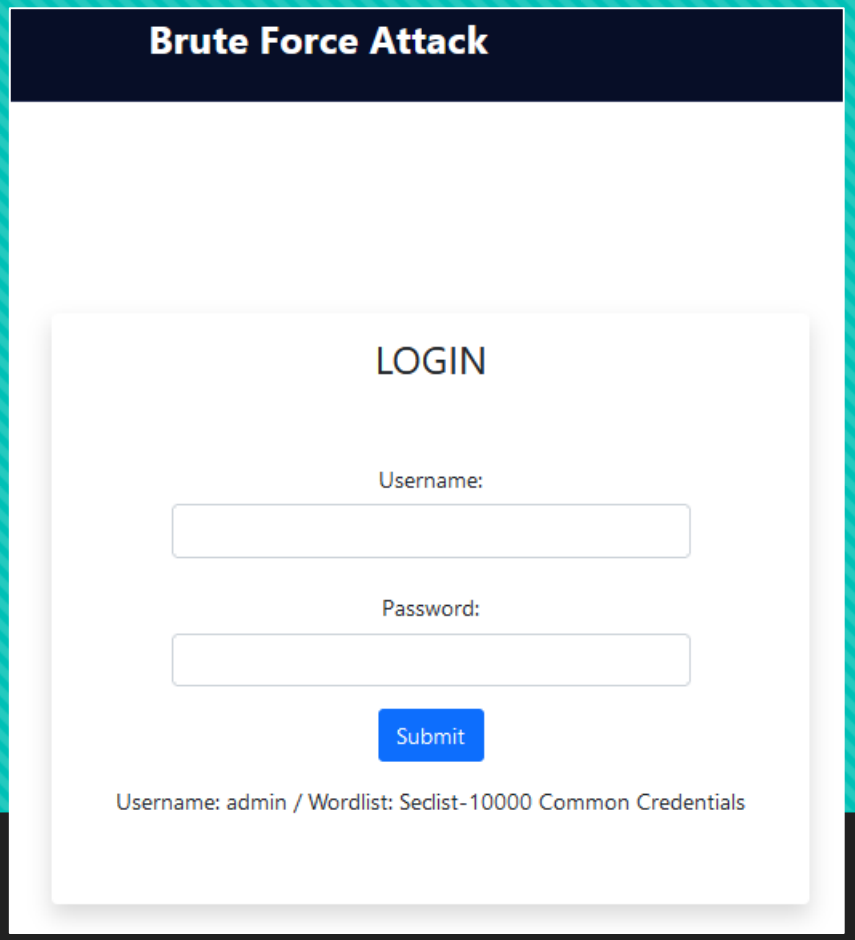
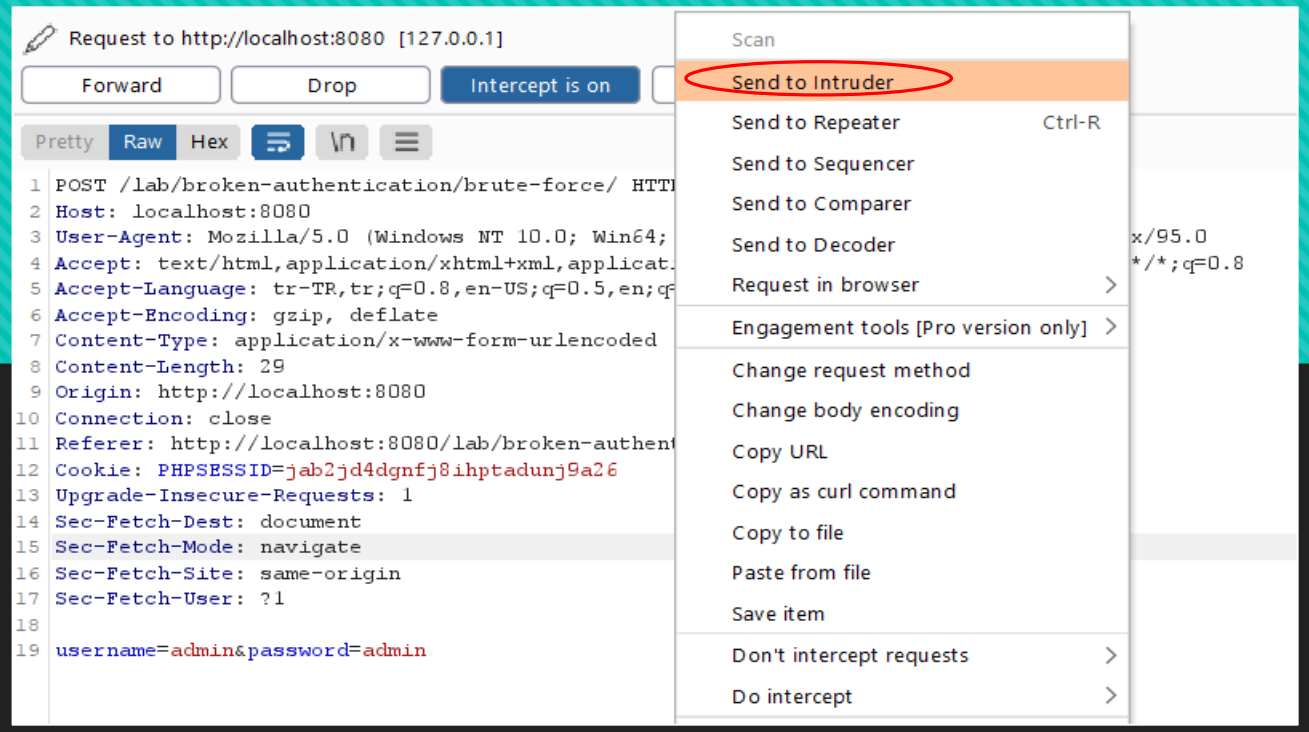
# Broken Authentication Rapor



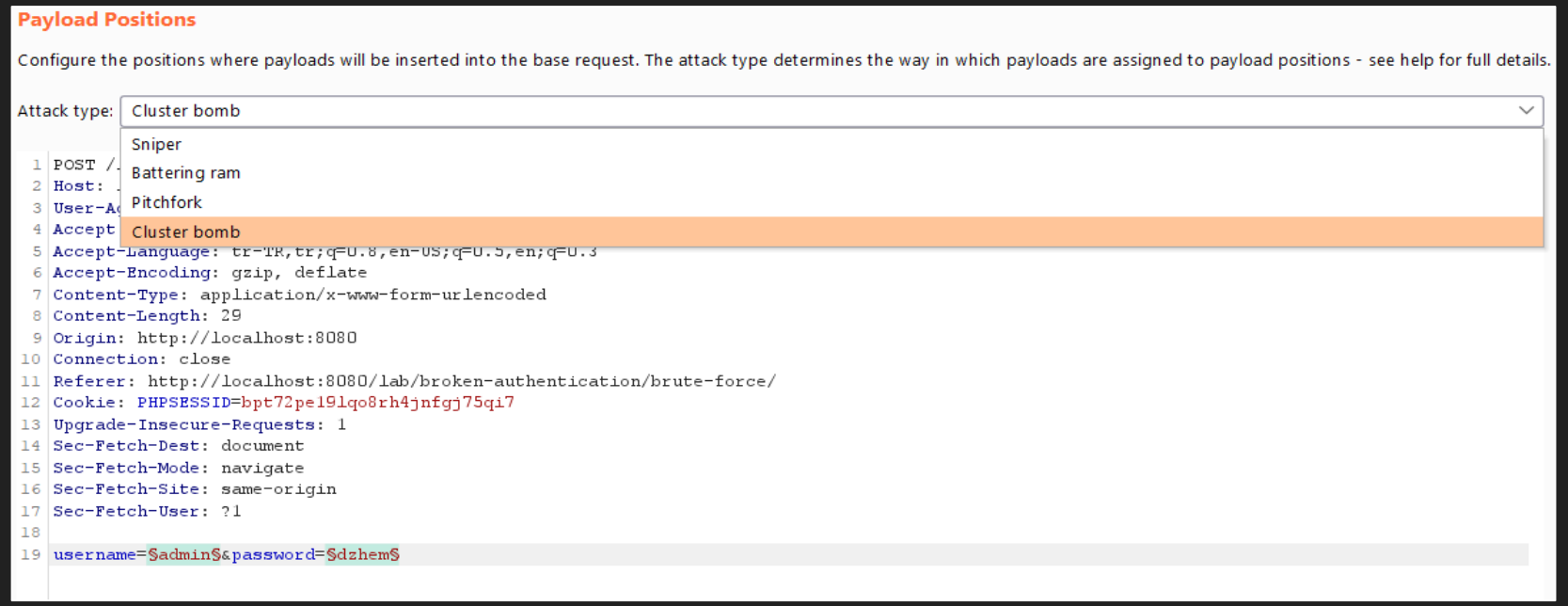

Siteye girdiğimizde bizi bir giriş ekranı karşılıyor.Kullanıcı adı «admin» olarak sistem tarafından bize tanımlanmış ancak şifre bilgisi elimizde yok.

Burp-Suite programını kullanarak Brute-Force Attack gerçekleştiricez ve bu şekilde şifreyi öğrenmiş olucaz.

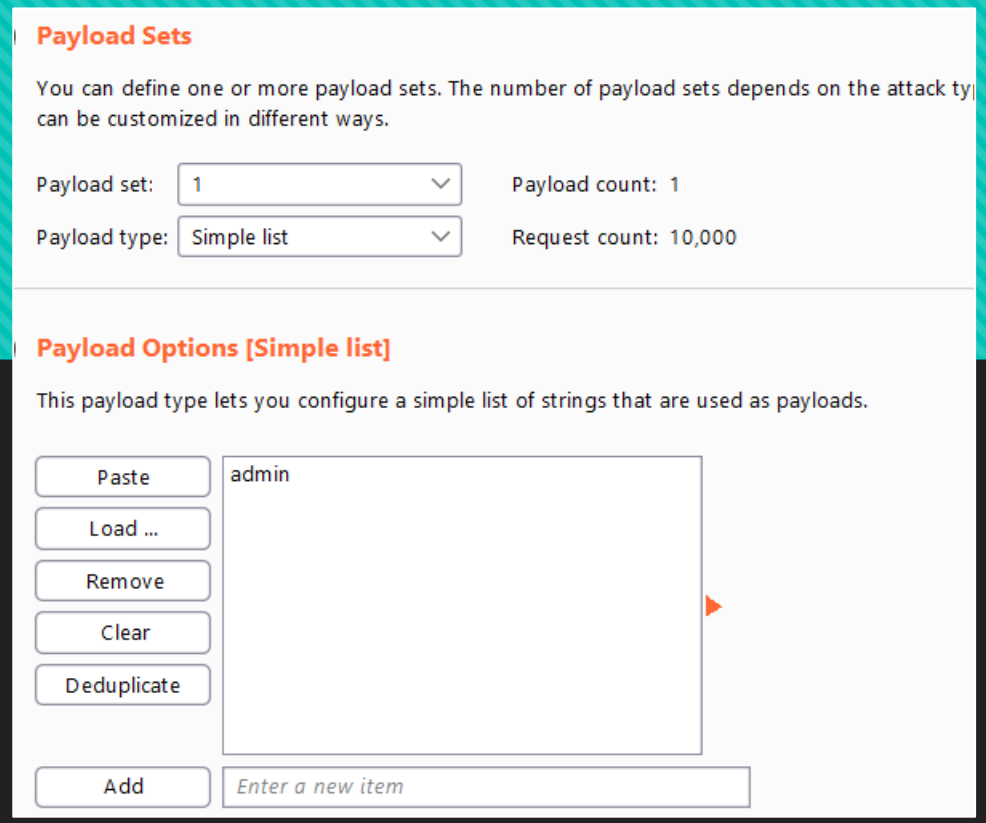



Burp-Suite uygulaması ile giriş ekranındaki girdiğimiz bilgileri yakalıyoruz.

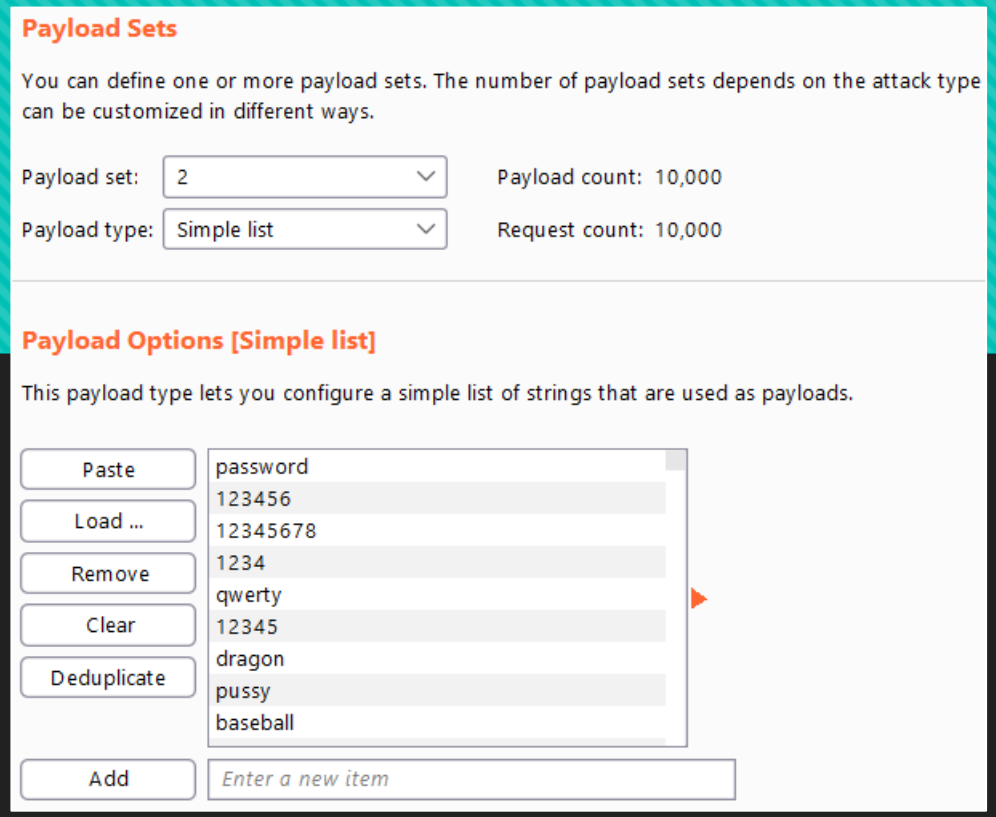
İstek ekranına sağ tıklayıp Send to Intruder seçeneğine tıklıyoruz.



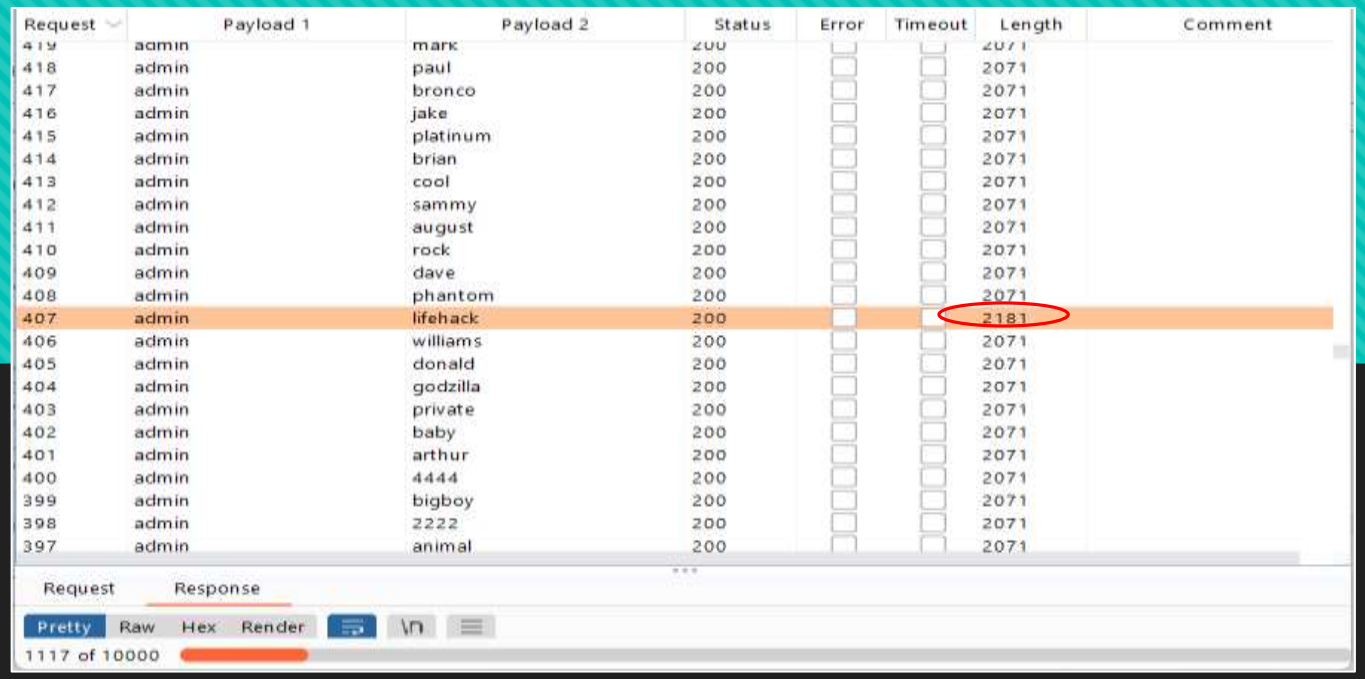

Attack Type olarak Cluster Bomb seçeneğini seçtikten sonra Brute-Force yapılacak payloadları işaretliyoruz.



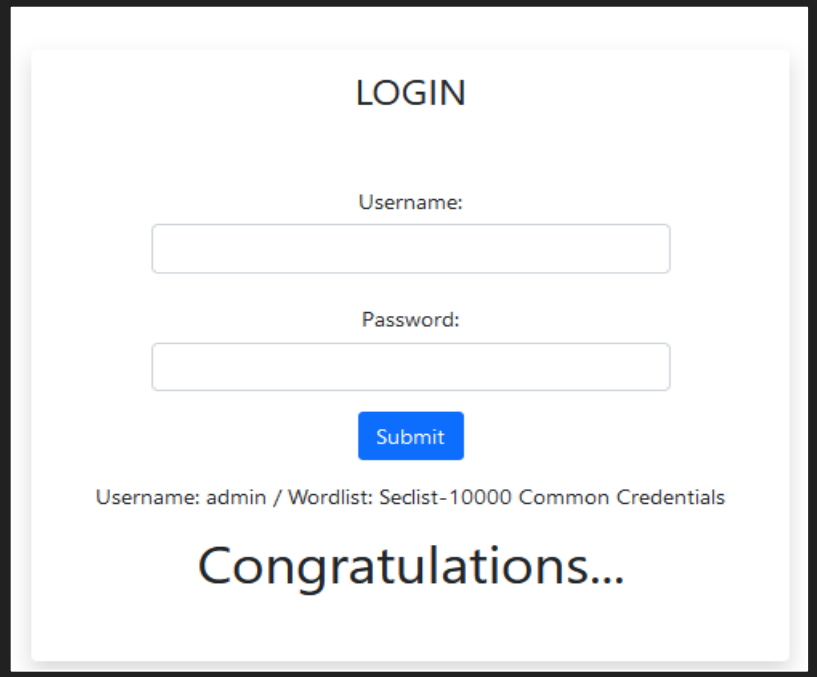

Payload 1 seçeneğimiz giriş ekranındaki kullanıcı adını temsil ediyor. Sistem tarafından kullanıcı adı tanımlandığı için tek bir değişken veriyoruz.



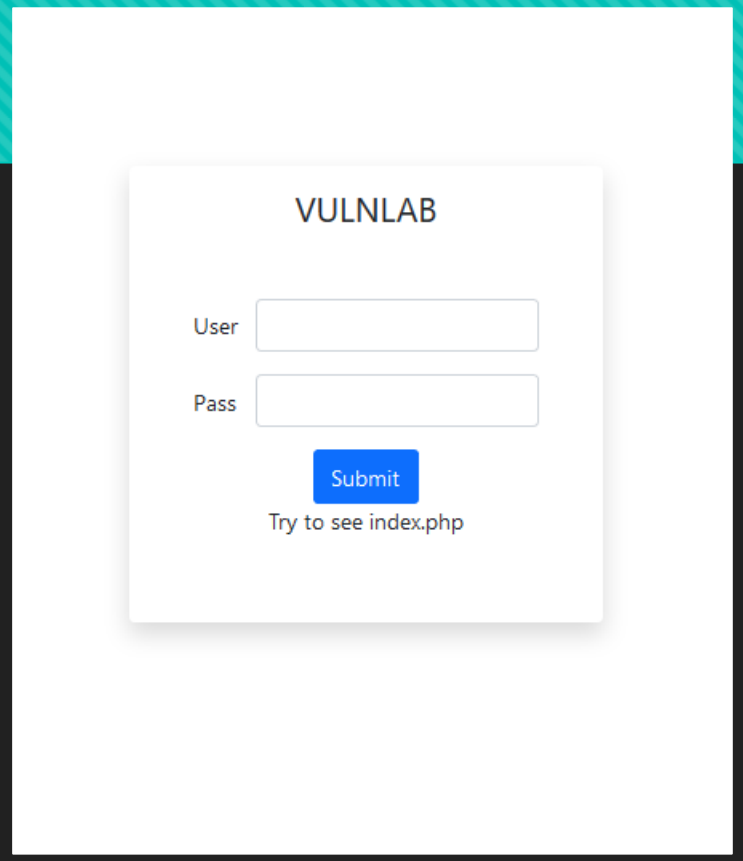

Payload 2 seçeneğimiz giriş ekranındaki şifre kısmını temsil ediyor. Sistem tarafından tanımlanan kullanıcı adı bilgisini kullanarak şifre için ise 10.000 kelimeden oluşan bir liste tanımlıyoruz ve bu şekilde ilerliyoruz.



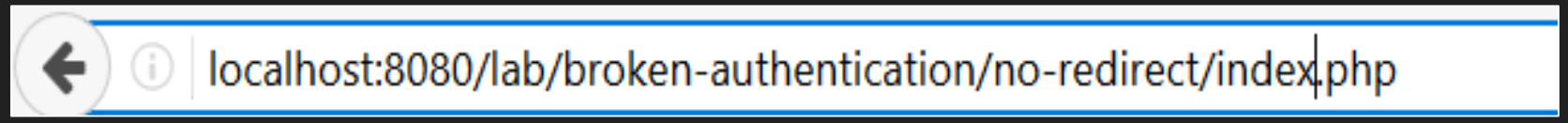

Gönderilen istekler arasında istek uzunluğu farklı olan tek bir seçenek var bu şekilde giriş yapmayı deniyoru.

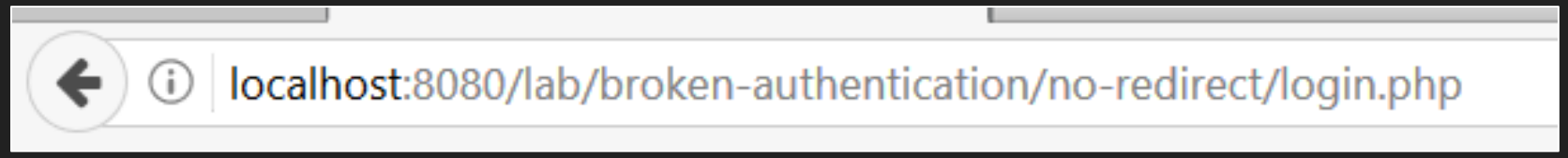



Bu bilgileri kullanarak giriş yapmayı denediğimizde başarılı bir şekilde sisteme giriş yapıyoruz.



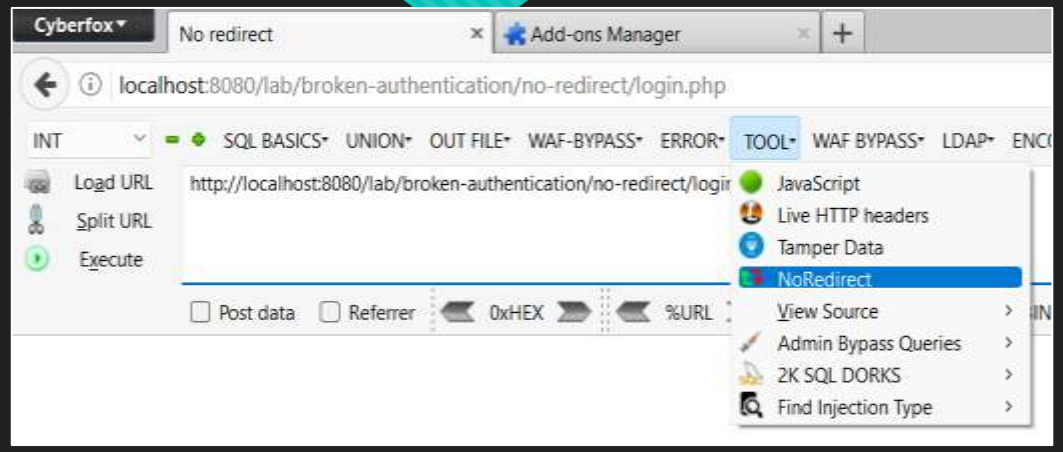

Giriş ekranın altında bize index.php dosyasını görüntülememizi istiyor.Ancak URL üzerinden gitmeye veya giriş yaparak gitmeye çalışsakta bizi sürekli login.php sayfasına yönlendiriyor.

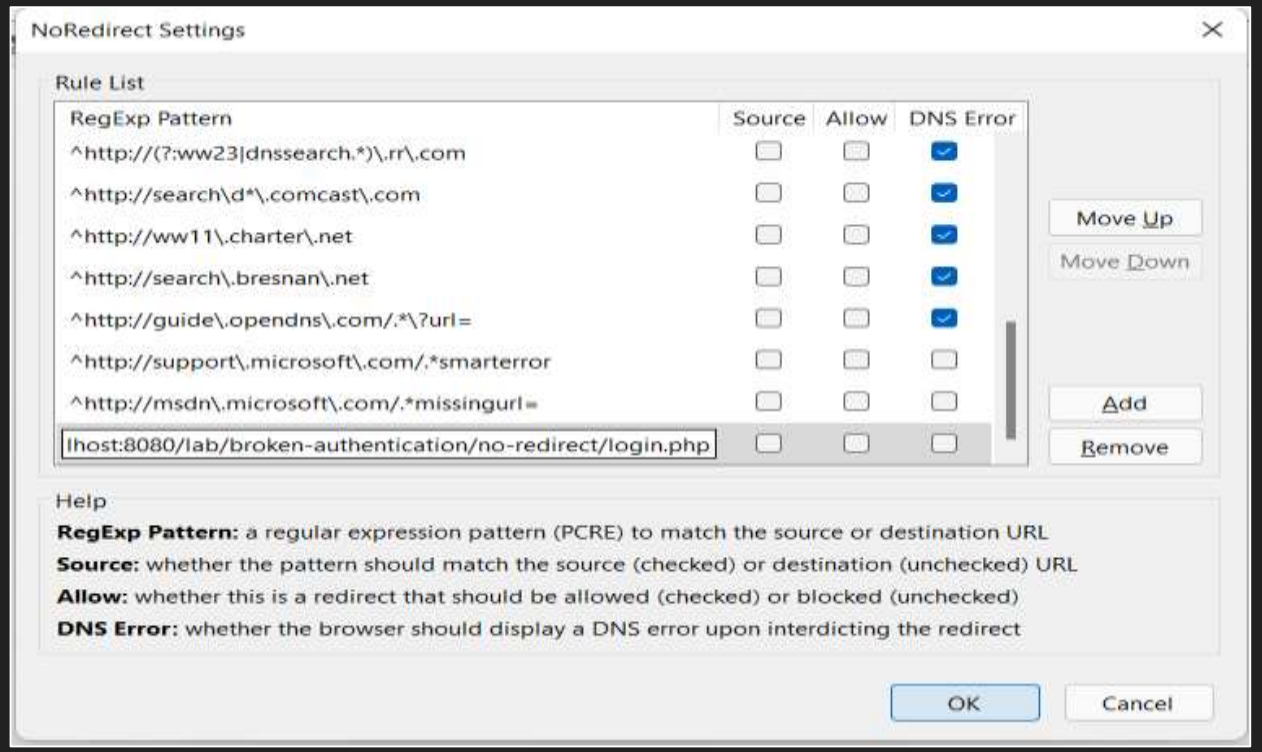


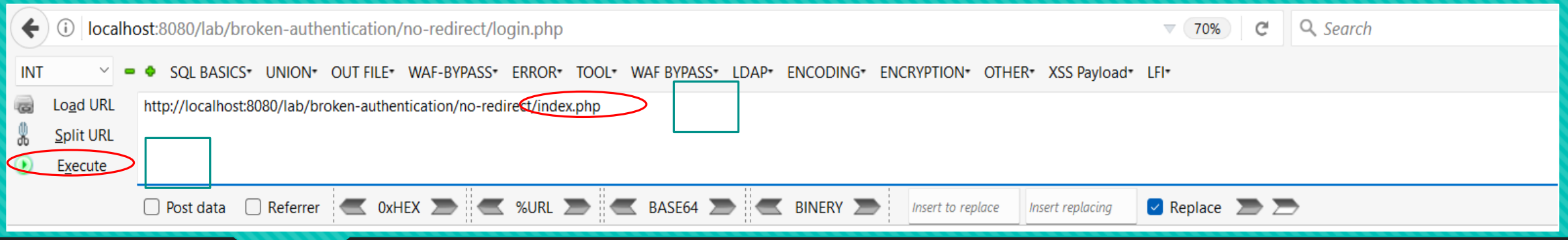



Burdan anlıyoruz ki giriş ekranındaki form işlevsiz durumda girilen veriler herhangi bir yere gönderilmiyor bu yüzden diğer bir sayfaya yönlendirme yapılmıyor.

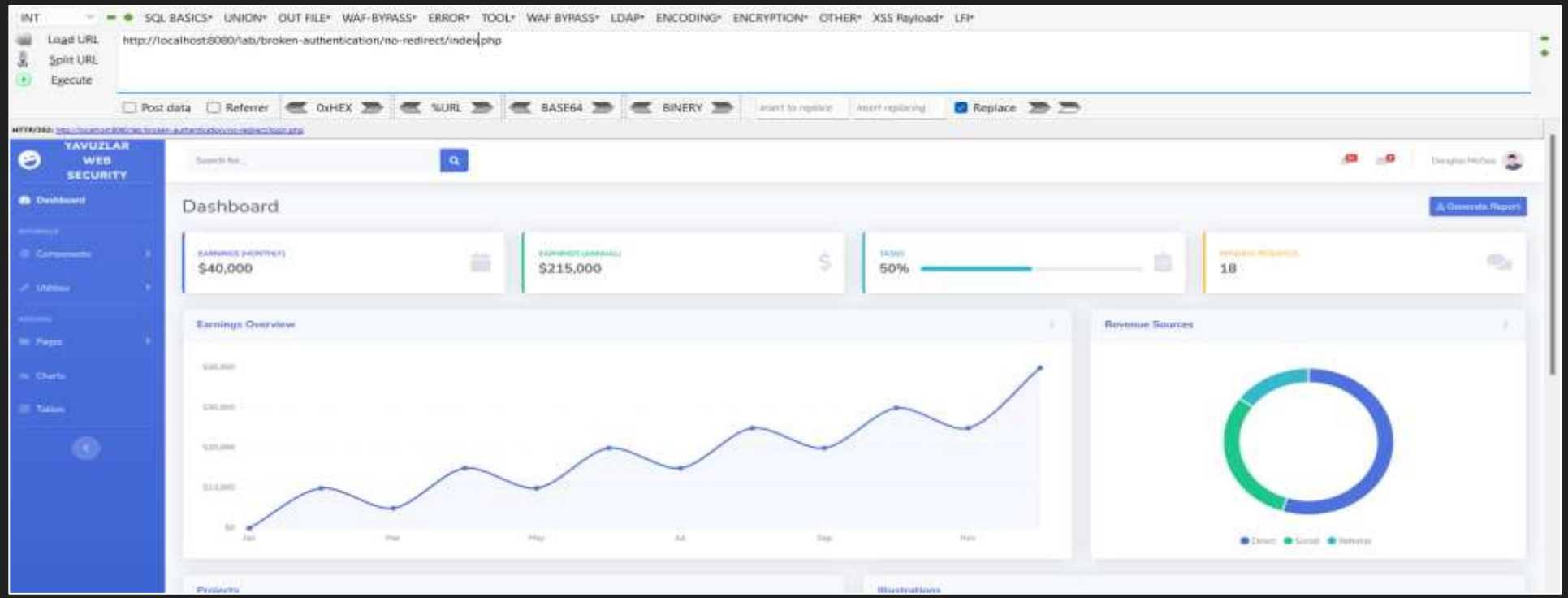
Bu yönlendirmeyi aşmak için HackBar eklentisinden yararlanacağız. URL adresimizi aldıktan sonra Tool bölümünden açılan sayfada NoDirect kısmına tıklıyoruz ve ardından kopyaladığımız URL adresimizi buraya ekliyoruz.






Ekleme yaptıktan sonra isteğimizi index.php şeklinde düzenliyoruz. Ardından bu şekilde isteğimizi gönderiyoruz.




İstek bu şekilde yollandığında index.php sayfasına ulaşmış oluyoruz.