

# PortSwigger Access Control Lab: Unprotected admin functionality

Herkese selamlar ben Mansur Derda. Bugün PortSwigger üzerinde bulunan Access Control zafiyetinin laboratuvarını anlatacağım.

Soru açıklamasında korunmasız bir yönetici paneli olduğu söyleniyor.

Bizden istenen ise Carlos kullanıcısını silmek

**WebSecurity Academy**


Unprotected admin functionality


LAB Not solved

Back to lab description >>


[Home](#) | [My account](#)

WE LIKE TO


SHOP 




Picture Box  
★★★★★ \$44.13  
[View details](#)



AbZorba Ball  
★☆☆☆☆ \$3.42  
[View details](#)



Conversation Controlling Lemon  
★★★★★ \$79.28  
[View details](#)



Your Virtual Journey Starts Here  
★★★☆☆ \$81.67  
[View details](#)

Aklıma gelen şeylerden biri sayfa içeriğinde saklanmış kritik bir bilgi olabilir mi diye bakıyorum. Kullanıcı adı şifre ya da herhangi bir uzantı gibi. lakin aradığım şeyleri

bulamıyorum. Aklıma gelen şey ise kullanıcı verilerinin tutulduğu dosyalara bakmak oluyor. İlk denemem /robots.txt uzantısı oluyor ve bingo

```
User-agent: *  
Disallow: /administrator-panel
```

robots.txt uzantısına gittiğimde böyle bi ekranlar karşılaşıyorum. Ardından /administrator-panel uzantısına gidiyorum ve bu şekilde yalnızca admin hesabından yapabileceğim bir işlem olan kullanıcı listeleme ekranını görüyorum

## Users

wiener - [Delete](#)  
carlos - [Delete](#)

---

Ve carlos kullanıcıasını sildiğim zaman laboratuari başarıyla tamamlamış oluyorum.

Umarım bu yazı sizler için faydalı olmuştur.