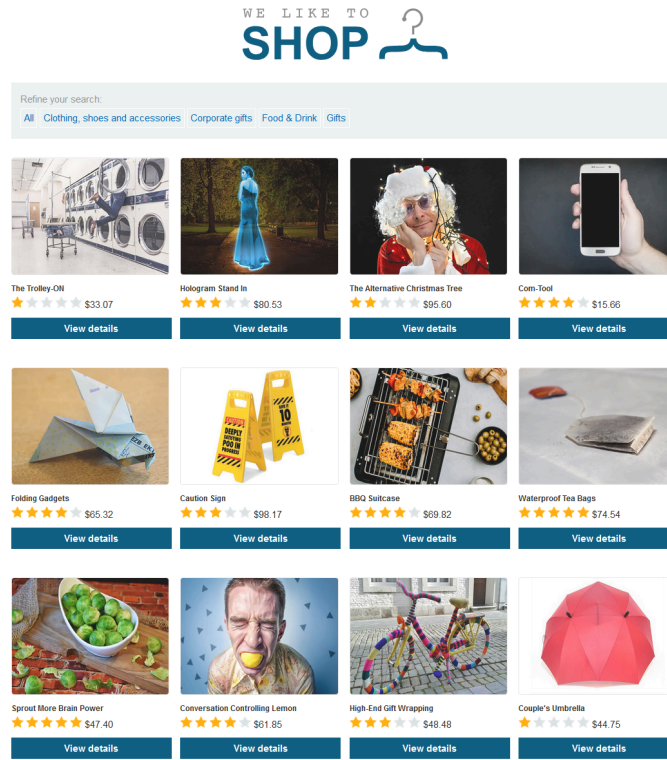


# Owasp Top 10 (3 zaafiyetli makine)

## 1 -) Portswigger - Sql injection

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

Siteye girdiğimizde tüm kategorilerde ki ürünleri listeliyoruz ve bize bu ürünler geliyor.

















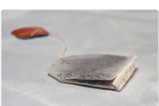





Bu ürünlerin satışta olduğunu görüyoruz. URL yi biraz incelediğimizde **category** parametresinin olduğunu görüyoruz. Buraya en çok bilinen injection komutunu yazmayı deniyoruz

```
.web-security-academy.net/filter?category=' or 1=1 --
```

' or 1=1 --

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Food & Drink](#) [Gifts](#)

 Portable Hat ★★★★★ \$9.10 <a href="#">View details</a>	 Snow Delivered To Your Door ★★★★★ \$0.27 <a href="#">View details</a>	 The Bucket of Doom ★★★★★ \$36.60 <a href="#">View details</a>	 The Giant Enter Key ★★★★★ \$16.44 <a href="#">View details</a>
 Single Use Food Hider ★★★★★ \$78.53 <a href="#">View details</a>	 The Trolley-ON ★★★★★ \$33.07 <a href="#">View details</a>	 Conversation Controlling Lemon ★★★★★ \$61.85 <a href="#">View details</a>	 What Do You Meme? ★★★★★ \$58.27 <a href="#">View details</a>
 Inflatable Dartboard ★★★★★ \$60.98 <a href="#">View details</a>	 Sarcastic 9 Ball ★★★★★ \$53.43 <a href="#">View details</a>	 Com-Tool ★★★★★ \$15.66 <a href="#">View details</a>	 Folding Gadgets ★★★★★ \$65.32 <a href="#">View details</a>
 Caution Sign ★★★★★ \$98.17 <a href="#">View details</a>	 BBQ Suitcase ★★★★★ \$69.62 <a href="#">View details</a>	 Waterproof Tea Bags ★★★★★ \$74.54 <a href="#">View details</a>	 Sprout More Brain Power ★★★★★ \$47.40 <a href="#">View details</a>
 Hologram Stand In ★★★★★ \$80.53 <a href="#">View details</a>	 The Alternative Christmas Tree ★★★★★ \$95.60 <a href="#">View details</a>	 High-End Gift Wrapping ★★★★★ \$48.48 <a href="#">View details</a>	 Couple's Umbrella ★★★★★ \$44.75 <a href="#">View details</a>

Satışa sunulmamış birçok ürünün olduğunu görüyoruz.

## 2 -) Portswigger - Access control

### Lab: Unprotected admin functionality with unpredictable URL

APPRENTICE

LAB

Not solved



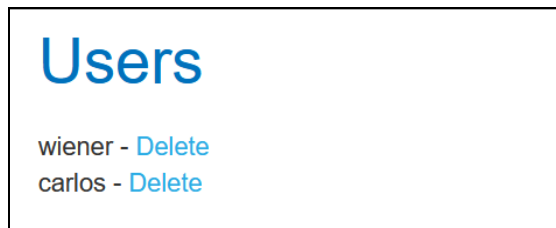
This lab has an unprotected admin panel. It's located at an unpredictable location, but the location is disclosed somewhere in the application.

Solve the lab by accessing the admin panel, and using it to delete the user `carlos`.

Sitedeki kaynak kodu incelediğimizde bir admin panel dizini buluyoruz.

```
var isAdmin = false;
if (isAdmin) {
  var topLinksTag = document.getElementsByClassName("top-links")[0];
  var adminPanelTag = document.createElement('a');
  adminPanelTag.setAttribute('href', '/admin-p6rpou');
  adminPanelTag.innerText = 'Admin panel';
  topLinksTag.append(adminPanelTag);
  var pTag = document.createElement('p');
  pTag.innerText = '|';
  topLinksTag.appendChild(pTag);
}
```

Bu dizine gittiğimizde admin yetkileri elimizde oluyor.



### 3 -) Portswigger - Authentication

#### Lab: 2FA simple bypass

APPRENTICE

LAB Not solved



This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page.

- Your credentials: wiener:peter
- Victim's credentials carlos:montoya

Bize verilen bilgiler ile sisteme giriş yapıp doğrulama kısmını geçiyoruz. Sonra URL adresini kontrol ettiğimizde karşımıza şu şekilde çıkıyor. ( /my-account?id=wiener )

## My Account

Your username is: wiener

Your email is: wiener@exploit-0aea00ce047995d68064ac1d019600df.exploit-server.net

Email

Update email

Sonra kurban bilgileri ile sisteme giriş yapıyoruz.

## Login

Username

Password

Log in

URL kısmının sonuna /my-account?id=carlos yazıyoruz.

Please enter your 4-digit security code

Login

Bu şekilde 2FA yı atlattmış oluyoruz.

# Bilal GÜNEŞ