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

INVOICE

1001

Bill To:
John Doe <john.doe@securemail.hv>

Date: Jan 5, 2024

Balance Due: $2,700.00

Item	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

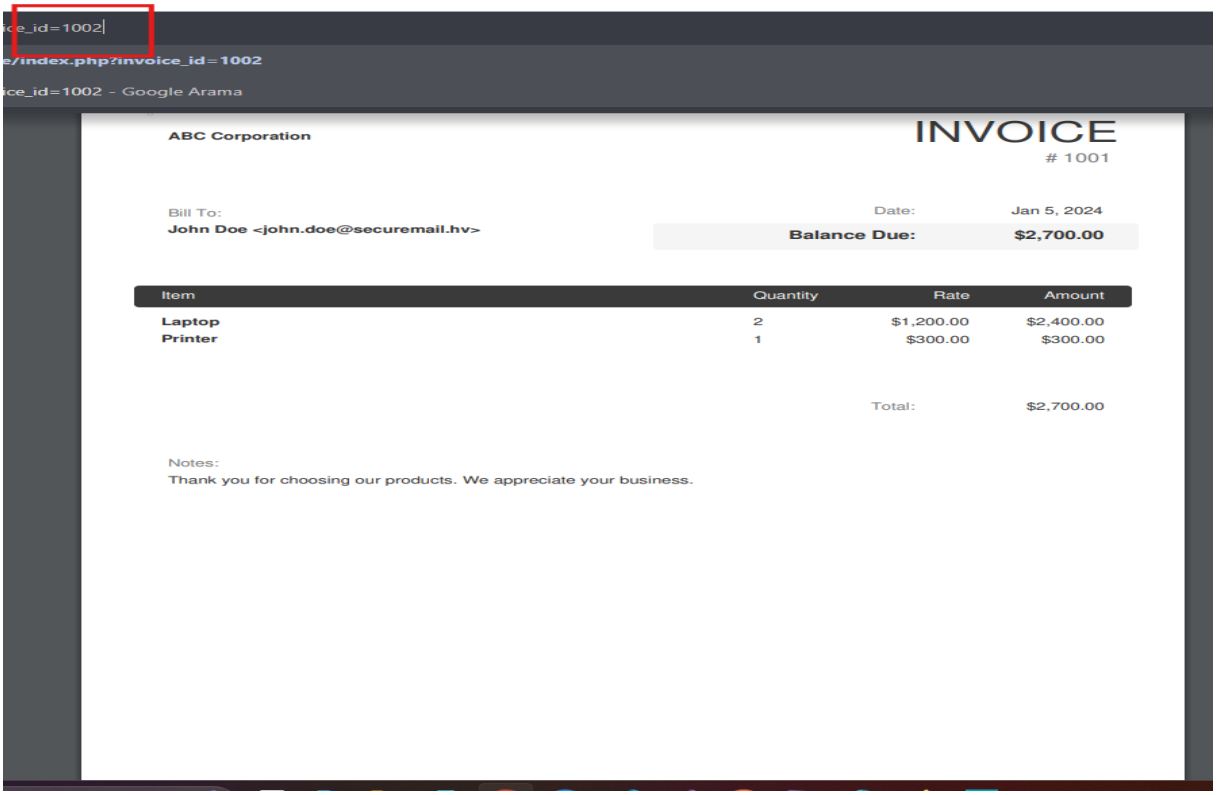
Bill To:
Emilia Rawne <rawneelia@securemail.hv>

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

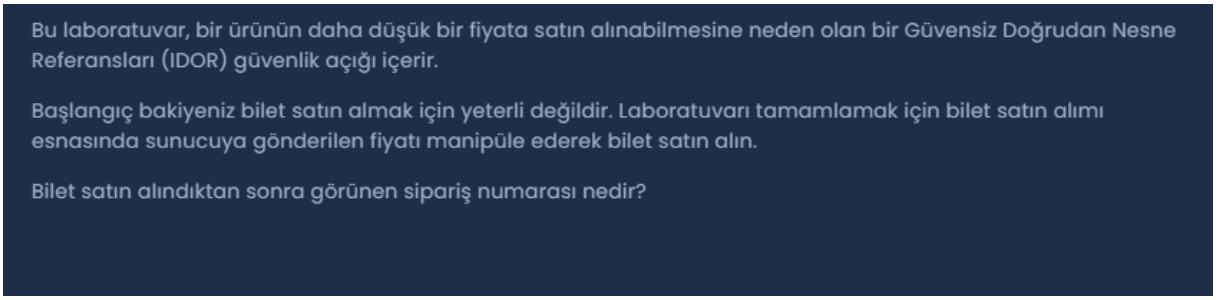
Balance Due: $4,900.00

Item	Quantity	Rate	Amount
Custom Web Development	1	$2,500.00	$2,500.00
Graphic Design Services	3	$800.00	$2,400.00

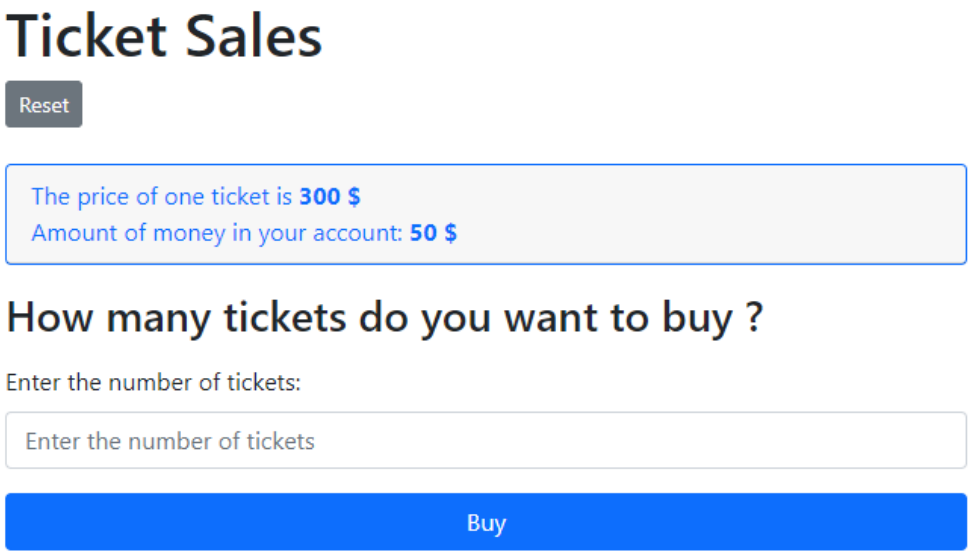
Total: $4,900.00

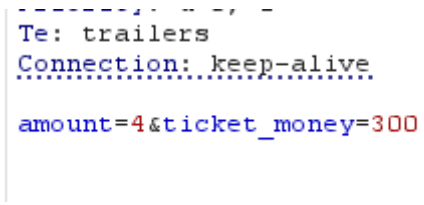
Notes:

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

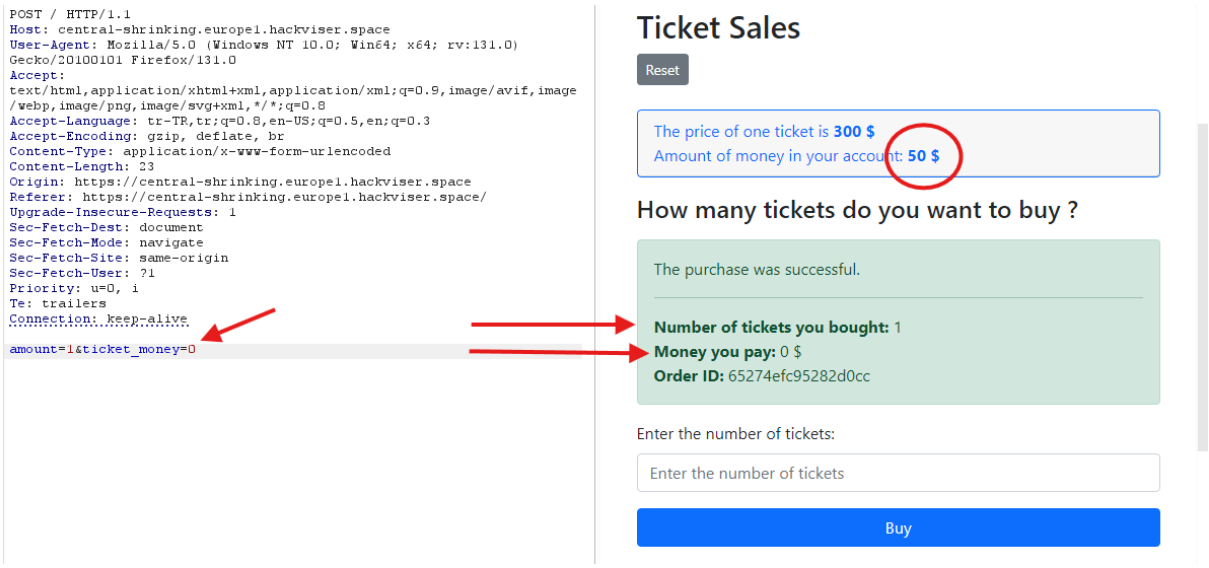


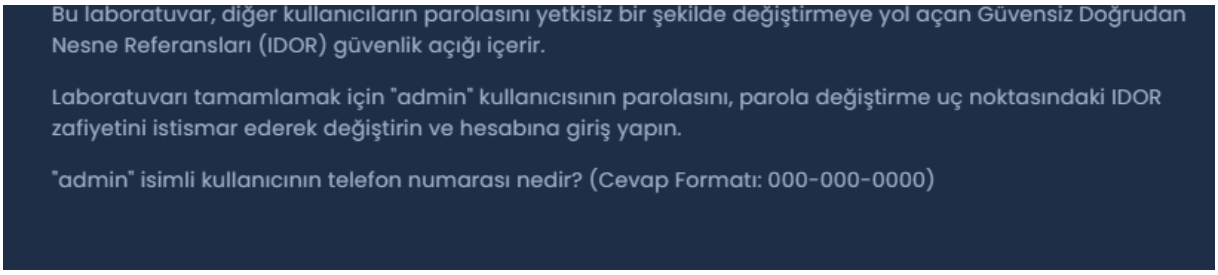
İkinci görevimiz ise fiyat bilgisini manipüle ederek daha az ya da bedavaya ürün satın almak.





Burp ile araya girip ticked_money değerini değiştirmem yeterli.





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

Login

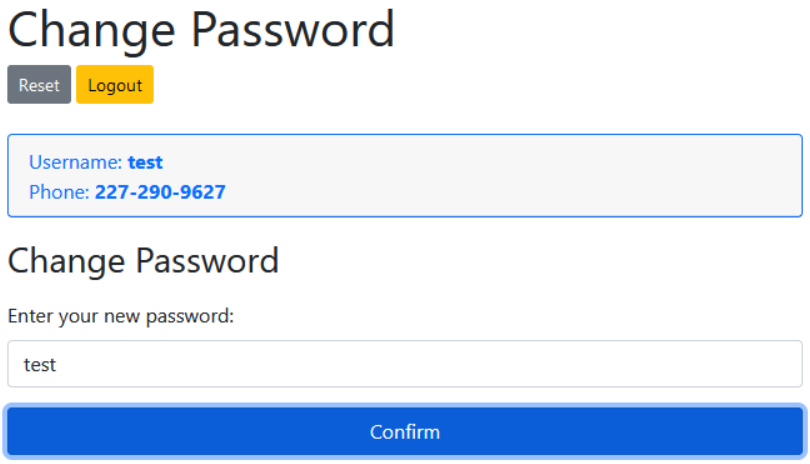
Username

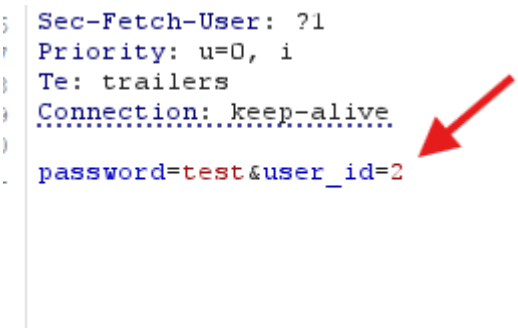
Password

Login

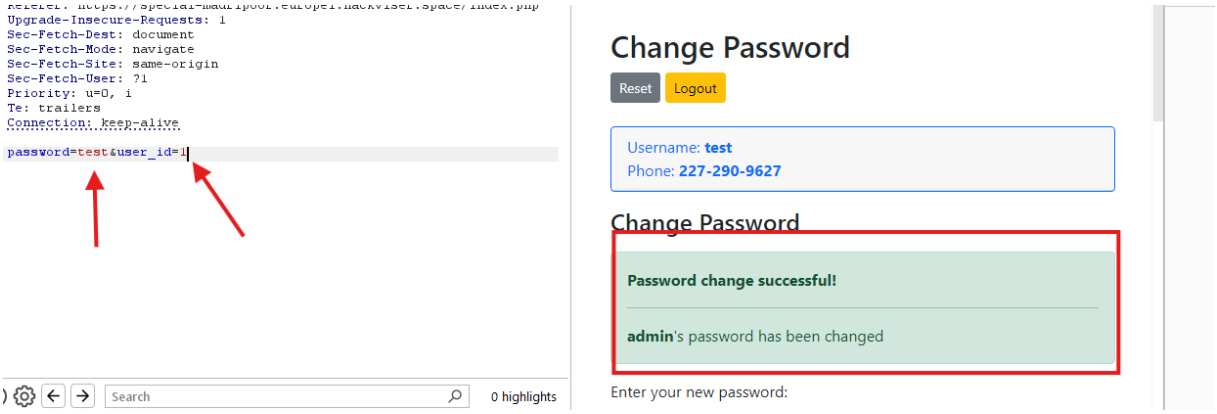
Username: test / **Password:** test

Reset





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.

Login

Username

admin

Password

test

test

Login

Username: test / **Password:** test

Reset

Change Password

Reset Logout

Username: **admin**
Phone: **876-987-8489**

Change Password

Enter your new password:

Enter your new password

Confirm