

CSRF

8.2 Money Transfer

Amaç : Kullanıcı hesabına para geldiğinde görünen transfer numarası nedir?

Para Transferi

Sıfırla

Hesabınızdaki paranız: 1000 \$

Hoş geldiniz kullanıcı

Transfer tutarı:

Transfer tutarı

Alıcı:

Seçmek

Onaylamak

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

Kendinize para gönderemezsiniz!

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

```
GET /index.php?transfer_amount=1&receiver=admin HTTP/1.1
```

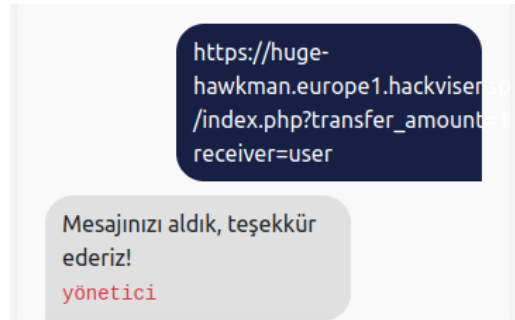
=admin kısmını user yapıp admine atalım destek ekibden.

https://huge-hawkman.europe1.hackviser.space/index.php?transfer_amount=1&receiver=user

Ve tüm URL'i ayarladım ve destek ekibine atalım.

Bu linki eğer biz enterlarsak sistem bizim COOKIE mizi kontrol edip zaten user kullanıcısının biz olduğunu tespit edip parayı atmıcağıdır. Ancak bu url'i başkasında çalıştırırsak, o bize COOKIE uyuşmadığı için parayı atabilecektir.

Temel mantığı bu.



Money came to your account!
Transaction ID: fe96d3dcee84e89cd
Your money in your account: 1001 \$

Ve para transferimiz gerekleřti paramız geldi.

Cevap : fe96d3dcee84e89cd