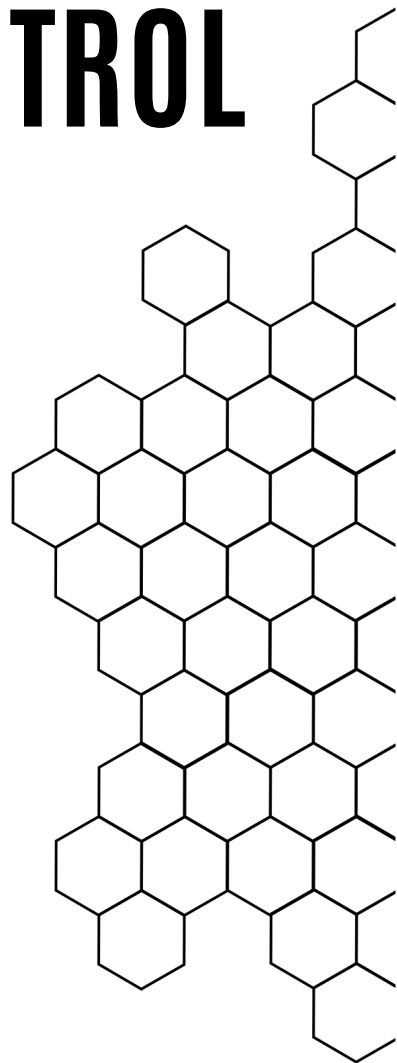
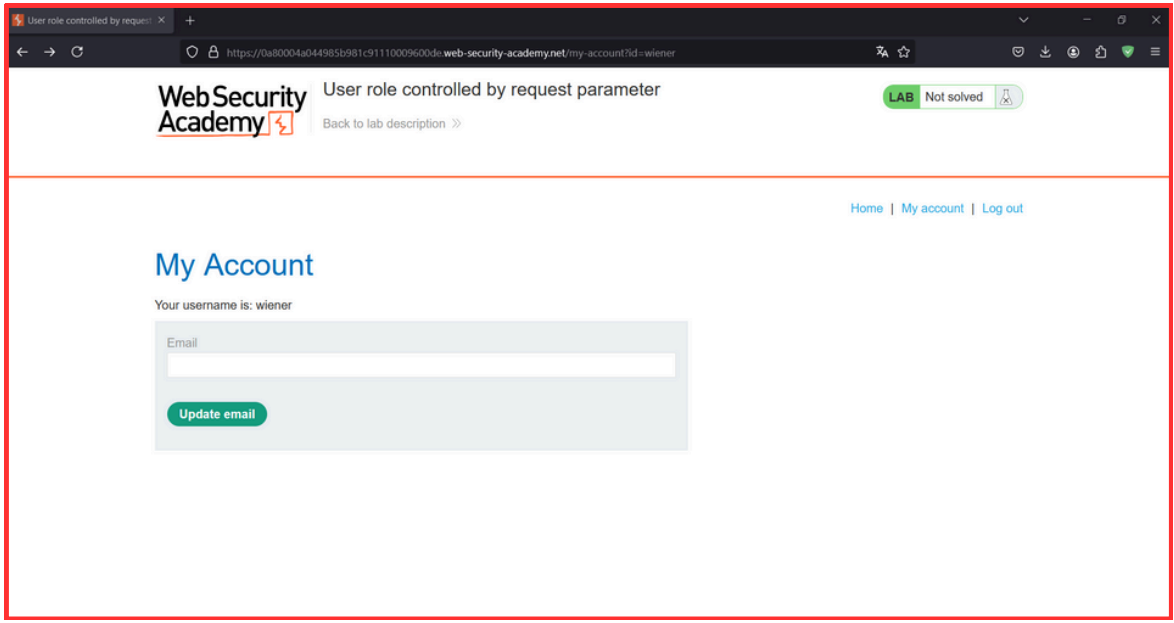


BROKEN ACCESS CONTROL

LAB 3

TARİH: 28.08.2024

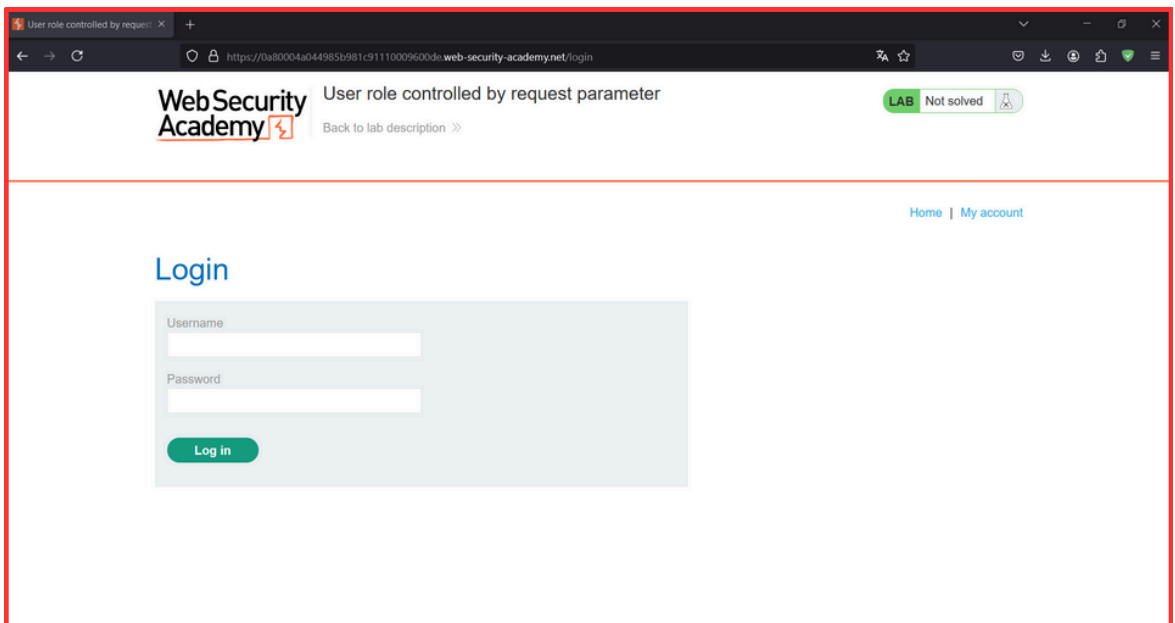


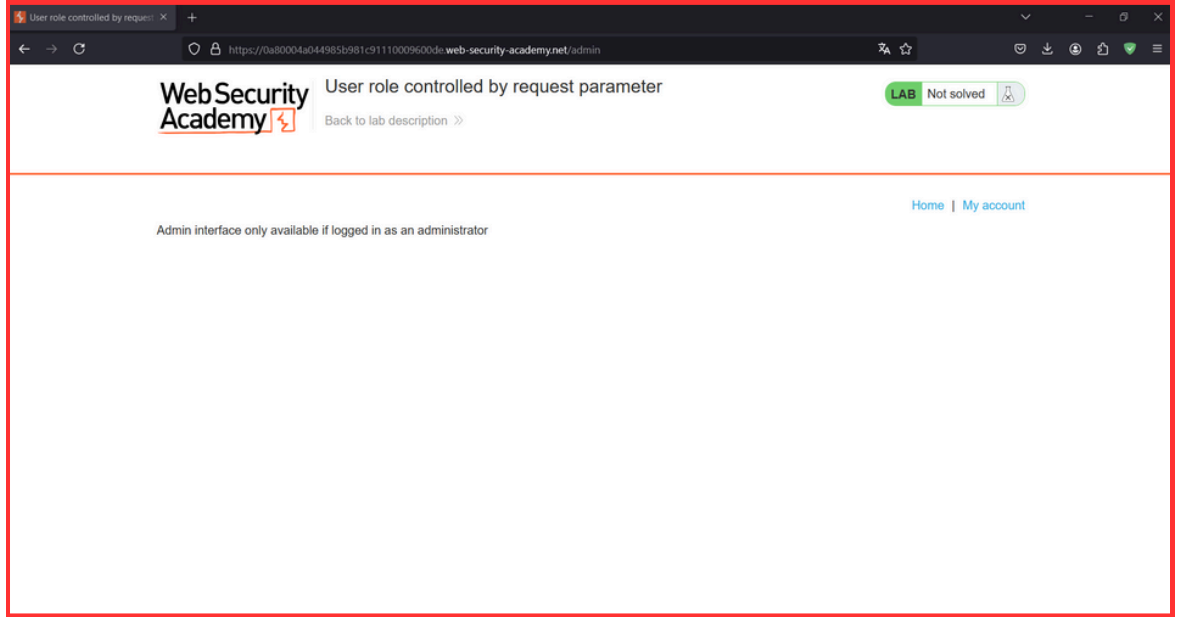


Bu lab için giriş kısmında /admin dizini belirtilmiş ve buraya girerek yine carlos kullanıcısını silmemiz isteniyor. İlk olarak wiener:peter bilgileriyle verilen kullanıcı olarak giriş yaptım.

https://0a80004a044985b981c91110009600de.web-security-academy.net/my-account?id=wiener

Giriş yaptıktan sonra URL kısmındaki id parametresi dikkatimi çekti. Buradaki kullanıcı adı yerine admin yazarak admin hesabına geçiş yapmayı denedim ancak tekrar giriş sayfasına yönlendirildim.





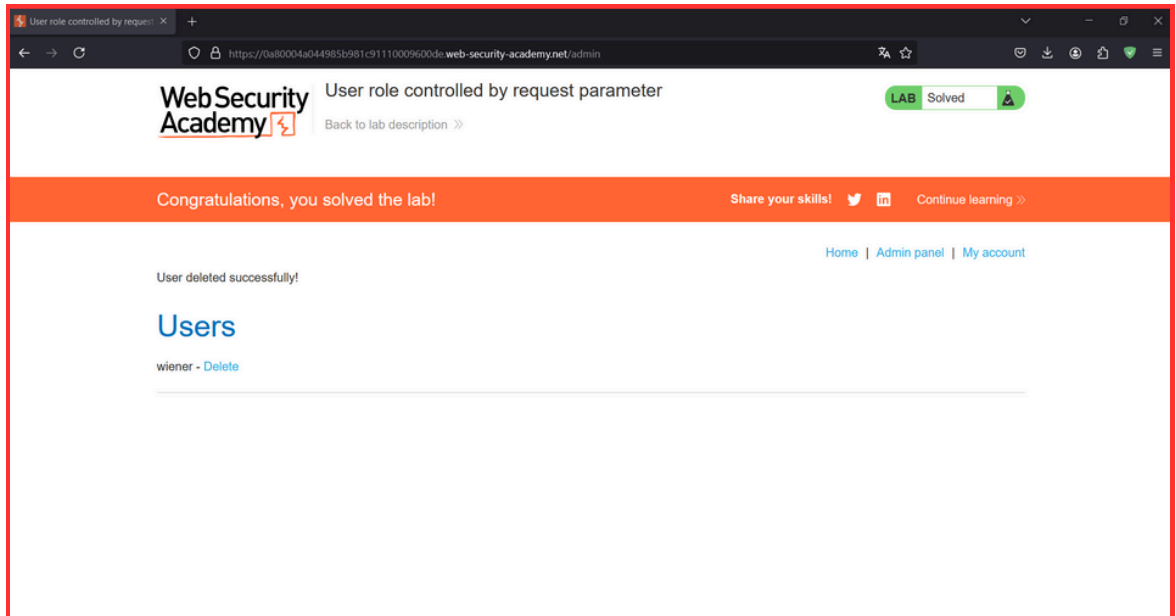
Wiener kullanıcısına tekrar giriş yapıp admin sayfasına erişmeye çalıştım. Ama yine administrator olarak giriş yapmamızı istedi.

Öğeleri filtrele		
Adı	Değer	Domain
Admin	false	0a80004a044985b981c91110009600de.web-
session	mpMBYSQolXGig0bnPvPsTBtnFUJw...	0a80004a044985b981c91110009600de.web-

Daha sonra çerezleri kontrol ettim ve Admin adındaki bir değerin false olduğunu gördüm. Bunu true olarak değiştirdim.

Öğeleri filtrele		
Adı	Değer	Domain
Admin	true	0a80004a044985b981c91110009600de.web-
session	mpMBYSQoIXGig0bnPvPsTBtnFUJw...	0a80004a044985b981c91110009600de.web-

Admin adlı çerezin değerini true olarak değiştirdikten sonra sayfayı yeniledim.



Sayfayı yenilediğimde bir uyarı ile karşılaşmadım ve kullanıcıları silebildiğimiz ekrana geldim. Burada da carlos kullanıcıasını silerek labı tamamladım.