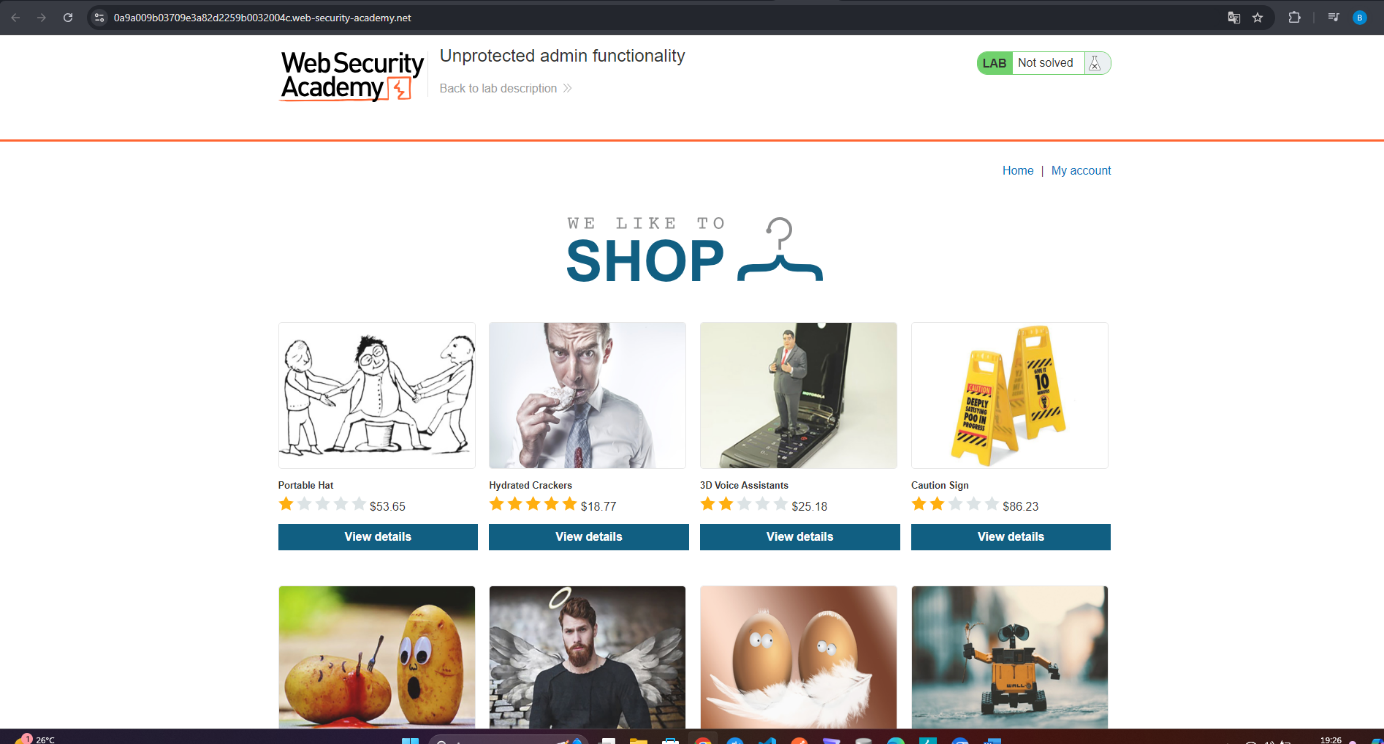
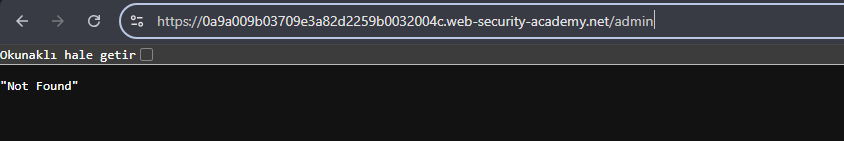
Broken Access Control

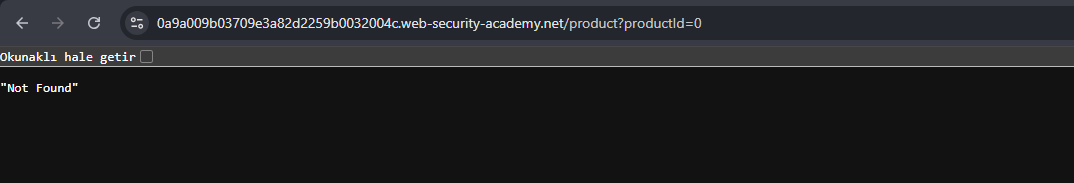
Broken Access Control, kullanıcıların erişim yetkilerinin kontrol edilmediği ya da yanlış yönetildiği durumlarda ortaya çıkar. Aşağıda Portswigger ile yapılmış birkaç örnek vardır.



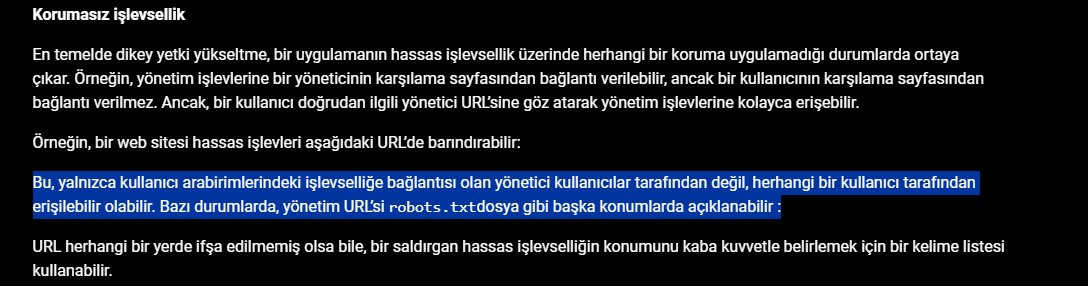
İlk Labtaki siteye giriyorum. (İlk denememde SQL injection denedim, Broken Access olduğunu unuttum)

Herhangi bir ürüne tıkladığımda ürünlerin ID lerini değiştirdim ve bazı yöntemler denedim.

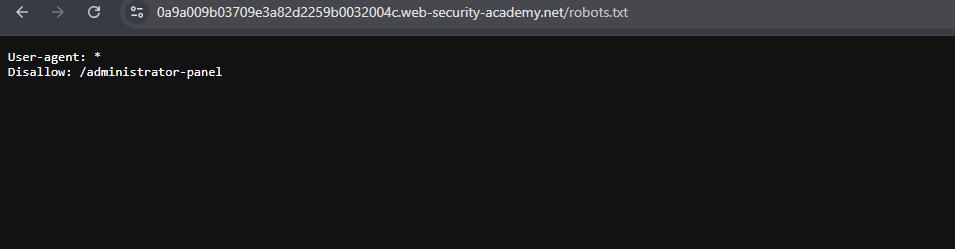


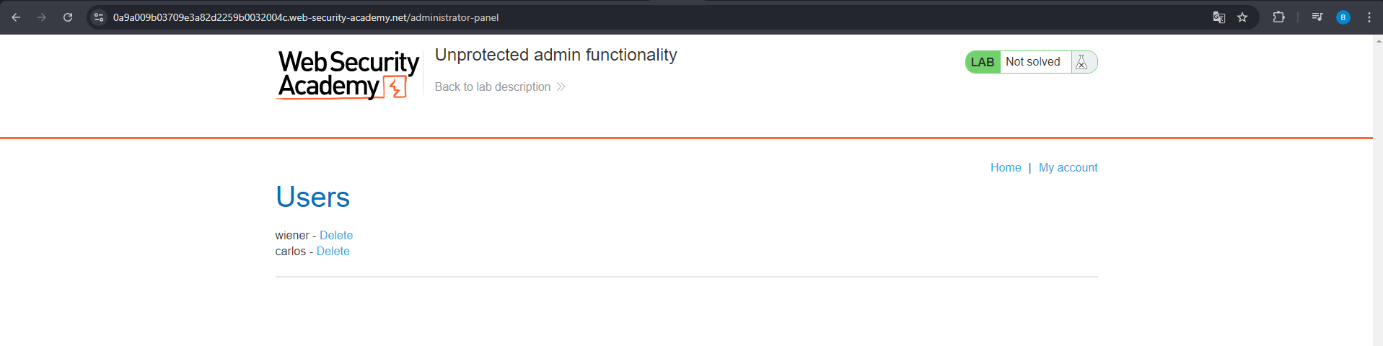


Broken Access Control zafiyetini araştırırken admin url’i robots.txt gibi dosyada da tutulabileceğini gördüm.



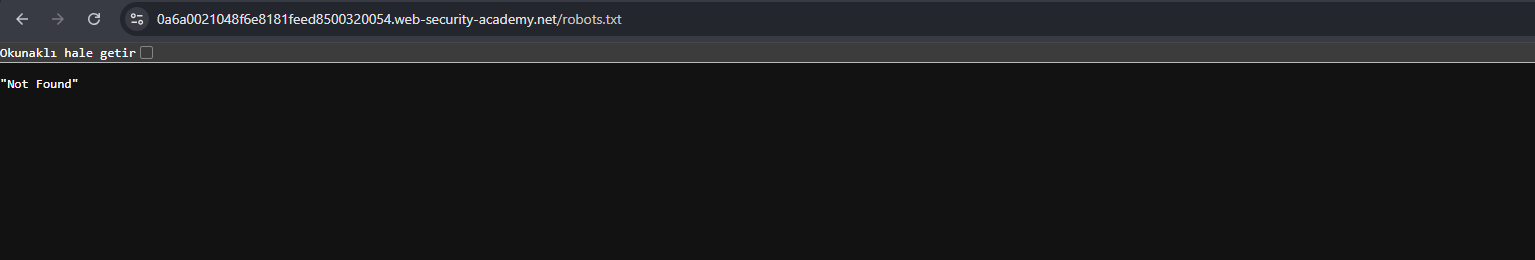
(<https://www.ozztech.net/siber-guvenlik/broken-access-control-acigi-nedir/>)

Siteye tekrar girip robots.txt dosyasını yazdığımda karşıma yönetim url’ çıktı. 

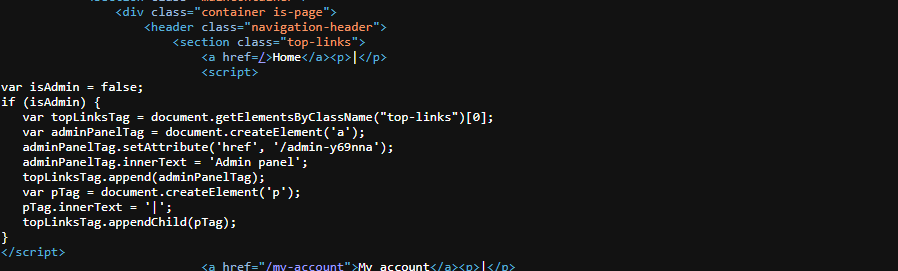


Sistemden Carlos’u sil görevini yaptıktan sonra lab’ı tamamlamış oluyoruym.

İkinci Lab’ta ise daha önce okuduğum yazının devamında olan hatayı görüyorum.

İkinci Lab’a girdiğimde robots.txt dosyasını çağırıyorum ama bu sefer not found ile hata alıyorum.

Login ekranına gidiyorum ve sayfanın kaynak koduna bakıyorum.



Login ekranında doğrulandığı taktirde hangi konuma gönderileceğini scrpit kodları içinde görünür halde yazılmış. Görevim olan Carlos kullanıcısını silerek Lab’ı tamamlıyorum.

