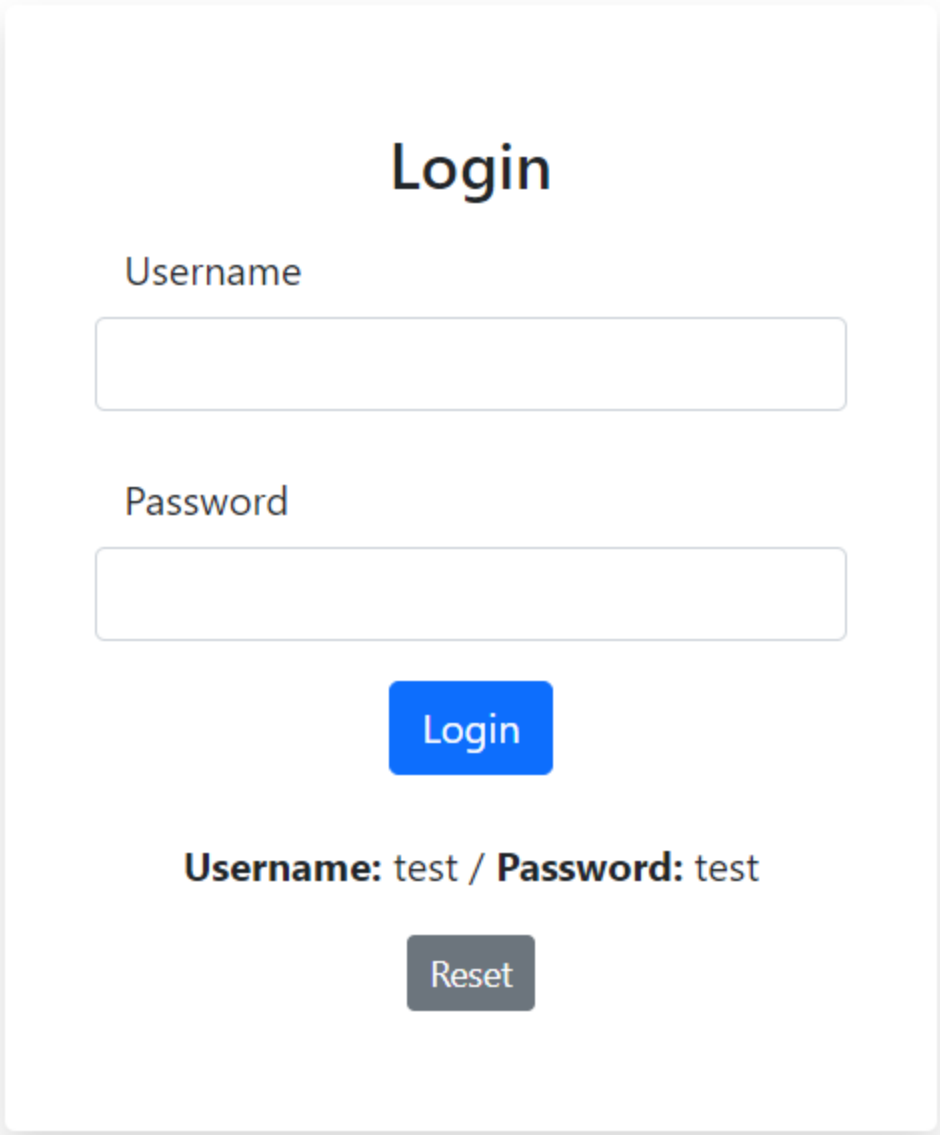
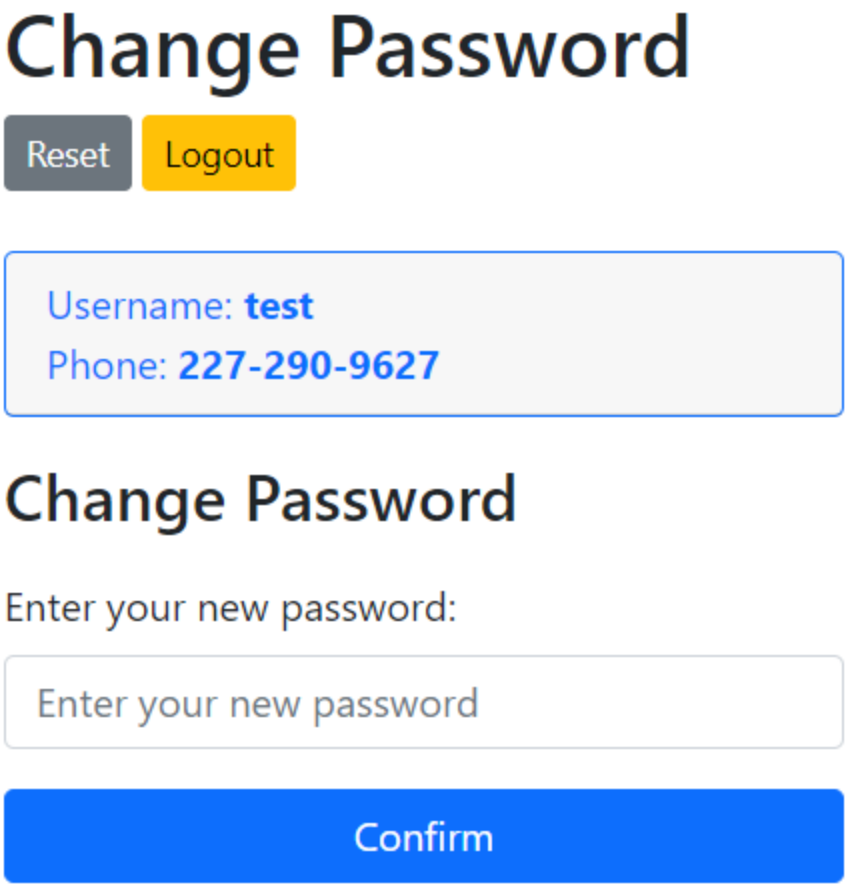
Insecure Direct Object References (IDOR)/Change Password

Herkese selamlar bu yazımda Hackviser üzerinde bulunan Web security lablarından biri olan **Insecure Direct Object References (IDOR)/Change Password** labının çözümünü anlatacağım.

Öncelikle bize verilen siteye gittiğimizde aşağıdaki gibi bir login page karşılıyor.

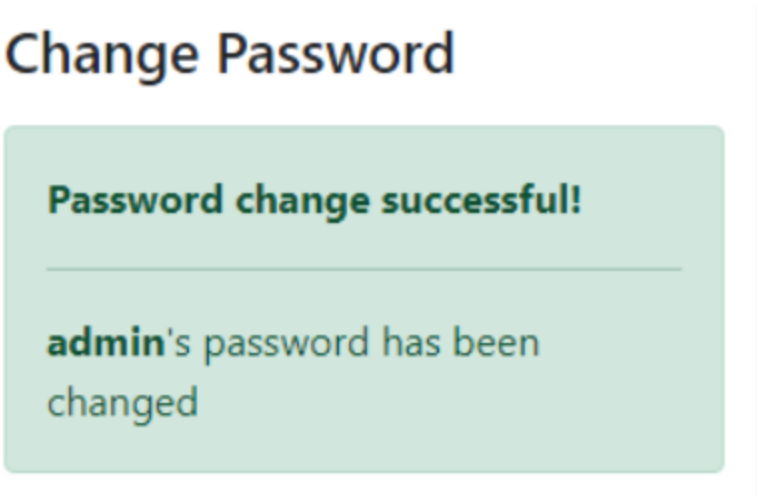


Default verilen test:test bilgileri ile giriş yaptığımda ise aşağıdaki gibi bir ekran karşılıyor



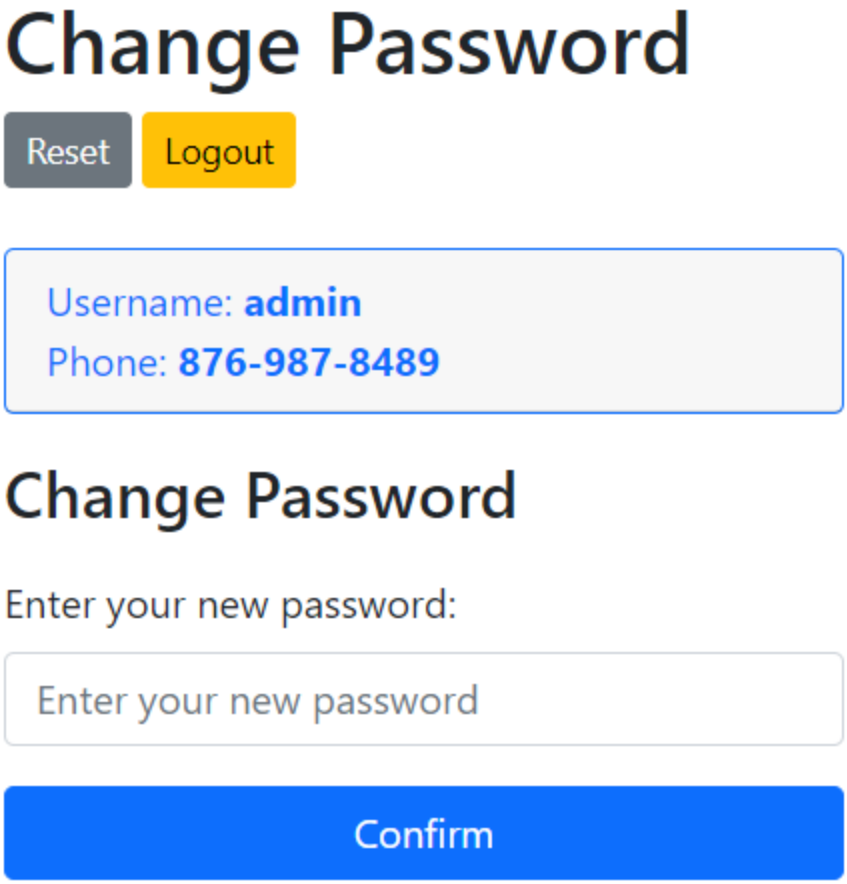
Şifre değiştirme işlemi yaparken isteği tutup izlemeye alıyorum.

Görselin alt kısmında “user_id=2” kısmı dikkatimi çekiyor. Zaten aktif olan bir admin kullanıcısının olduğunu biliyoruz. Admin kulllancısının id’sinin 1 olabileceğini tahmin ediyorum. Ve bu kısımda isteği değiştirerek id değerini 1 yapıyorum. Ardından isteği gönderiyorum.



Görseldeki gibi admin kullanıcısının şifresini başarılı bir şekilde değiştirdiğimin bilgisini alıyorum.

admin:test bilgileri ile giriş yaptığımda aşağıdaki gibi başarılı bir şekilde giriş yapabiliyorum.



Bu kısımda phone bilgisi ise flag değeri oluyor.

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar!