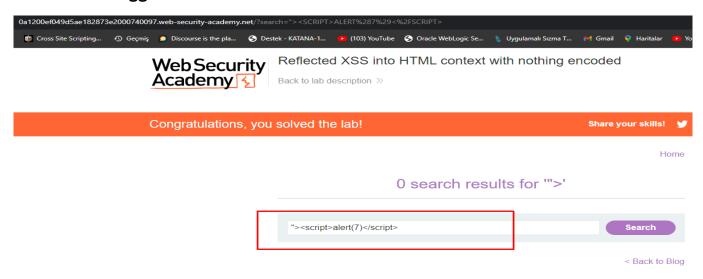
LAB 1:Portswigger Reflected Xss

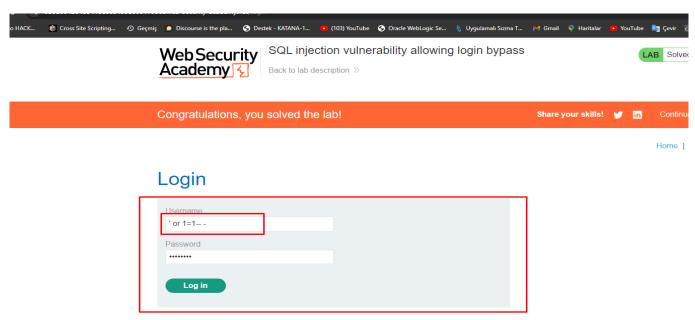


Search parametresinde filtreleme özelliği olmadığını fark ettim ve kaçış stringiyle beraber payloadı yolladım.

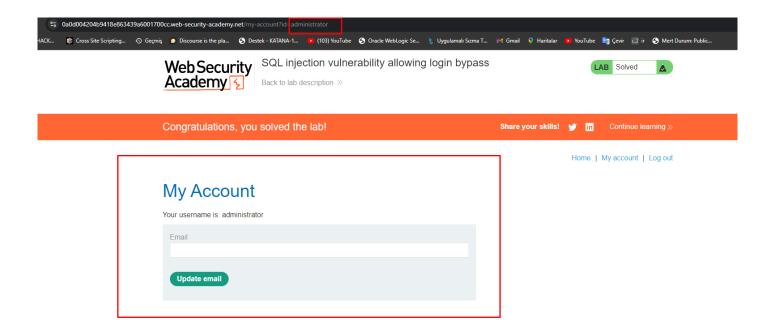


Payload sorunsuz çalıştı ve burada Reflected Xss zafiyeti olduğunun tespitini yaptım.

LAB 2:Portswigger Sql injection

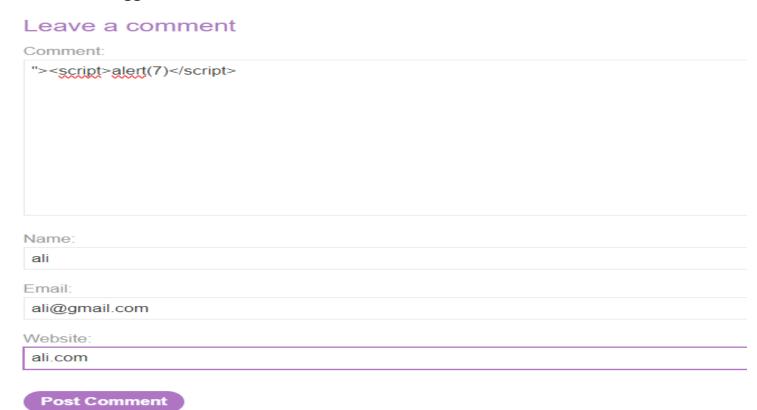


Login ekranında potansiyel sql injection varlığını düşünerek klasik sql injection payload denemesi gerçekleştirdim.



Administrator yetkisiyle login oldum.

LAB 3: Portswigger Stored Xss



Yorum yapma yerine gelerek xss payloadımı yolladım.



Congratulations, you solved the lab!

Thank you for your comment!

Your comment has been submitted.

Yorum başarıyla gönderildi.



Yorumlar sayfasına geldiğimde database kaydolan xss yükü her sayfayı yenilediğimde ekrana basıldı.