MONEY TRANSFER WRİTE-UP

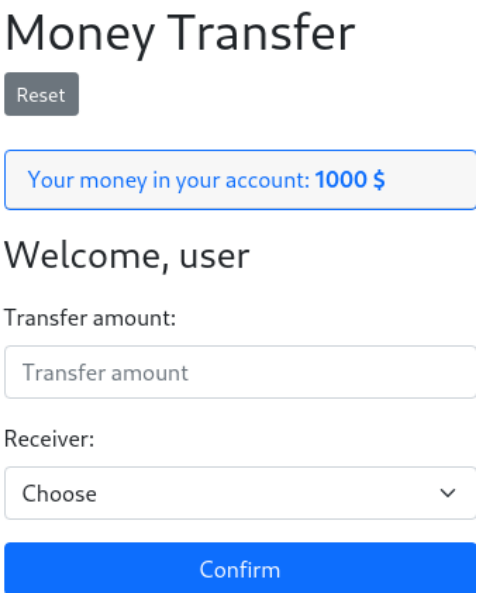
Bu yazımda sizlere Hackviser platformu üzerinde bulunan Web Lab kısmı altında CSRF zafiyetinin Money Transfer labının çözümünü anlatacağım.

SENARYO: Bu laboratuvar bir CSRF güvenlik açığı içermektedir.

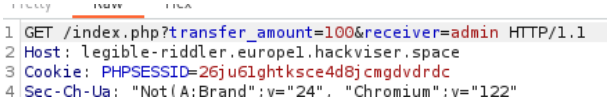
Laboratuvarı tamamlamak için, hesabınıza para aktarmak için bir URL oluşturun ve bağlantıyı sağ alttaki canlı destek aracılığıyla gönderin. Destek personeli gönderdiğiniz bağlantıyı çalıştıracak ve istemeden hesabınıza para aktaracaktır.

Kullanıcı hesabına para geldiğinde görünen transfer numarası nedir?

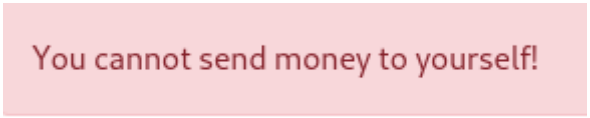
ÇÖZÜM: Sitemize bir giriş yapalım.



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



Burada admin yazan yeri user olarak değiştirip deneyelim.

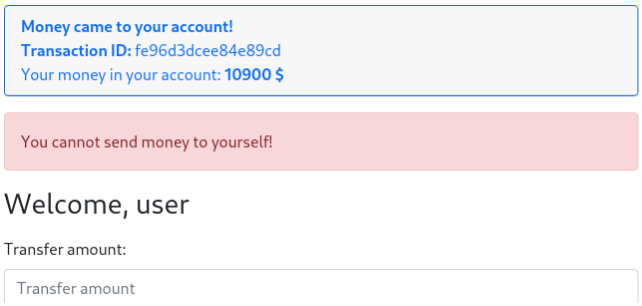


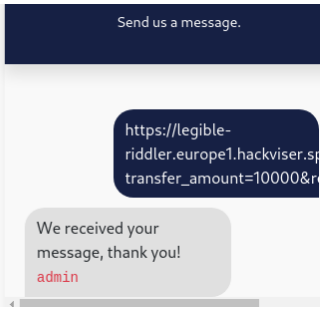
Cevabını aldık. Senaryoda da dediği gibi canlı desteğe URL isteği göndererek o bizim için bu işlemi yapabilir.

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.

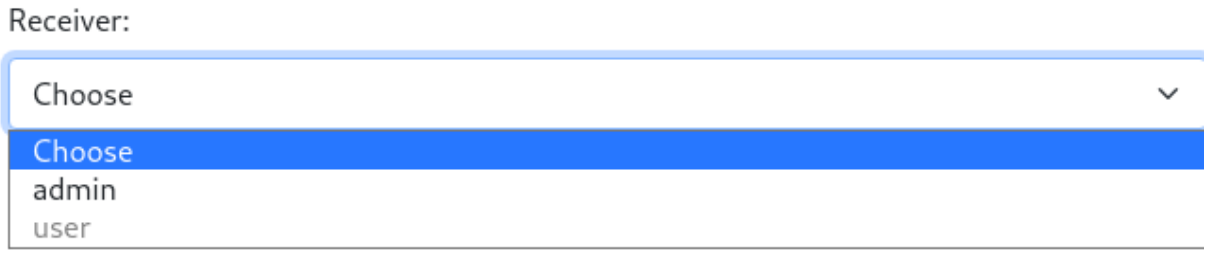




İşlemimiz başarılı oldu.

Cevap: **fe96d3dcee84e89cd**

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



Burada bizim user olduğumuzu gördük.