

Hackviser Insecure Direct Object References (IDOR)

Invoices

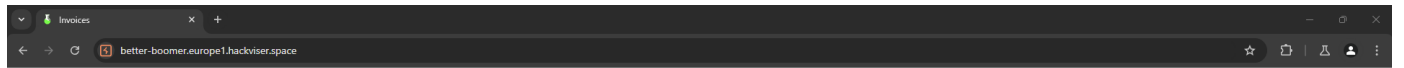
Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar, uygulamadaki diğer müşterilerin faturalarına yetkisiz erişime izin veren bir Güvensiz Doğrudan Nesne Referansları (IDOR) güvenlik açığı içerir.

Laboratuvarı tamamlamak için URL'deki "invoice_id" değerini değiştirerek diğer müşterilerin faturalarına erişin ve "Emilia Rawne" adlı müşterinin faturasını bulun.

Emilia Rawne adlı müşterinin e-posta adresi nedir?

Öncelikle web sitesine gidelim

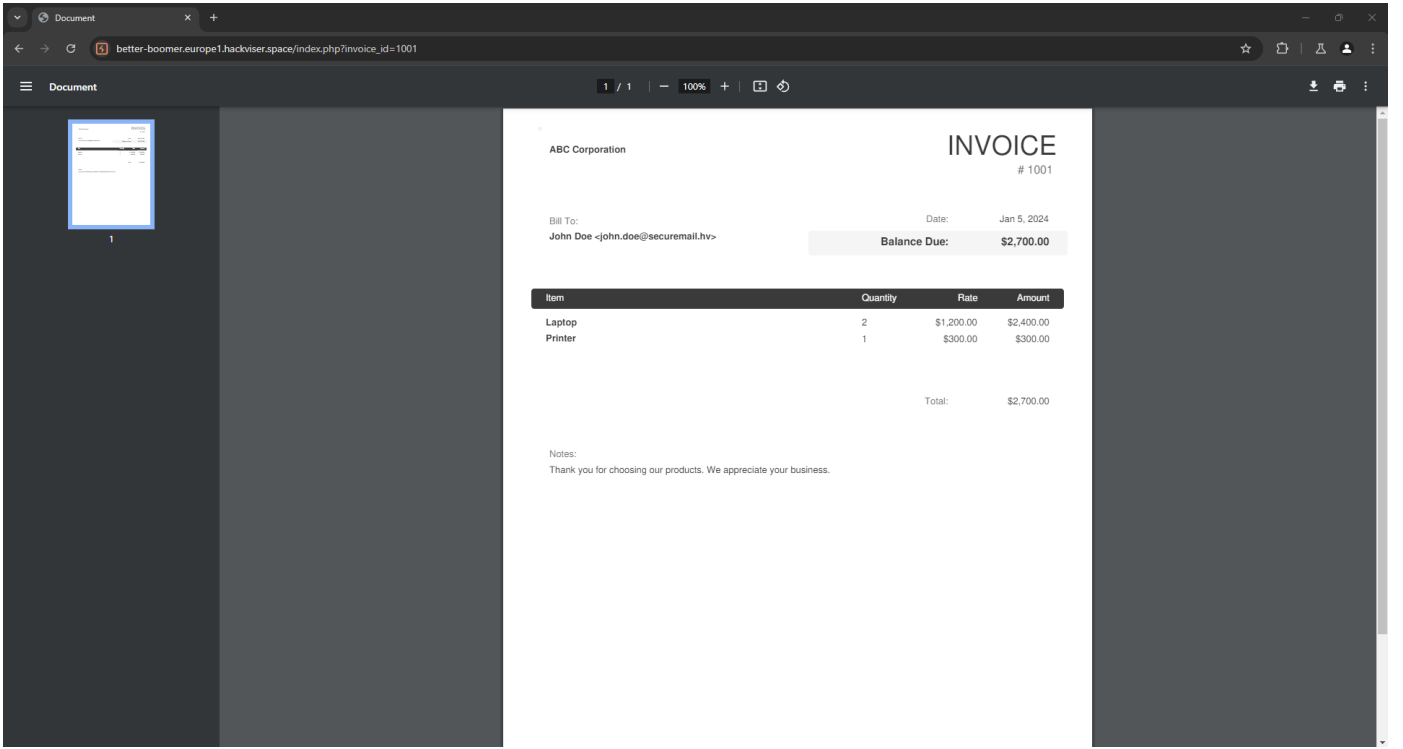


Faturalar

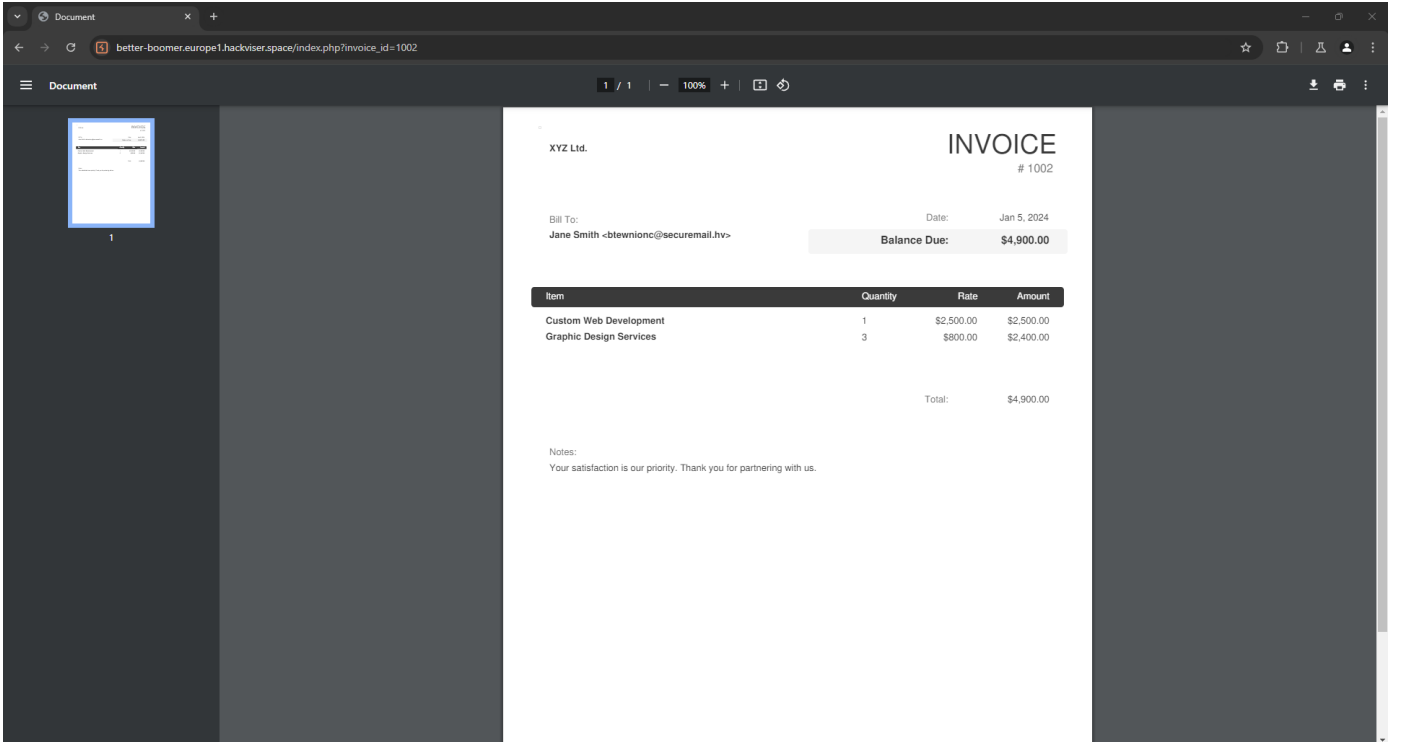
Yeni bir faturanız var!

Faturanızı görüntülemek için tıklayın!

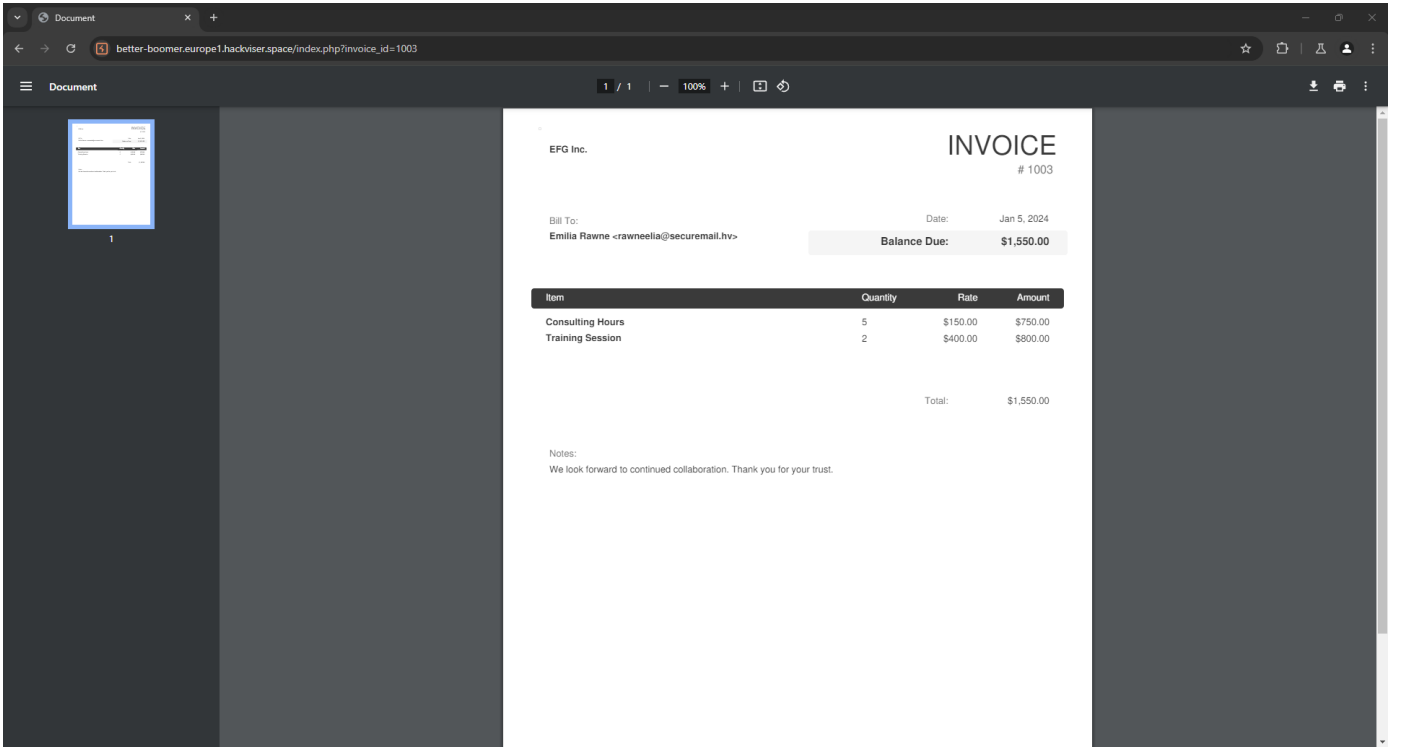
Görüntüleyelim



Görüntülediğimizde urlde invoice kısmı ilgimi çekiyor ve arttırmayı deniyorum



1002 yaptığımda Jane Smith adında bir kişinin e posta bilgilerine erişiyorum



1003 yaptığımda ise Emilia Rawne adlı müşterinin e-posta adresine ulaşmayı başarıyorum

Ticket Sales

Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar, bir ürünün daha düşük bir fiyata satın alınabilmesine neden olan bir Güvensiz Doğrudan Nesne Referansları (IDOR) güvenlik açığı içerir.

Başlangıç bakiyeniz bilet satın almak için yeterli değildir. Laboratuvarı tamamlamak için bilet satın alımı esnasında sunucuya gönderilen fiyatı manipüle ederek bilet satın alın.

Bilet satın alındıktan sonra görünen sipariş numarası nedir?

Öncelikle web sitesine gidelim



Ticket Sales

Reset

The price of one ticket is 300 \$
Amount of money in your account: 50 \$

How many tickets do you want to buy ?

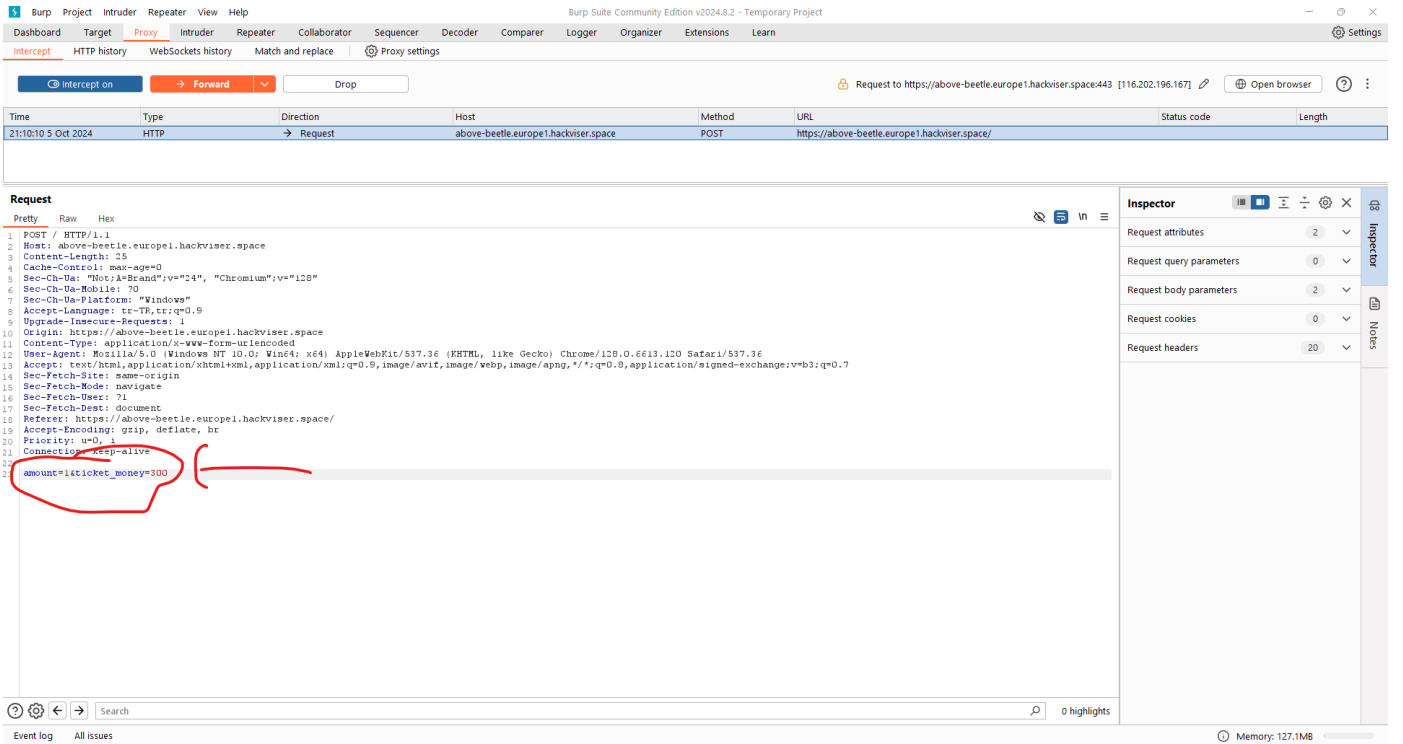
You do not have enough balance in your account!

Enter the number of tickets:

Enter the number of tickets

Buy

50 dolar bakiyemiz var bilet almak için 300 dolara ihtiyacımız varmış. Satın al dedikten sonra burp ile araya girerek IDOR zafiyetini uygulamaya çalışabiliriz



Burp ile araya girdiğimizde bilet adetini ve fiyatını görebiliyoruz. Fiyatı 0 Bilet sayısını da 2 yapmayı deneyebiliriz.

Ticket Sales

Reset

The price of one ticket is 300 \$
Amount of money in your account: 50 \$

How many tickets do you want to buy ?

The purchase was successful.

Number of tickets you bought: 2
Money you pay: 0 \$
Order ID: 65274efc95282d0cc

Enter the number of tickets:

Enter the number of tickets

Buy

Ve evet sipariş numarasını görüntülemeyi başardık.

Change Password

Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar, diğer kullanıcıların parolasını yetkisiz bir şekilde değiştirmeye yol açan Güvensiz Doğrudan Nesne Referansları (IDOR) güvenlik açığı içerir.

Laboratuvarı tamamlamak için "admin" kullanıcısının parolasını, parola değiştirme uç noktasındaki IDOR zafiyetini istismar ederek değiştirin ve hesabına giriş yapın.

"admin" isimli kullanıcının telefon numarası nedir? (Cevap Formatı: 000-000-0000)

Öncelikle web sitesini ziyaret edelim



Login

Username

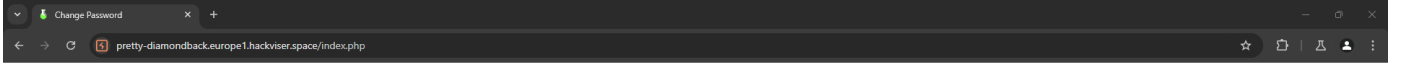
Password

Login

Username: test / Password: test

Reset

test / test yazarak giriş yapalım



Change Password

Reset Logout

Username: test

Phone: 227-290-9627

Change Password

Enter your new password:

Confirm

Bi parola değıştirme ekranımız var. Şifremizi değıştirelim değıştirirken de burp ile araya girelim

Request to https://pretty-diamondback.europe1.hackviser.space:443 [116.202.196.167] Open browser

Time	Type	Direction	Host	Method	URL	Status code	Length
21:16:06 5 Oct 2024	HTTP	→ Request	pretty-diamondback.europe1.hackviser.space	POST	https://pretty-diamondback.europe1.hackviser.space/index.php		

Request

Pretty Raw Hex

```
1 POST /index.php HTTP/1.1
2 Host: pretty-diamondback.europe1.hackviser.space
3 Cookie: PHPSESSID=3ngod6vumu8iq397q3rahbicz5
4 Content-Length: 25
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="120"
7 Sec-Ch-Ua-Mobile: 70
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: tr-TR,tr;q=0.9
10 Upgrade-Insecure-Requests: 1
11 Origin: https://pretty-diamondback.europe1.hackviser.space
12 Content-Type: application/x-www-form-urlencoded
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6613.120 Safari/537.36
14 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
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://pretty-diamondback.europe1.hackviser.space/index.php
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 Connection: keep-alive
23
24 password=deneme&user_id=2
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 1

Request headers 21

Event log All issues 0 highlights Memory: 127.1MB

Evet değiřtirmek istediđimiz řifreyi ve user_id yi g r yoruz user id miz 2 olarak verilmiř genellikle user id si 1 olan kullanıcı admindir site kurulduđu gibi a ılan ilk hesap onun olduđu i in ondan dolayı řimdi řifreyi deneme yapıp user id yide 1 olarak vereceđim ve admin hesabına admin / deneme olarak giriř yapmayı deneyeceđim

Evet adminin parolasının deđiřtiđini g r yoruz. řimdi gidip giriř yapalım



Ve evet adminin hesabına giriş yaparak telefon numarasını görüntülemeyi başardık.

Başka bir yazıda görüşmek üzere !

[Linkedin](#)

[Github](#)

[Instagram](#)

[Medium](#)

Ayberk İlbaş