Cross Site Request Forgery (CSRF)

Change Password

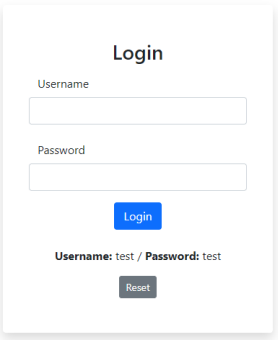
Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar bir CSRF zafiyeti içermektedir.

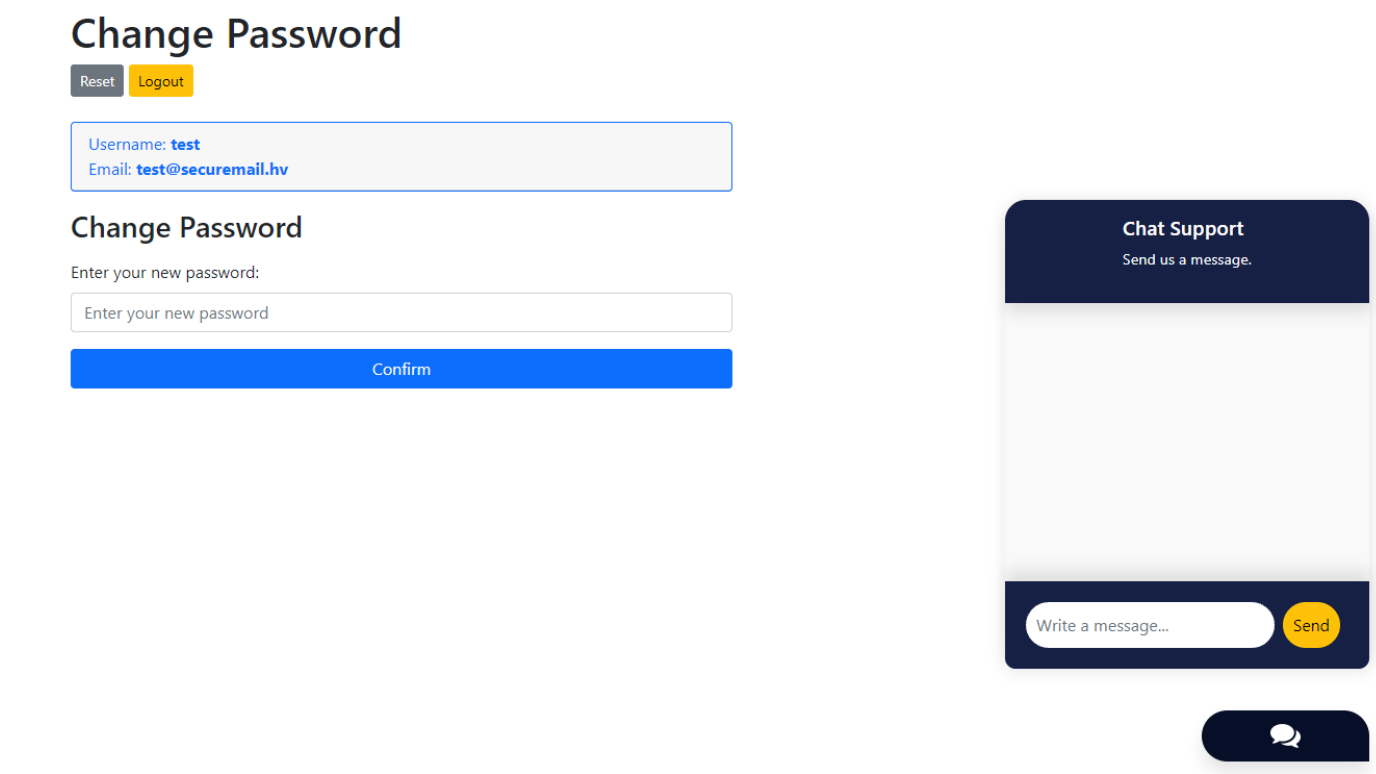
Laboratuvarı tamamlamak için parola değiştirme uç noktası ile özel bir URL oluşturun ve bağlantıyı sağ alttaki canlı destek aracılığıyla gönderin. Destek personeli gönderdiğiniz bağlantıyı açacak ve parolası değiştirilecektir. Yeni parola ile yönetici kullanıcının hesabına giriş yapın.

Yönetici kullanıcı hesabına giriş yaparken görülen e-posta adresi nedir?

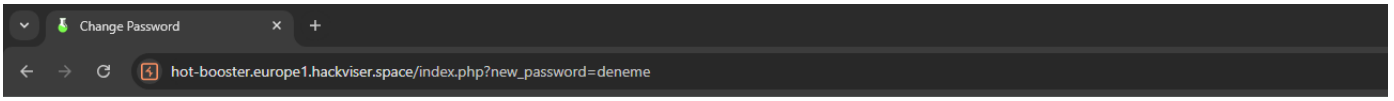
Öncelikle bi web sitesini ziyaret edelim

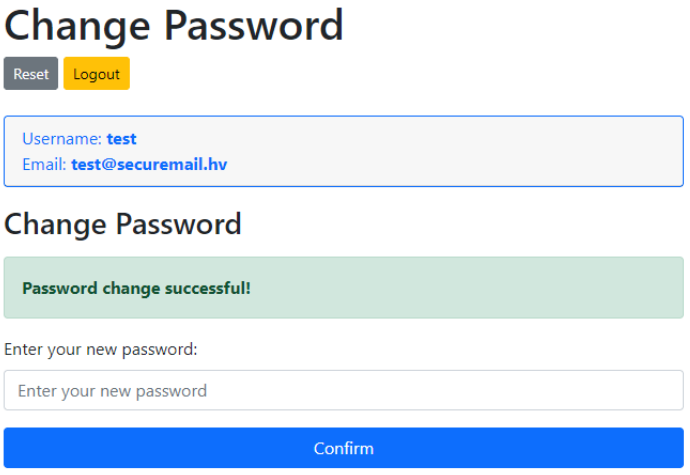


Böyle bi sayfa karşıladı giriş yapalım

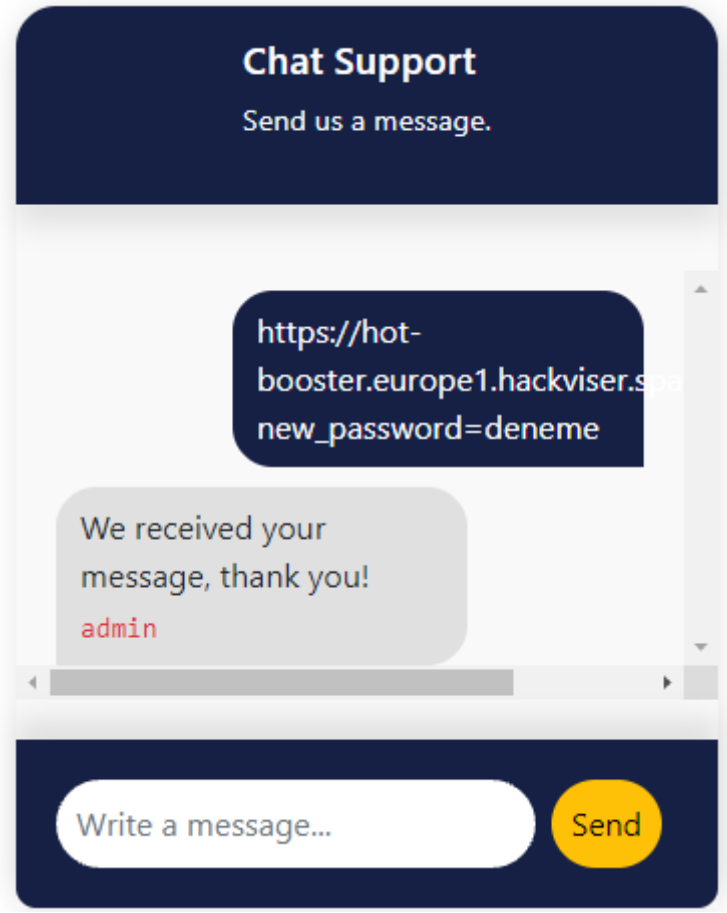


Şifremizi değiştirmemiz için bir alan var. Şimdi parolamızı deneme olarak değiştirelim.

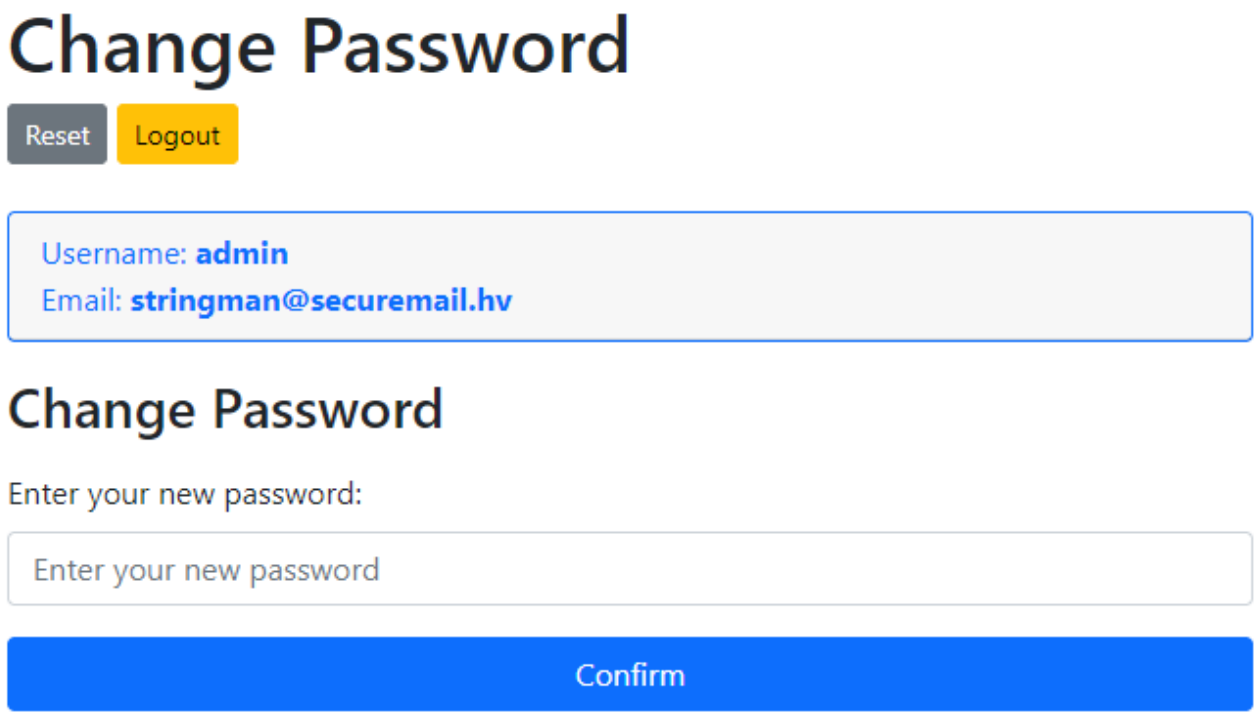




Göründüğü üzere URL alanında parolamızı değiştirmek için gönderdiğimiz istek çıktı. Şimdi bunu chatbotdan admine göndererek urlyi açıp şifresini deneme olarak değiştirtip adminin hesabına ulaşabiliriz.



Şimdi admin olarak giriş yapmayı deneyelim.



Ve evet adminin e posta adresini görüntülemeyi başarıyoruz.

Money Transfer

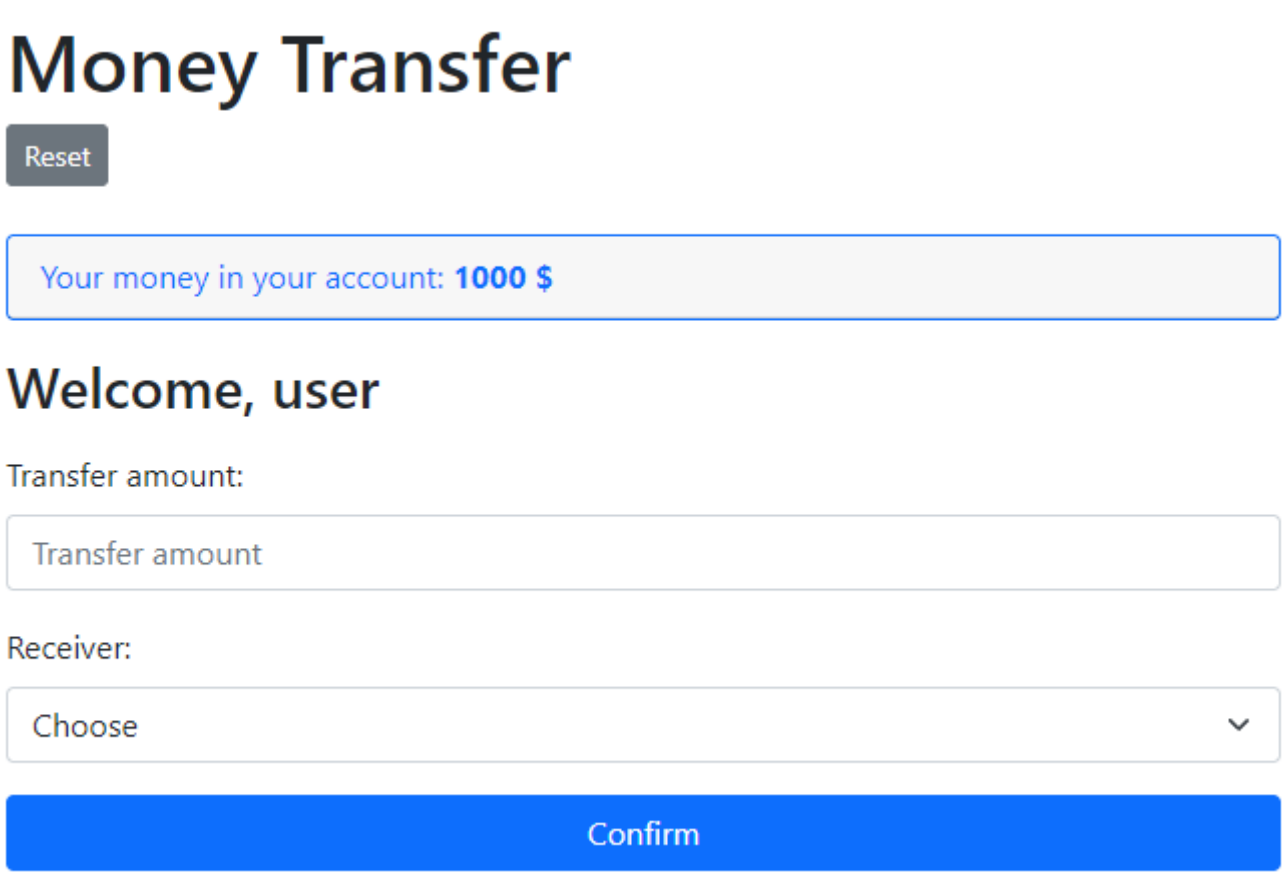
Başlangıçta bize lab hakkında bilgi vermiş

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?

Öncelikle web sitesini ziyaret edelim

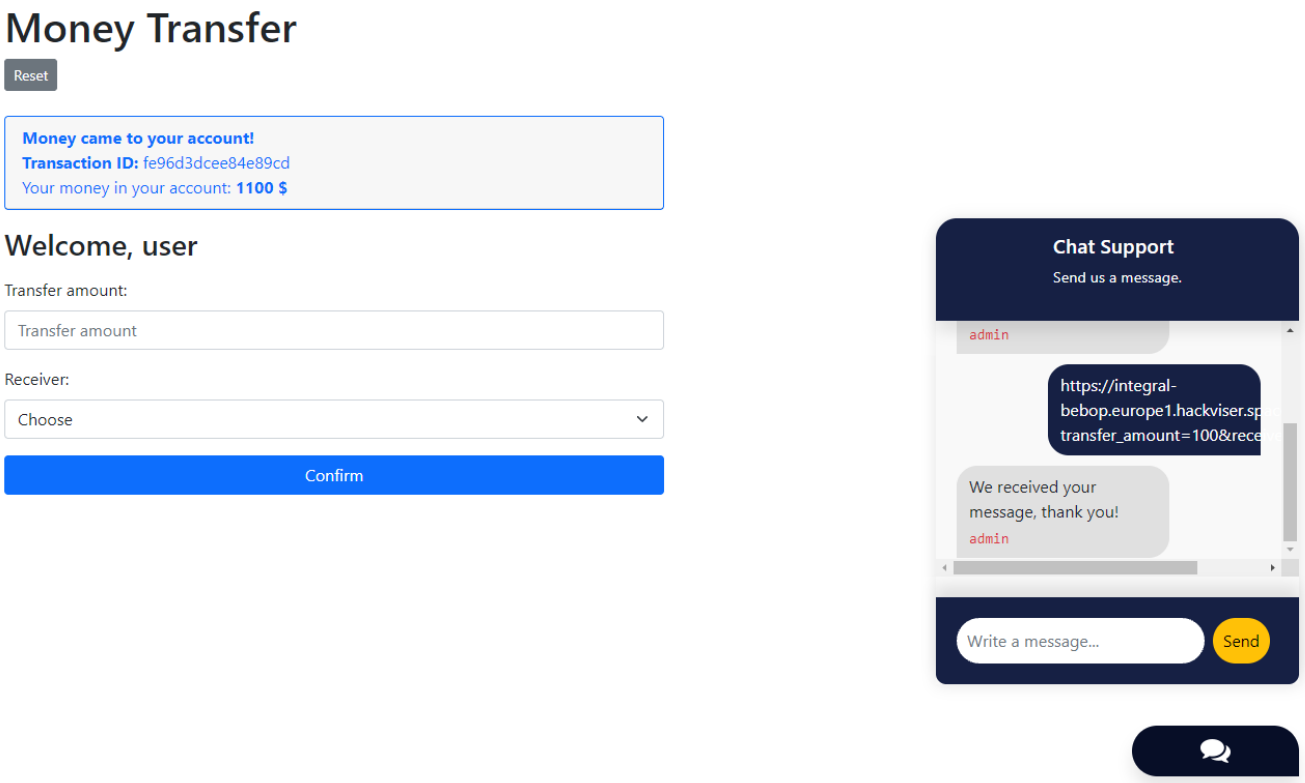


Bizi böyle bir sayfa karşılıyor. Şimdi yapmamız gereken chatbottan admine bir link göndererek kendi hesabımıza para aktarmak ve transfer numarasını öğrenmek. İsteğimizi yapalım ve burp ile araya girelim

Get isteğini burada görüntüleyebiliyoruz. Şimdi gönderilecek kişiyi user olarak değiştirelim ve bunu urlye uyarlayalım.

https://integral-bebop.europe1.hackviser.space/index.php?transfer_amount=100&receiver=user

Şu şekilde bi url elde ettik şimdi bunu canlı desteğe gönderelim.



Ve evet başarılı olduk ve transfer id yi elde etmeyi başardık.

Başka bir yazıda görüşmek üzere !

Linkedin

Github

İnstagram

Medium

Ayberk İlbaş