## **IDOR**

## **4.2 Change Password**

Sorunun bizden istediği şey;

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

Login
Username
test
Password
test
Login
Username: test / Password: test
Reset

Ve bizleri login alanı ve bizlere verilmiş bir kullanıcı görüyoruz giriş yapalım.

Şifre değiştir  Sıfırla Oturumu kapat
Kullanıcı adı: <b>test</b> Telefon: <b>227-290-9627</b>
Şifre değiştir
Yeni şifrenizi girin:  Yeni şifrenizi girin
Onaylamak

Burada kullanıcı'nın şifresini yenileme alanı var şifreyi değiştirmeden önce burp ile dinliyelim.

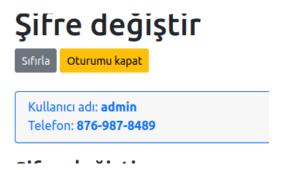
```
Connection: keep-alive
password=servet&user_id=2
```

Ve parola değiştirme alanı şu şekilde kullanıcı adı çıkmıyor ben test kullanıcısını admin yaparım diye düşünmüştüm ama burada id kullanılmış bizim id değerimiz 2, 1 daima admin diyebiliriz çünkü ilk kullanıcı olduğundan dolayı ilk 1i deniyelim bakalım.

## Şifre değiştir

Şifre değişikliği başarılı!
yöneticinin şifresi değiştirildi

Ve yönetici parolası değiştirildi dedi, deniyelim. Ve admin:servet ile giriş yaptım.



**Cevap:** 876-987-8489