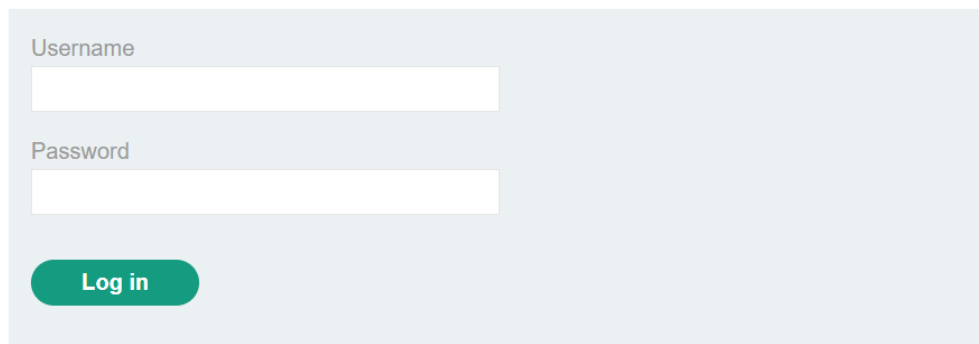


PortSwigger Lab: SQL injection vulnerability allowing login bypass

Herkese selamlar ben Mansur Derda. Bugün PortSwigger üzerinde bulunan SQL injection zafiyetinin laboratuvarını anlatacağım

Soru başlığından da anlayacağımız üzere sayfanın aşağıdaki login kısmında SQL injection bulunuyor. Bizden istenen ise "administrator" kullanıcısı ile hesaba giriş yapmak.

Login



A login form with a light blue background. It contains two input fields: 'Username' and 'Password'. Below the 'Password' field is a green 'Log in' button.

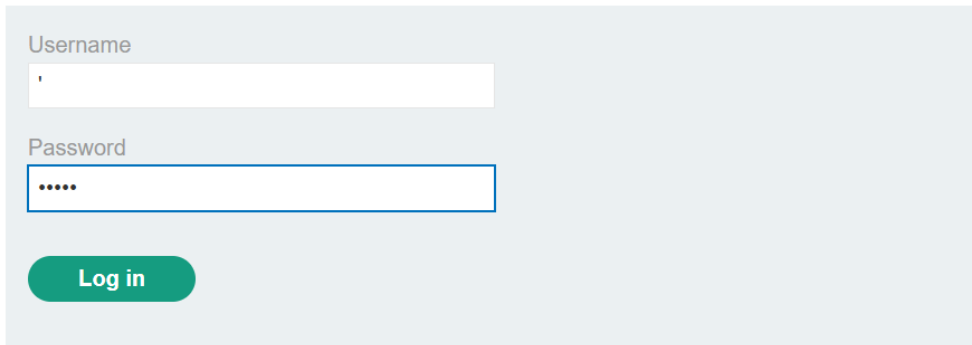
Username

Password

Log in

öncelikle default kullanıcı adı ve şifre olan admin admin kombinasyonunu deniyorum ve herhangi bir sonuç alamıyorum. Sırada ise SQL injection aramanın şanındandır diyerek " ' " işareti koyma kısmı var. Sıra ile farklı seçenekleri deniyorum. önce username: ' | password: admin denedim.

Login



A login form with a light blue background. It contains two input fields: 'Username' and 'Password'. The 'Username' field has a single quote character (') entered. The 'Password' field has five dots (.....) entered. Below the fields is a green 'Log in' button.

VEE süprizz nur topu gibi error geldi.

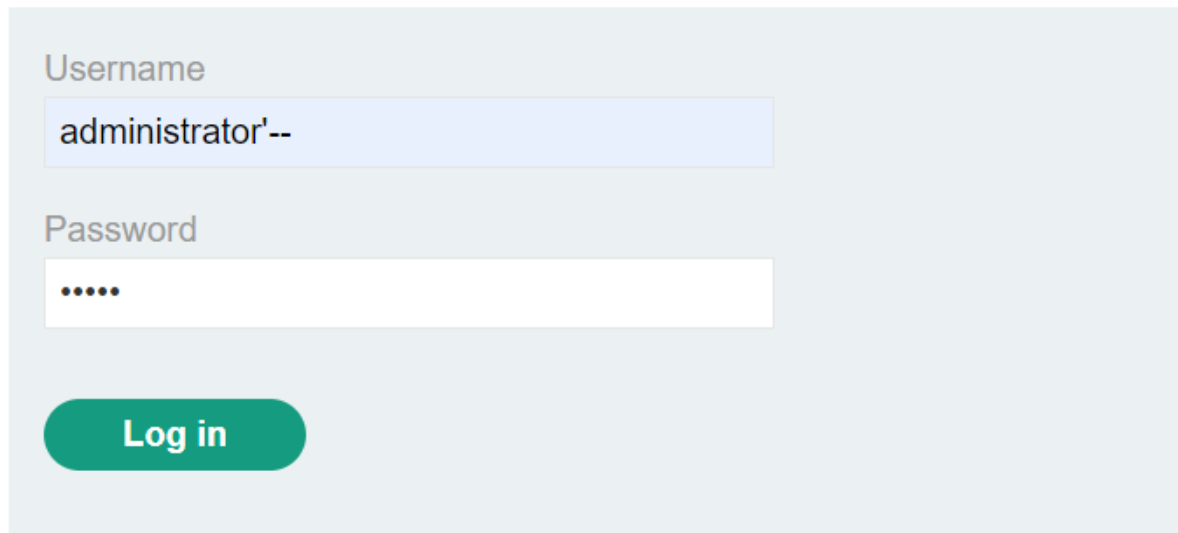


Peki ben bu hataya neden bu kadar sevindim sebebi ise şu: ben database'ye bi istek gönderdim. Bu istek database'nin ayarlarıyla oynamak içindi herhangi bir filtrelemeden geçmedi ve db ye gitti böyle bir değer olmadığı için de hata verdi. Ben bu kısmı kullanarak istediğim işlemleri yapabileceğim.

Aklıma ilk olarak önceki laboratuarda kullandığım yorum satırı tekniği geliyor. Eğer "administrator" kullanıcı adını girdikten sonra şifre kısmını iptal edersem administrator hesabına başarılı bir şekilde giriş yapmış olurum.

Bunu şu şekilde yapacağım "administrator'-- " bu şekilde yapmamın sebebi ise şu ' koyarak işlemi bitirdim ve -- ile yorum satırı ekledim bu sayede sonraki password kısmı geçersiz oldu.

Login



The image shows a login interface with a light blue background. It contains two input fields: "Username" and "Password". The "Username" field is highlighted with a light blue border and contains the text "administrator'--". The "Password" field is a standard white input box with a light gray border, containing five black dots. Below the fields is a green rounded rectangular button with the text "Log in" in white.

Yukarıdaki şekilde giriş yapmayı deniyorum.

[Home](#)

My Account

Your username is: administrator

Email

Update email

VEE hayırlı olsun. Siteye administrator olarak giriş yapmış oldum.

Umarım bu yazı sizler için faydalı olmuştur.