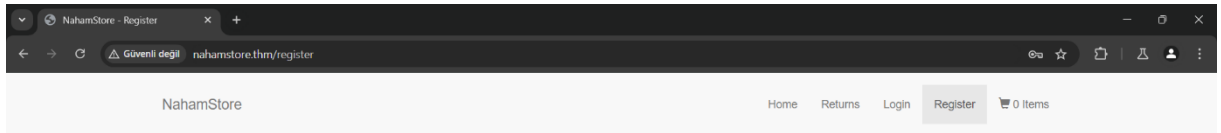
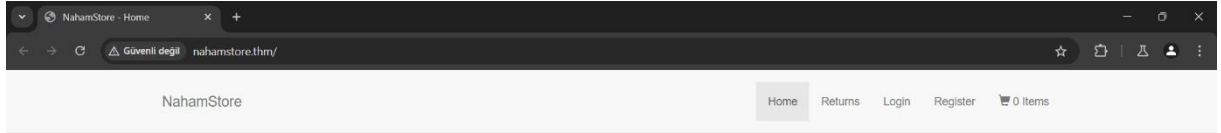


TryHackMe Lab: NahamStore Idor Write-Up

İlk önce burda idor bulmak için kullanıcı ile ilgili işlemler yapmamız lazım bu yüzden ilk hesap açmakla başlayalım.



Register An Account

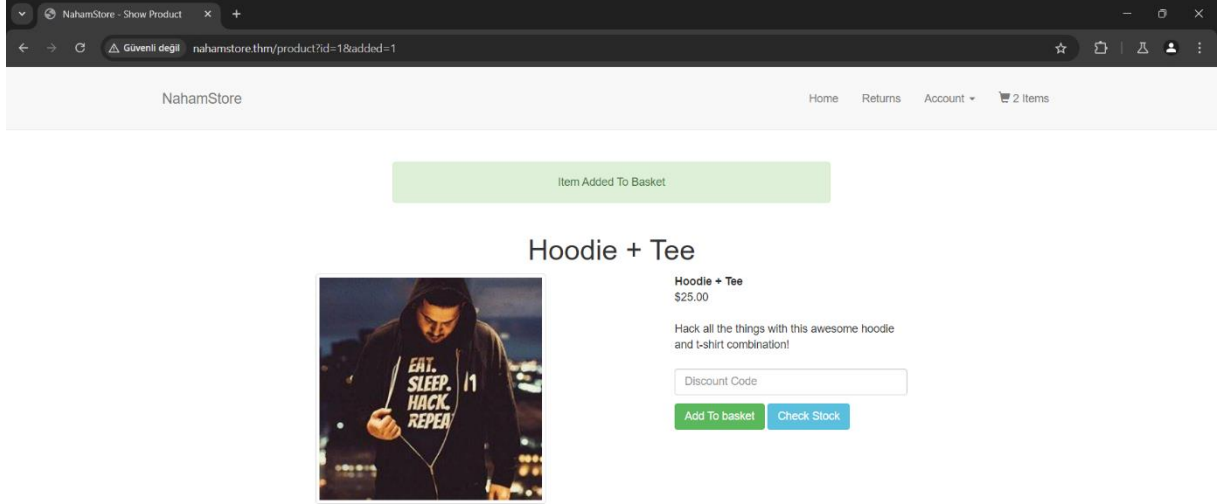
Create a NahamStore Account

Email:
test123@test.com

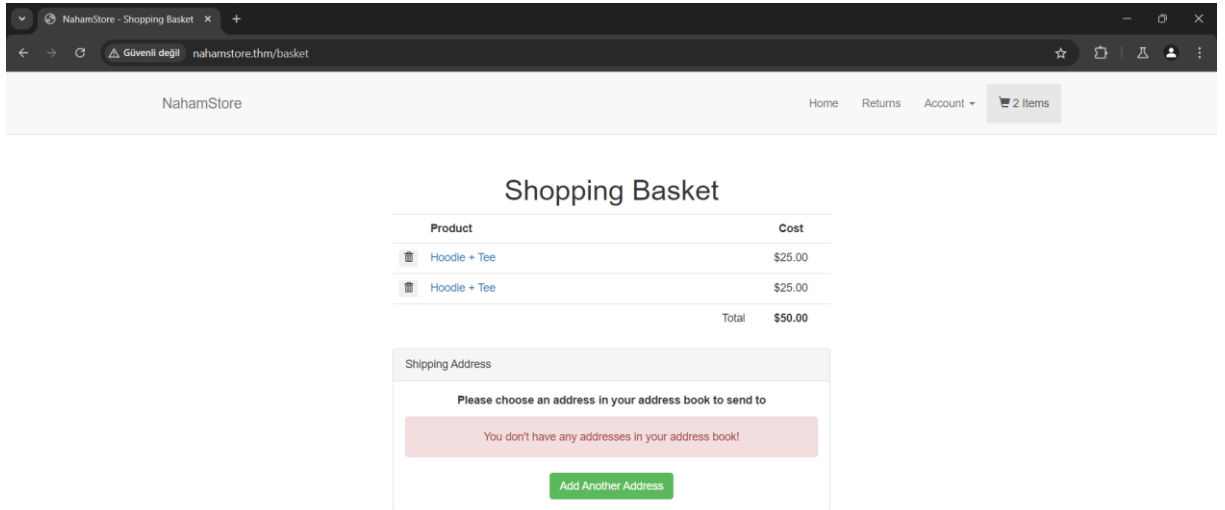
Password:

Register

Burda bir hesap oluşturduk ve sitede gezindik bizden istenen 2 soru vardı birincisi new york olan bir adres isteniliyordu ikincisi ise 3. Order id ye sahip siparişin tarih ve saati falan isteniliyor şimdi önce adreste işimiz olduğu için adres girebilecek yer arıyoruz ve aklımıza sipariş vermek geliyor 2 ürün ekleyelim.



Ekledik şimdi bu ürünlerimize bakalım.



Evet burda adres ekleme yeri bulduk hemen bir tane ekleyelim.

NahamStore - Address Book x +

← → ↻ Güvenli değil nahamstore.thm/account/addressbook?redirect_url=/basket ☆ 📄 🗑️ 👤 ⋮

NahamStore Home Returns Account ▾ 🛒 2 Items

Create Address

Title:
Mr ▾

First Name:
bdfbdfb

Last Name:
dfbdf

Address:
bdfbdf
bdfb
dfbdf

State / County:
bdfbdfb

Zip / Post Code:
dfbdf

Add Address

Hemen bir adres ekledik ve bunu kullanalım.

NahamStore - Shopping Basket x +

← → ↻ Güvenli değil nahamstore.thm/basket ☆ 📄 🗑️ 👤 ⋮

NahamStore Home Returns Account ▾ 🛒 2 Items

Shopping Basket

Product	Cost
🗑️ Hoodie + Tee	\$25.00
🗑️ Hoodie + Tee	\$25.00
Total	\$50.00

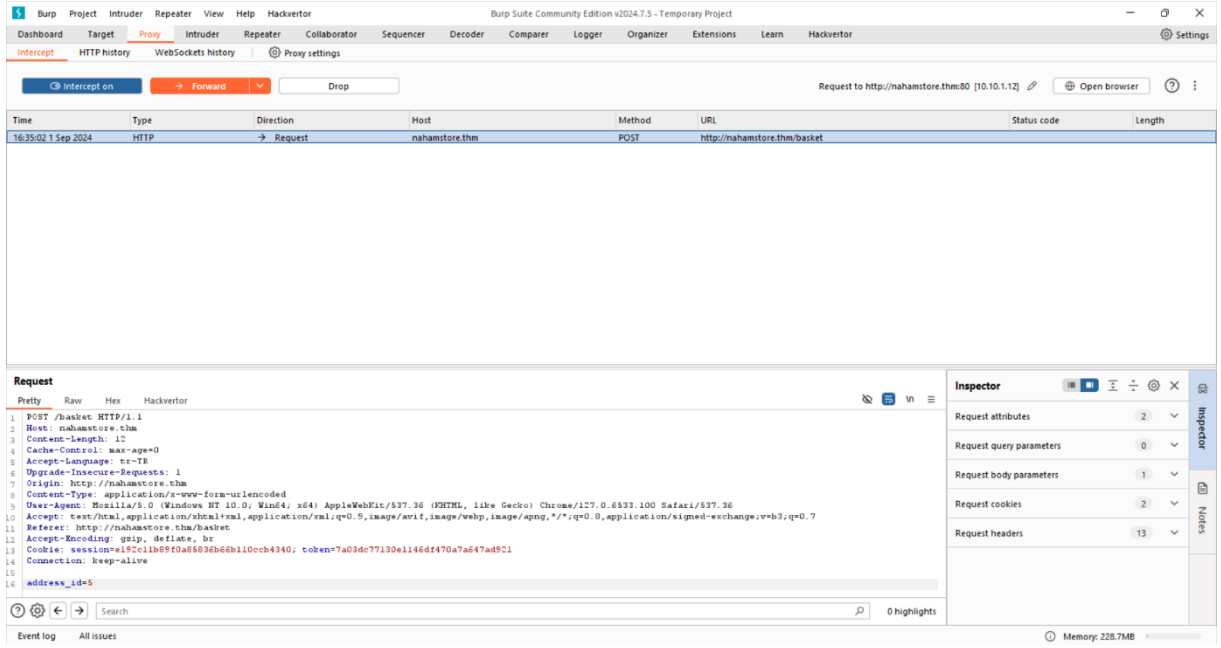
Shipping Address

Please choose an address in your address book to send to

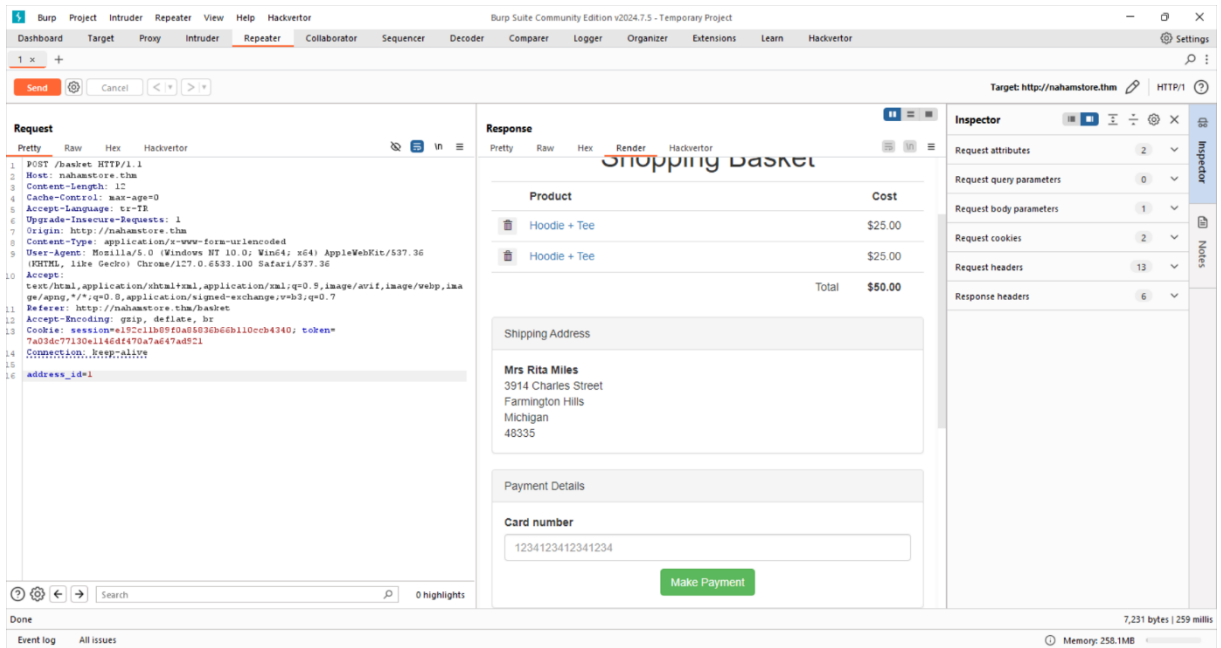
Mr bdfbdfb dfbdf

Add Another Address

Şimdi burda adres seçerken burp suite ile izleyelim.



Burda karřımıza adress id parametresi çıktı bunu 1 olarak deęiřtirip deneyelim.



Tek tek biraz böyle bakalım arayalım new york daki adresi.

Two screenshots of Burp Suite Community Edition v2024.7.5 showing a web application security tool interface. The top screenshot shows a request to the NahamStore application, and the bottom screenshot shows the response, which is a "Shopping Basket" page. The response contains a table of items and a shipping address.



Request (Top Screenshot):

```
1 POST /basket HTTP/1.1
2 Host: nahamstore.thm
3 Content-Length: 12
4 Cache-Control: max-age=0
5 Accept-Language: tr-TR
6 Upgrade-Insecure-Requests: 1
7 Origin: http://nahamstore.thm
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
10 Accept:
11 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
12 Referer: http://nahamstore.thm/basket
13 Accept-Encoding: gzip, deflate, br
14 Cookie: session=a17c11b0f0a08503b6b110ccb4340; token=7a03dc77130e1146d4f70a7a647ad521
15 CONNECTION: keep-alive
16 address_id=1
```

Response (Bottom Screenshot):

NahamStore

Shopping Basket

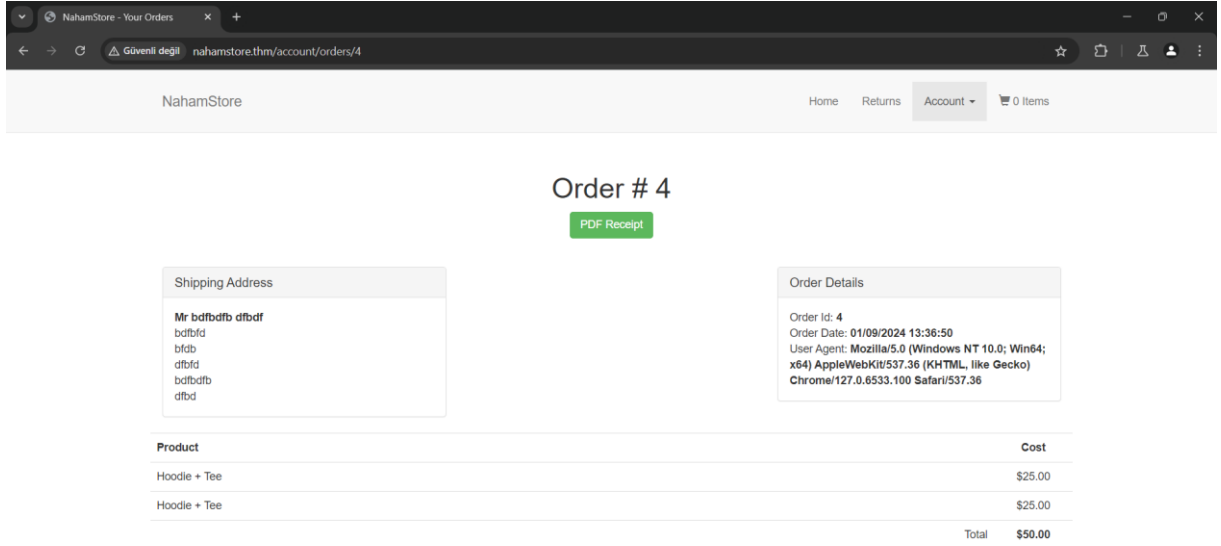
Product	Cost
 Hoodie + Tee	\$25.00
 Hoodie + Tee	\$25.00
Total	\$50.00

Shipping Address

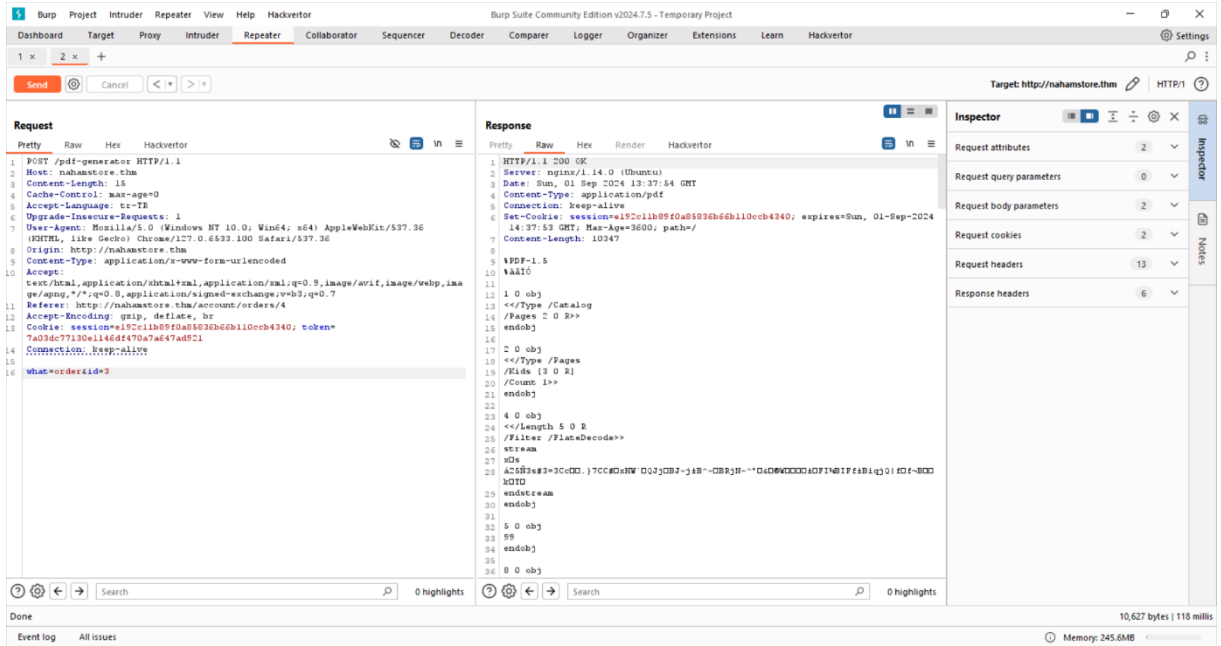
Mr Jimmy Jones
3999 Clay Lick Road
Englewood
Colorado
80112

Payment Details

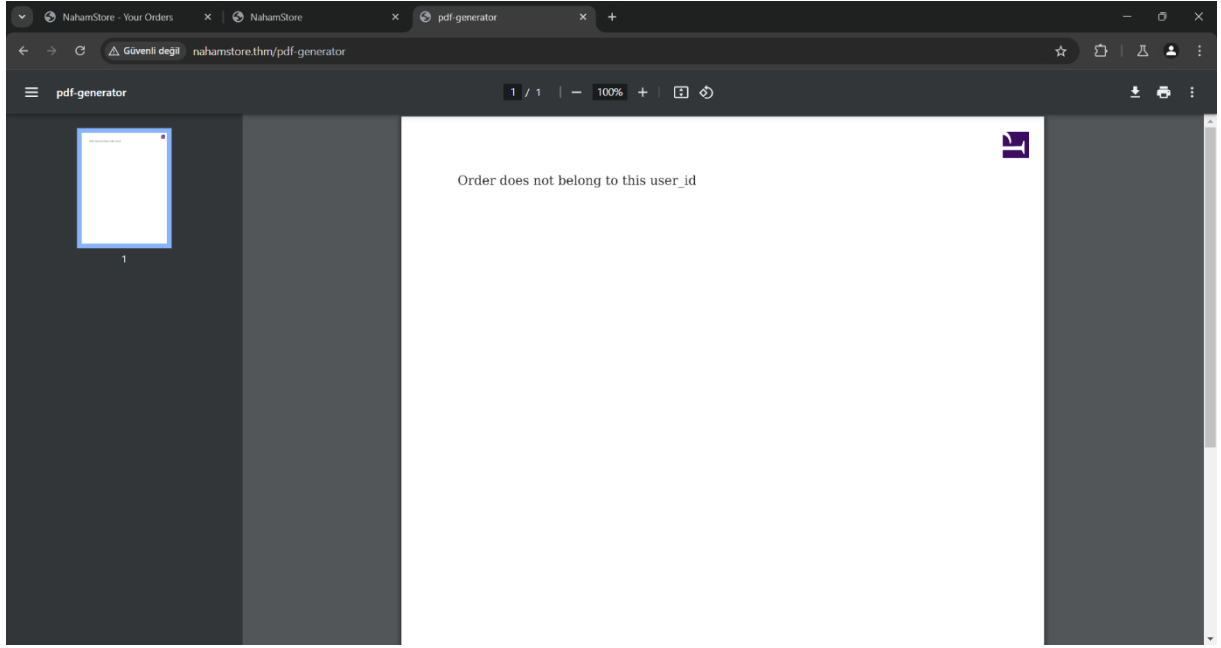
Ve id=3 te bulduk ilk satırı isteniliyordu bizden 160 Broadway olucak cevap.Şimdi ikinci kısmı bulmaya çalışalım ikinci kısımda bizden tarih saat falan isteniliyordu bunu bulmak için şipariş verelim bi tane.



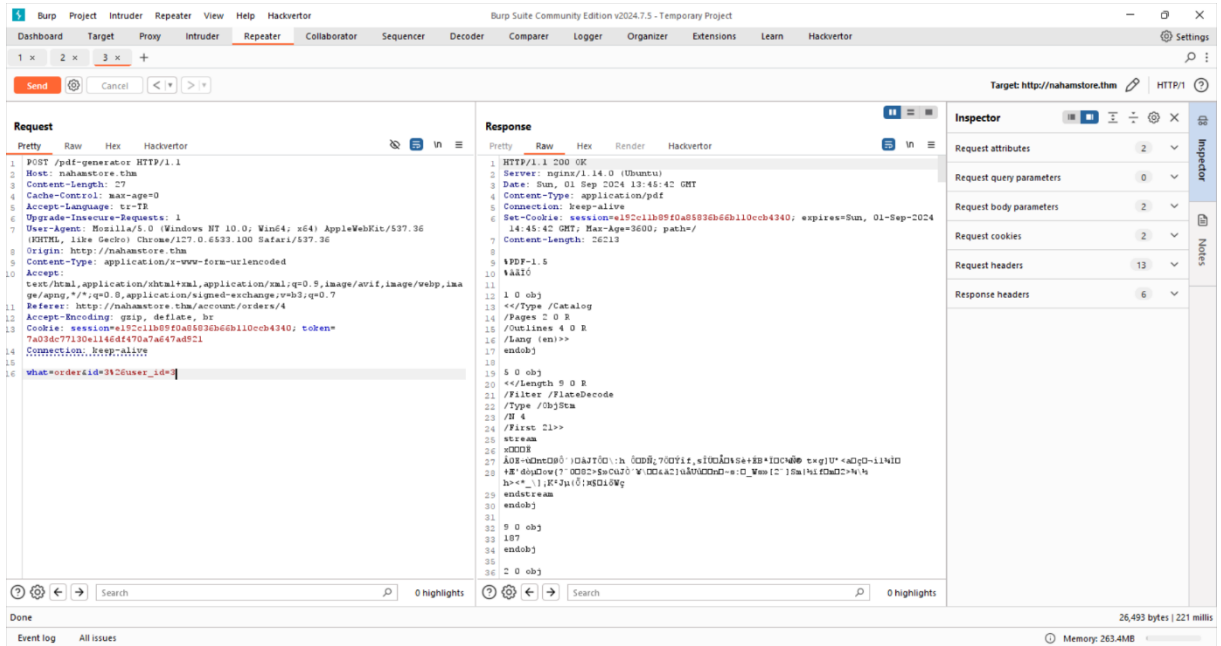
Burda siparişi oluşturduk ve tarih falan çıktı ama burda bir şey bulamadık değiştirebileceğimiz o yüzden pdf tuşuna basıp izliyoruz.



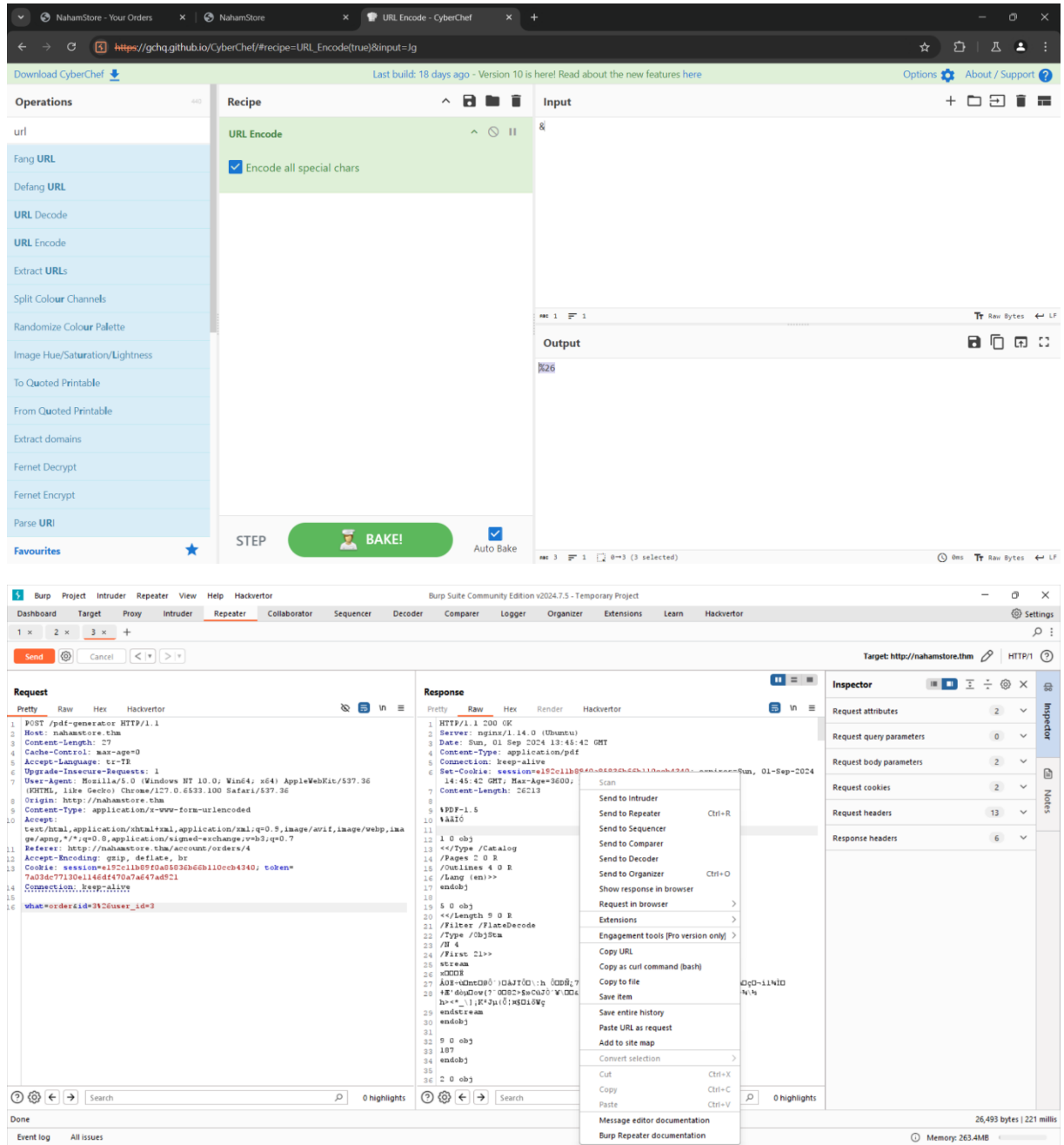
Parametremizi bulduk ve hemen 3 ile değiştirdik ama bize bir hata döndü.



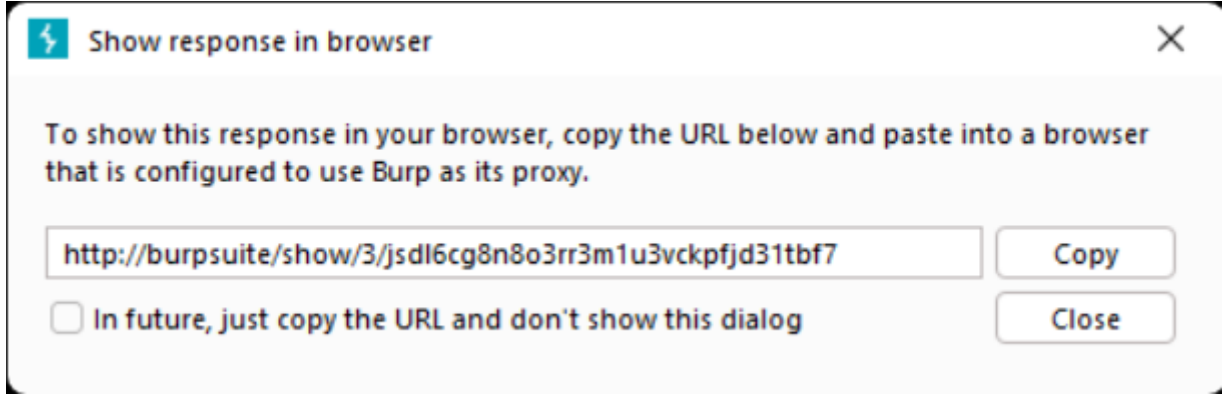
Bunu atlatmak için user_id ekleyip gönderelim.



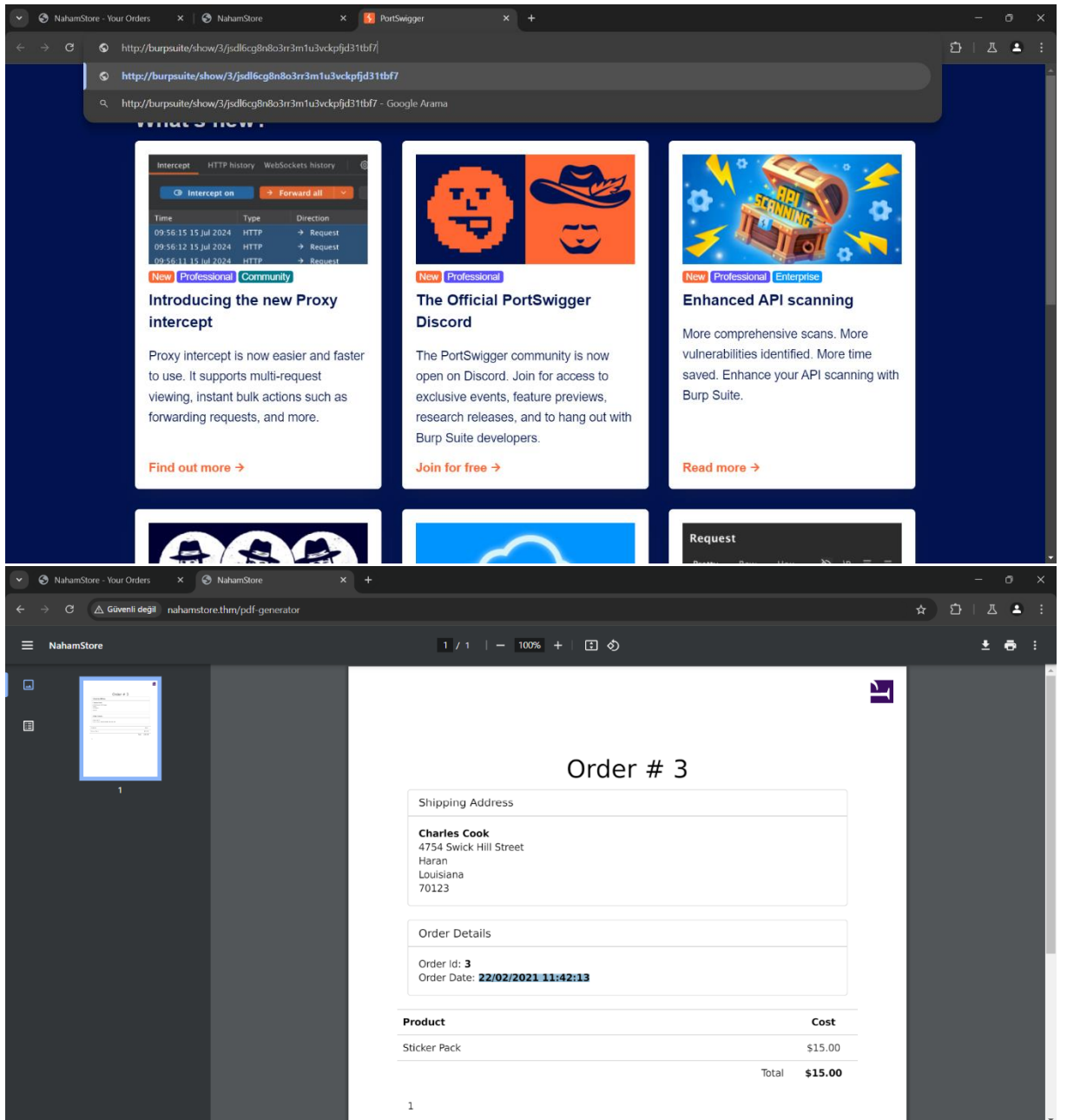
Burda &user_id=3 ekledik parametreye çalışmadı ondan dolayı & işaretini url encode yaptık %26 oldu bunu kullanarak yani son hali "what=order&id=3%26user_id=3" şeklinde oldu ve bunu gönderince sayfamızı açınca tarih karşımıza çıkacak. İlk resim %26 yı nerden bulduğum.



Burdan “show response in browser” seçeneğine tıklıyoruz ve karşımıza aşağıdaki gibi ekran çıkıyor.



Bu linki kopyalayıp tarayıcıdan açıyoruz.



Ve karşımıza bu ekran geliyor ve tarih seçili alanda yazıyor burada bulduk ve idor labını tamamlamış olduk.

The screenshot shows the TryHackMe NahamStore interface. At the top, there's a header with the title "NahamStore v1.2", the target IP address "10.10.1.12", and the expiration time "55min 14s". There are buttons for "?", "Add 1 hour", and "Terminate". Below the header, the main content area displays "Task 7 IDOR" with a green checkmark. The task description states: "In the web application, you'll find two IDOR vulnerabilities that allow you to read other users information." followed by two sub-tasks: "1) An existing user has an address in New York, find the first line of the address." and "2) The date and time of order ID 3". Below the description, it says "Answer the questions below". There are two input fields: "First Line of Address" with the value "160 Broadway" and "Order ID 3 date and time" with the value "22/02/2021 11:42:13". Both fields have a green "Correct Answer" button next to them. At the bottom, there are two more task cards: "Task 8 Local File Inclusion" and "Task 9 SSRF", both with red circles and down arrows. A small green "IDP" icon is visible in the bottom right corner.

Title	Target IP Address	Expires
NahamStore v1.2	10.10.1.12	55min 14s

Task 7 IDOR

In the web application, you'll find two IDOR vulnerabilities that allow you to read other users information.

- 1) An existing user has an address in New York, find the first line of the address.
- 2) The date and time of order ID 3

Answer the questions below

First Line of Address

160 Broadway

✓ Correct Answer

Order ID 3 date and time

22/02/2021 11:42:13

✓ Correct Answer

Task 8 Local File Inclusion

Task 9 SSRF