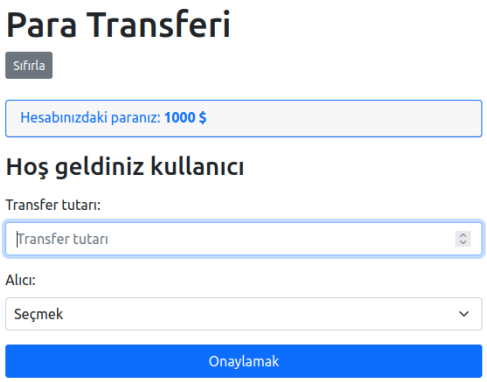
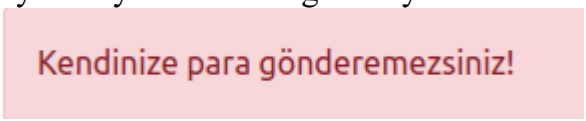
CSRF

8.2 Money Transfer

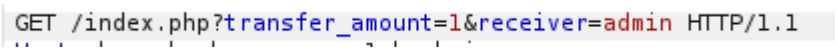
Amaç : Kullanıcı hesabına para geldiğinde görünen transfer numarası nedir?



Şu şekilde para transferi için panelimiz var buradan kendimize gönderemiyoruz kendine para gönderemezsin diye uyarı alıyoruz hemen göstereyim.

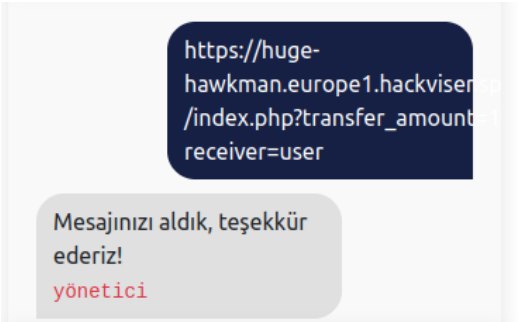


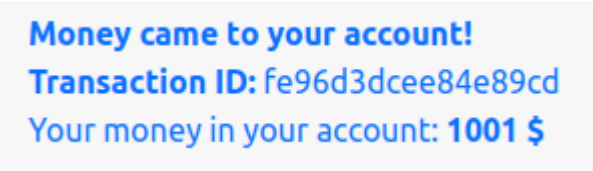
Zaten gönderebilsek bu farklı zafiyete girer bizim amacımız adminden para almak.
Yine arkada dönen isteğe göz atalım.



=admin kısmını user yapıp admine atalım destek ekibden.

Ve tüm URL'i ayarladım ve destek ekibine atalım.
Bu linki eğer biz enterlarsak sistem bizim COOKİE mizi kontrol edip zaten user kullanıcısının biz olduğunu tespit edip parayı atmicaktır. Ancak bu url'i başkasında çalıştırırsak, o bize COOKİE uyuşmadığı için parayı atabilicektir.
Temel mantığı bu.





Ve para transferimiz gerçekleşti paramız geldi.
Cevap : fe96d3dcee84e89cd