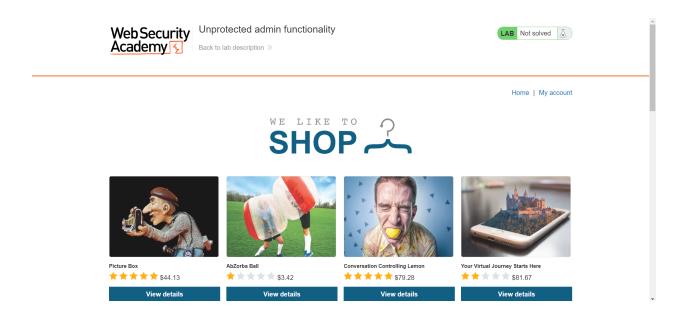
PortSwigger Access Control Lab: Unprotected admin functionality

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



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 kullanıcısını sildiğim zaman laboratuarı başarıyla tamamlamış oluyorum.

Umarım bu yazı sizler için faydalı olmuştur.