## **IDOR**

Yetki denetiminin eksikliğinden kaynaklanan bu zafiyet yetkisiz kişilerin yetkisi dışında ulaşamayacağı bilgilere ulaşabilmesinden kaynaklanıyor.

Güvenlik kontrollerine özen göstermek bu sorunu çözmektedir. Aksi takdirde yetkisi olmayan biri sadece id numarasını değiştirerek dahi farklı kullanıcıların bilgilerine erişebilir.

### **ABC Corporation**



Date:

Jan 5, 2024

Bill To:

John Doe <john.doe@securemail.hv> Balance Due: \$2,700.00

ltem	Quantity	Rate	Amount
Laptop	2	\$1,200.00	\$2,400.00
Printer	1	\$300.00	\$300.00
		Total:	\$2,700.00

Notes

Thank you for choosing our products. We appreciate your business.

EFG Inc.

INVOICE

# 1003

Bill To:

Emilia Rawne <rawneelia@securemail.hv>

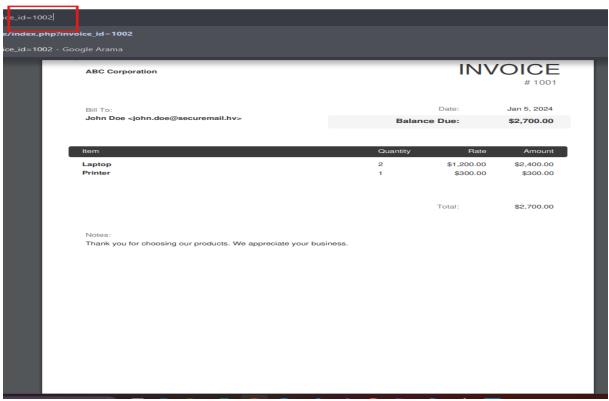
Date:

Jan 5, 2024

**Balance Due:** 

\$1,550.00

Item	Quantity	Rate	Amount
Consulting Hours	5	\$150.00	\$750.00
Training Session	2	\$400.00	\$800.00
		Total:	\$1.550.00



XYZ Ltd.

**INVOICE** 

# 1002

Bill To:
Jane Smith <btewnionc@securemail.hv>

Date: Jan 5, 2024

Balance Due: \$4,900.00

Item	Quantity	Rate	Amount
Custom Web Development	1	\$2,500.00	\$2,500.00
Graphic Design Services	3	\$800.00	\$2,400.00
		Total:	\$4,900.00

#### Notes:

Your satisfaction is our priority. Thank you for partnering with us.

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 alını.

Bilet satın alındıktan sonra görünen sipariş numarası nedir?

İkinci görevimiz ise fiyat bilgisini manipüle ederek daha az ya da bedavaya ürün satın almak.

## **Ticket Sales**



The price of one ticket is 300 \$

Amount of money in your account: 50 \$

## How many tickets do you want to buy?

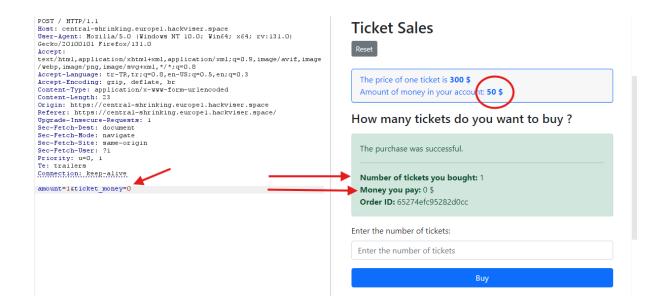
Enter the number of tickets:

Enter the number of tickets

Buy

Te: trailers
Connection: keep-alive
amount=4&ticket\_money=300

Burp ile araya girip ticked\_money değerini değiştirmem yeterli.

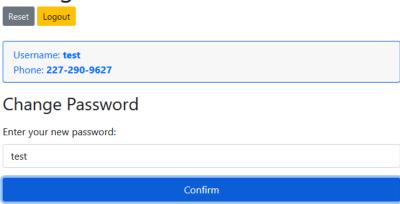


Bu laboratuvar, diğer kullanıcıların parolasını yetkisiz bir şekilde değiştirmeye yol açan Güvensiz Doğrudan Nesne Referansları (IDOR) güvenlik açığı içerir. Laboratuvarı tamamlamak için "admin" kullanıcısının parolasını, parola değiştirme uç noktasındaki IDOR zafiyetini istismar ederek değiştirin ve hesabına giriş yapın. "admin" isimli kullanıcının telefon numarası nedir? (Cevap Formatı: 000-000-0000)

Üçüncü görevimiz ise yine bu zafiyeti sömürerek adminin hesabına giriş yapmak.

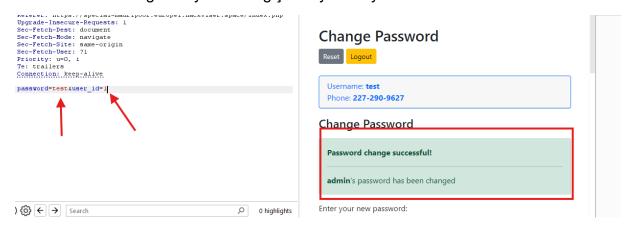
	Login
Username	
Password	
	Login
Usernam	ne: test / Password: test

# Change Password

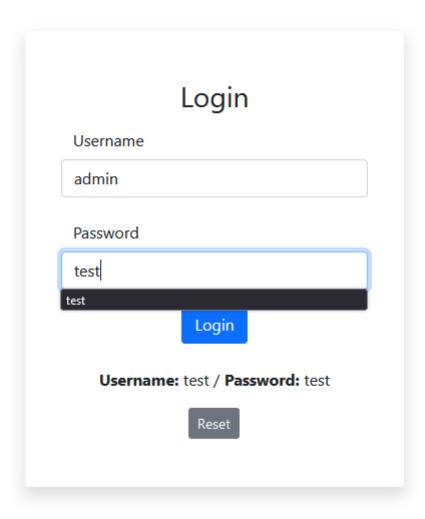


```
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
password=test&user_id=2
```

Yukarıyı inceleyecek olursak user\_id değerimiz 2 bu değer parolanın değiştirileceği kullanıcının id sini gösteriyor. 1 i değiştirmeyi deneyelim.



İd' yi 1' e çektiğimde adminin hesabına yeni parolamızı kaydetmiş olduk.



# Change Password



Username: admin Phone: 876-987-8489

# Change Password

Enter your new password:

Enter your new password

Confirm