhangi bir kategori seçtiğimizde aşağıdaki gibi parametre “url” üzerinden gitmektedir yani bir “GET” parametresidir.



4) SQL hatası almadan sorguyu istediğimiz hale getirebilmek için verilen sorguda ki “Gifts” kısmına “‘ “ eklediğimiz zaman sorgunun kalanı yorum haline gelecek ve aşağıdaki gibi olacaktır:

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

5) Bu durumda sorguda bulunan koşul kısmı her değer için doğru olacağı için, bütün ürünler listelenecektir.



Challenge 2: SQL injection vulnerability allowing login bypass

1) Bu lab da login fonksiyonundan kaynaklı bir zafiyet olduğu söyleniyor. Login fonksiyonundaki SQLi zafiyeti nedeniyle admin olacak girmemizi istiyor.

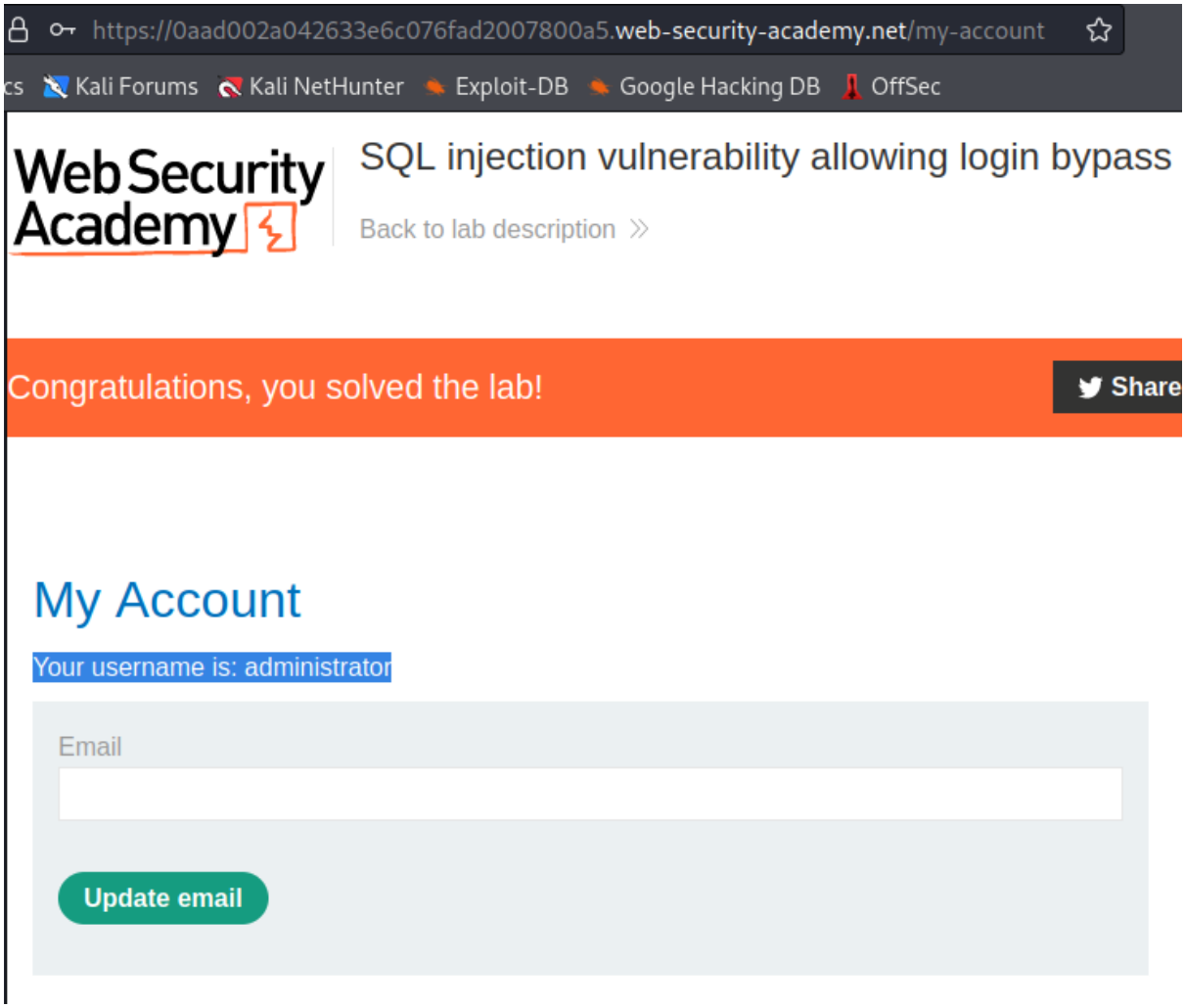
2) Sayfadaki “my account” bölümünden, giriş ekranına geliyoruz. Burada zaten SQLi olduğunu biliyoruz. Önceki sorunun aksine, bu soruda SQL sorgusunu bize vermemiş. Ancak biz yinede tahmin yürütebiliriz. Tahminen SQL sorgusu aşağıdaki gibi olacaktır.

```
-- Sorgu örneği, standart bir tek aşamalı sorgu
Select * from USERS Where username='$Username' and password='$password' Limit 1;
```

3) Bu labda da “ **‘ or ‘1’=’1**“ değerini hem parola hem kullanıcı adı bölümüne yazarsak sorguyu aşağıdaki gibi manipüle edebiliriz.

```
Select * from USERS Where username=' ‘ or ‘1’=’1' and password=' ‘ or ‘1’=’1' Limit 1;
```

4) Bu durumda, sorguya cevap olarak bütün tablo dönecek ama “Limit” fonksiyonundan dolayı sadece en üstteki değer baz alınacaktır. Bu değer “Administrator” hesabı olduğu için lab bu şekilde çözülebiliyor.



5) Ancak, sorguya dönen kullanıcı bilgisi bizim istediğimiz bilgi olmasaydı, kullanıcı adını elle vererek de giriş yapabilirdik.

Kullanıcı adı: “Administrator’ -- “ olarak denediğimizde de sorgu aşağıdaki hale gelecektir. Böylece parola koşulu da otomatik olarak yorum satırına alınacaktır. Bu durumu ayrıca parola, veritabanı sorgusu öncesinde bir “hash” fonksiyonundan geçiriliyorsa da kullanabiliriz.

```
Select * from USERS Where username='Administrator' -- ' and password=' ‘ or ‘1’=’1' Limit 1;
```