CHANGE PASSWORD WRİTE-UP

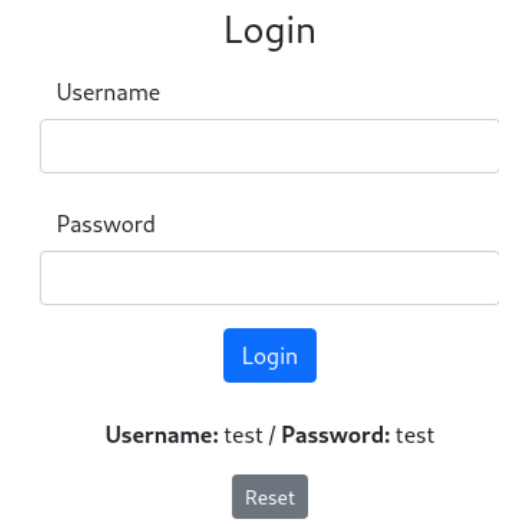
Bu yazımda sizlere Hackviser platformu üzerinde bulunan Web Lab kısmı altında IDOR zafiyetinin Change Password labının çözümünü anlatacağım.

SENARYO: Bu laboratuvar, diğer kullanıcıların parolasını yetkisiz bir şekilde değiştirmeye yol açan Güvensiz Doğrudan Nesne Referansları (IDOR) güvenlik açığı içerir.

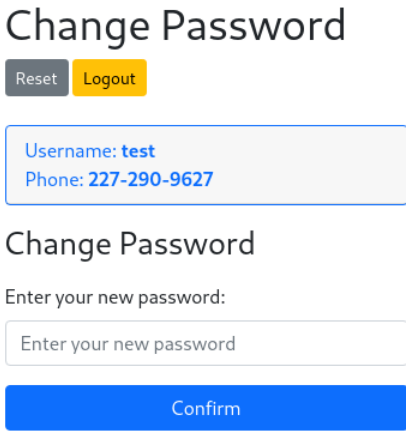
Laboratuvarı tamamlamak için "admin" kullanıcısının parolasını, parola değiştirme uç noktasındaki IDOR zafiyetini istismar ederek değiştirin ve hesabına giriş yapın.

"admin" isimli kullanıcının telefon numarası nedir? (Cevap Formatı: 000-000-0000)

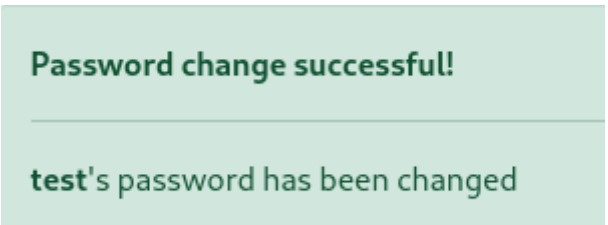
ÇÖZÜM: Siteye giriş yapınca login sayfası bizi karşılıyor.



test:test bilgileri ile giriş yapıyoruz.



Giriş yaptıktan sonra bizi böyle bir sayfa karşılıyor. Herhangi bir şey yazıp onaylayınca:

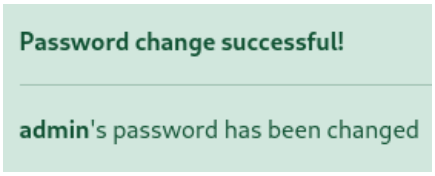


Bilgisini aldık.

Şimdi buraya deneme yazıp Burp Suite'e atıyoruz. Attıktan sonra en altta id kısmına rastlıyoruz.

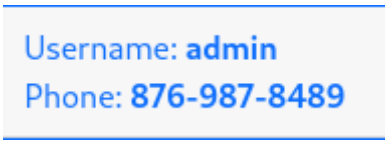
```
password=deneme&user_id=2
```

Burada id kısmını değiştirmeyi planladım. İd=1 yaptım.



Artık admin kullanıcısının şifresi "deneme"

Admin:deneme bilgileri ile giriş yapıyoruz.



Cevap: **876-987-84-89**