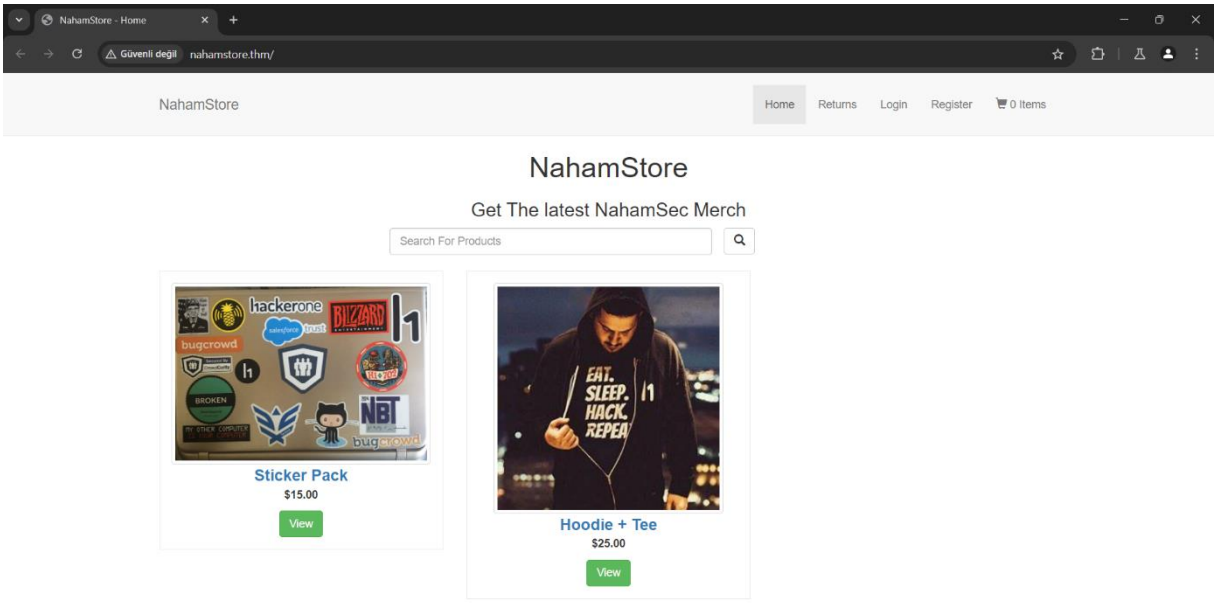
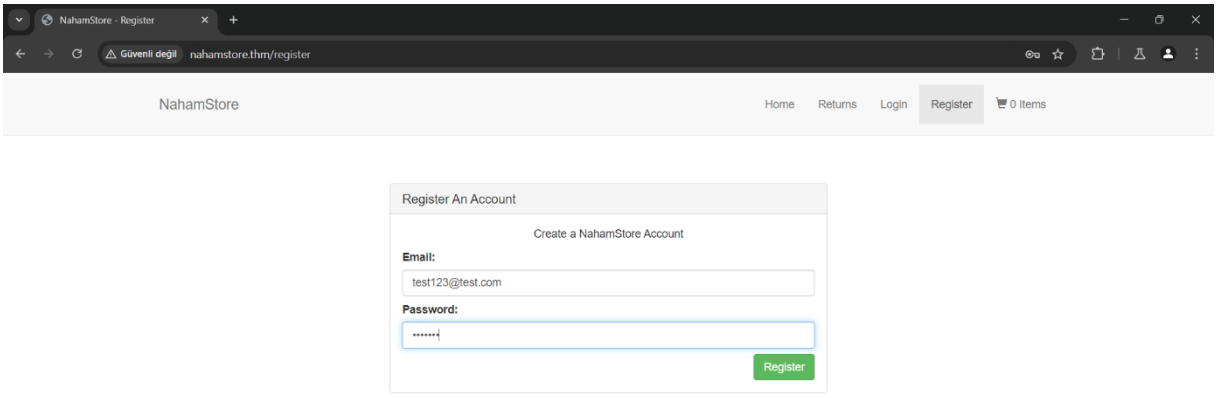
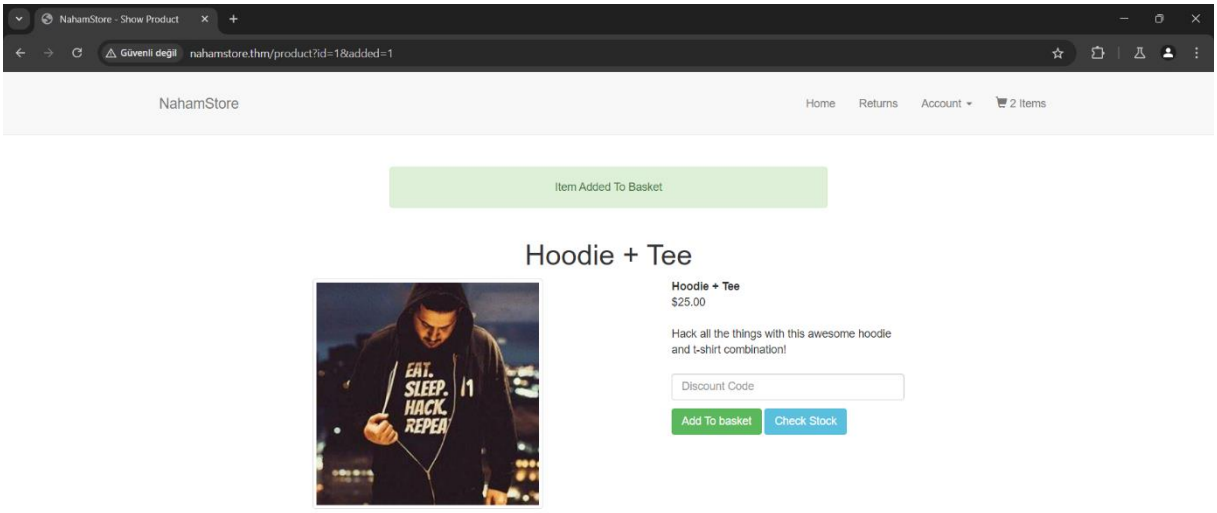
TryHackMe Lab: NahamStore Idor Write-Up

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

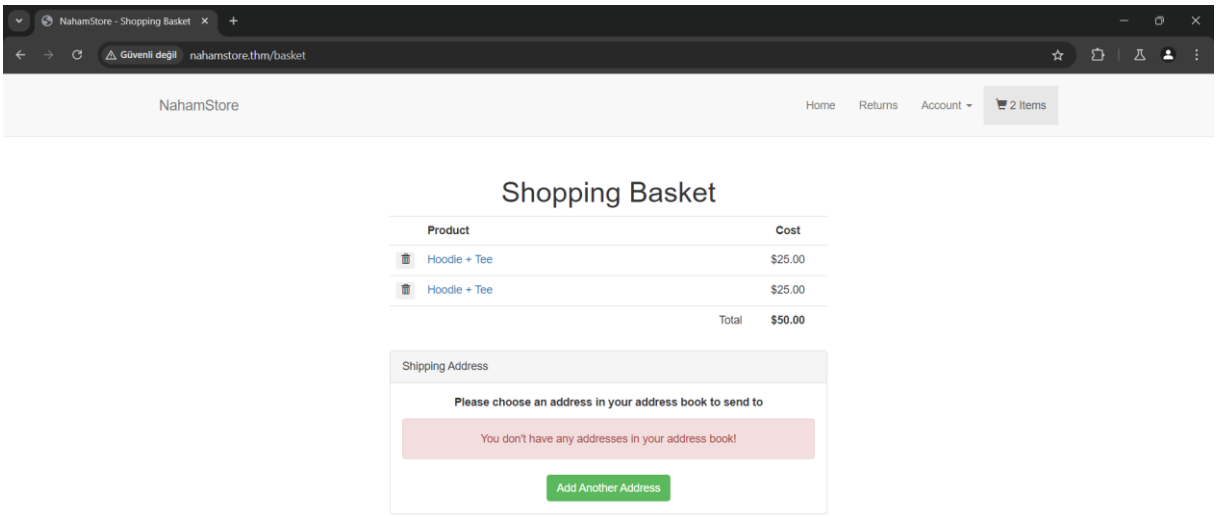




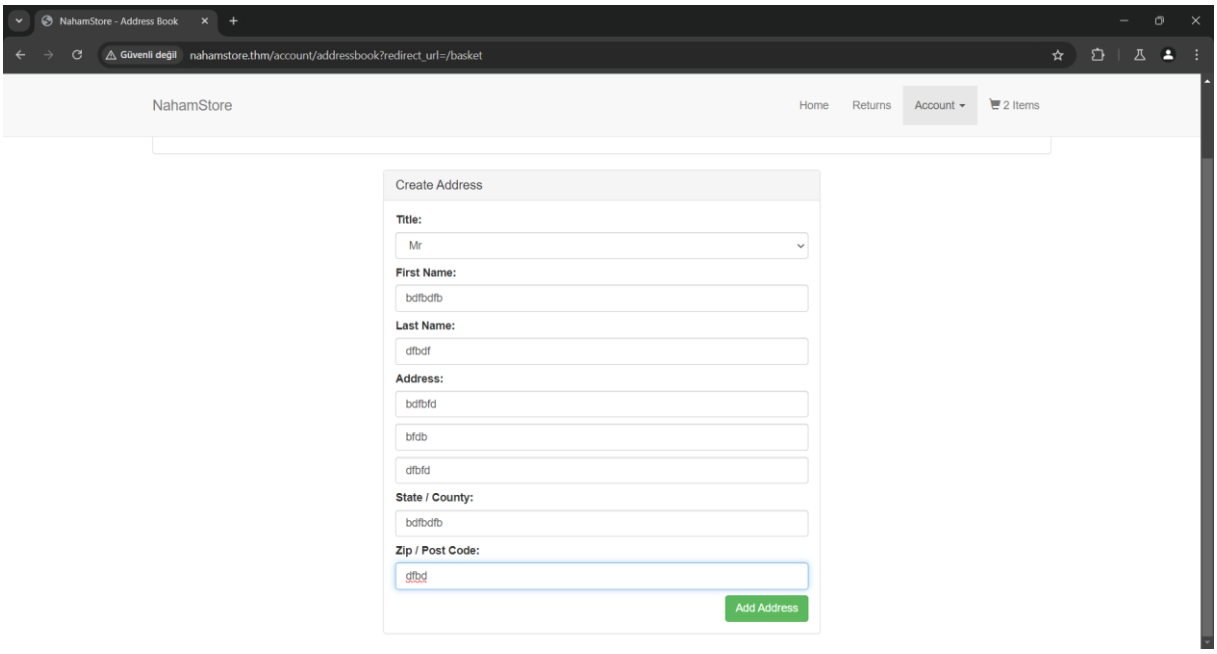
Burda bir hesap oluşturduk ve sitede gezindik bizden istenen 2 soru vardı birincisi new york olan bir adres isteniliyordu ikincisi ise 3. Order id ye sahip siparişin tarih ve saati falan isteniliyor şimdi önce adresle işimiz olduğu için adres girebilcek yer arıyoruz ve aklıma sipariş vermek geliyor 2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



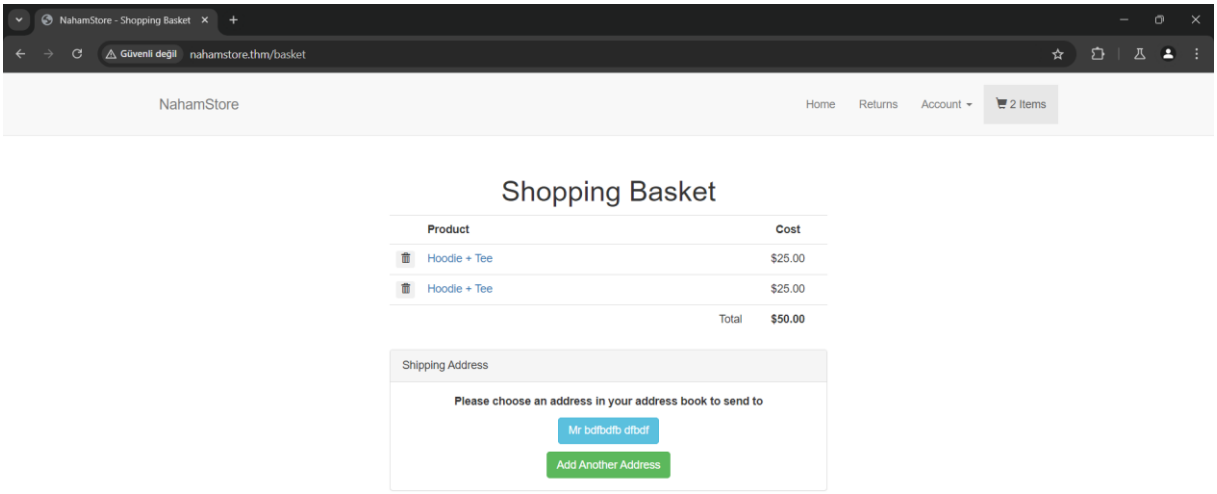
Ekledik şimdi bu ürünlerimize bakalım.



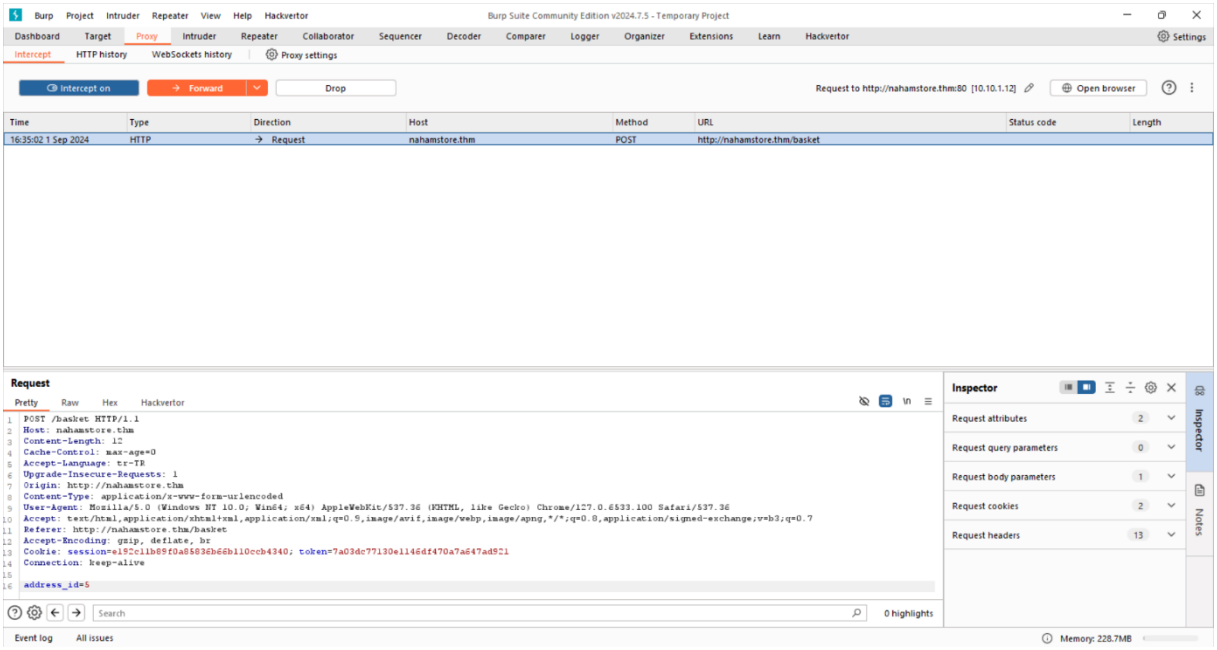
Evet burda adres ekleme yeri bulduk hemen bir tane ekleyelim.



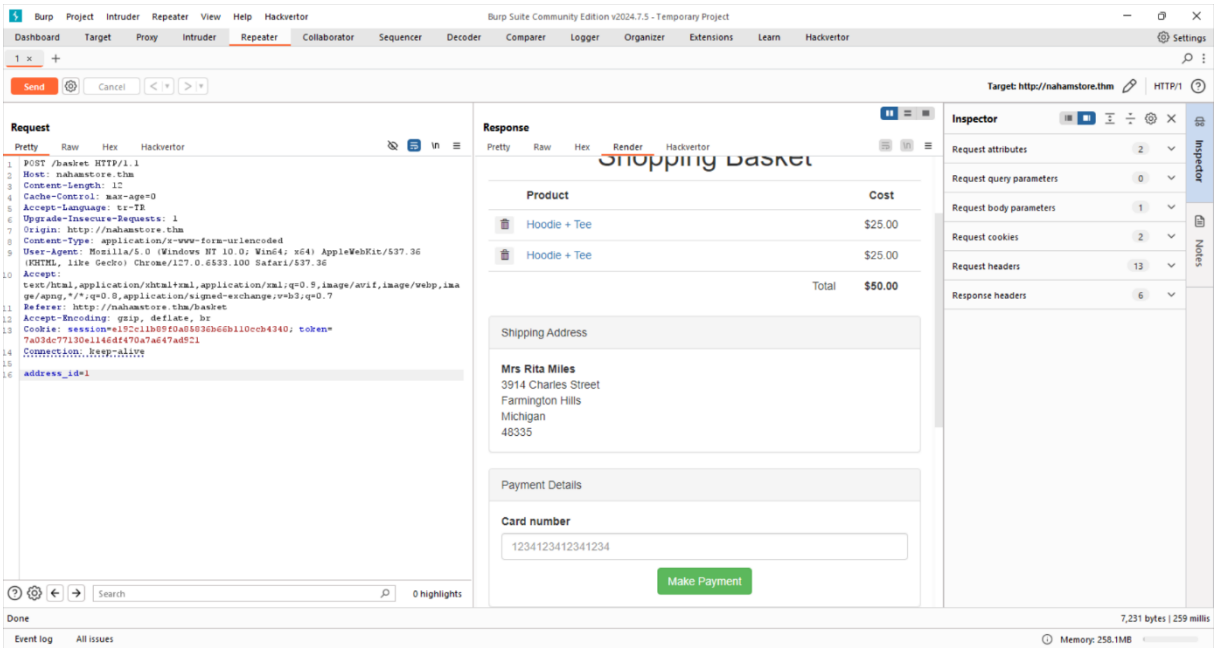
Hemen bir adres ekledik ve bunu kullanalım.



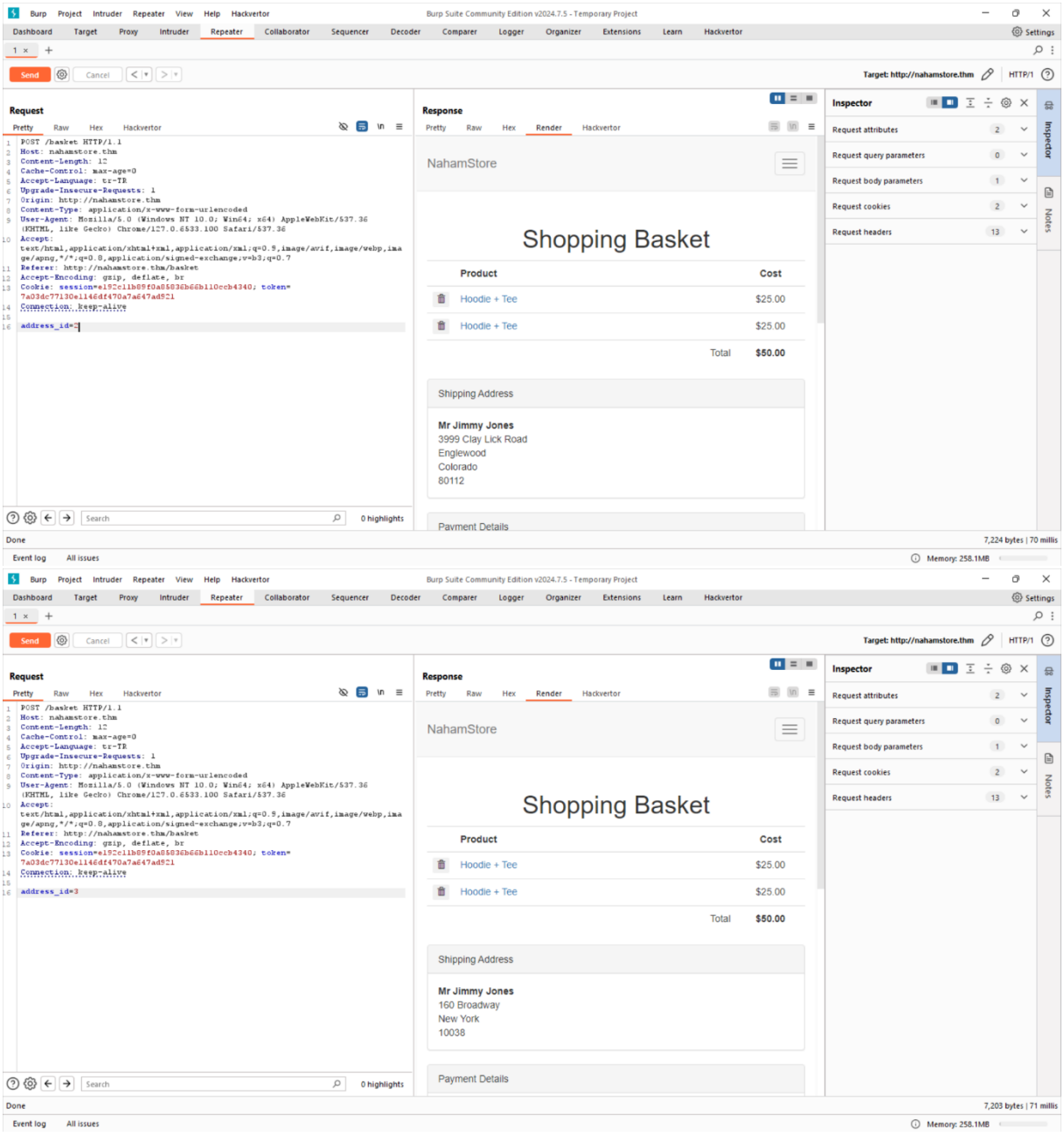
Şimdi burda adres seçerken burp suite ile izleyelim.



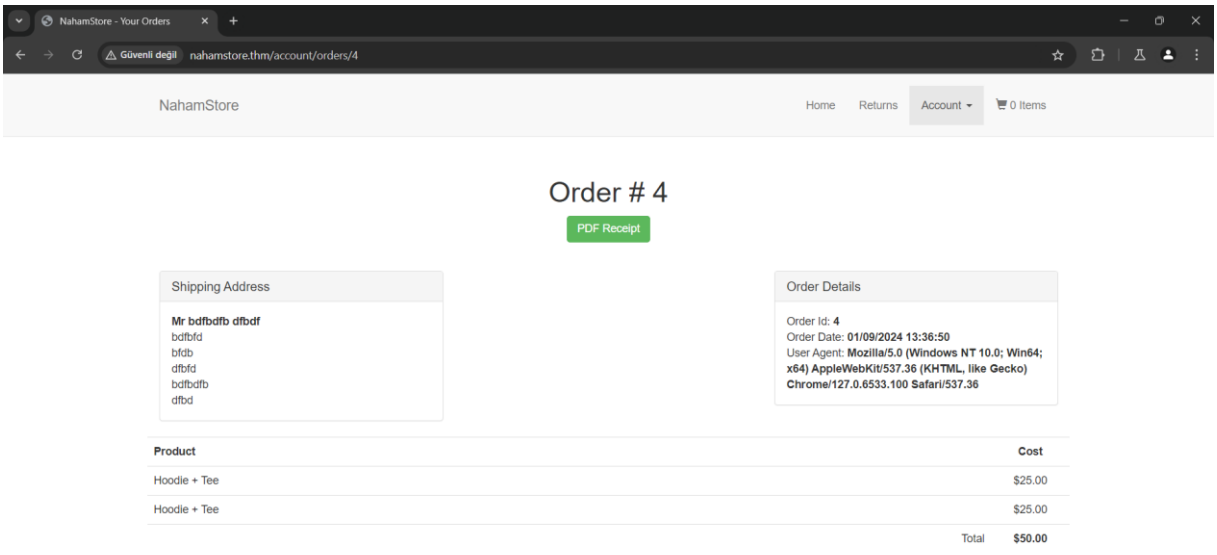
Burda karşımıza adress id parametresi çıktı bunu 1 olarak değiştirip deniyelim.



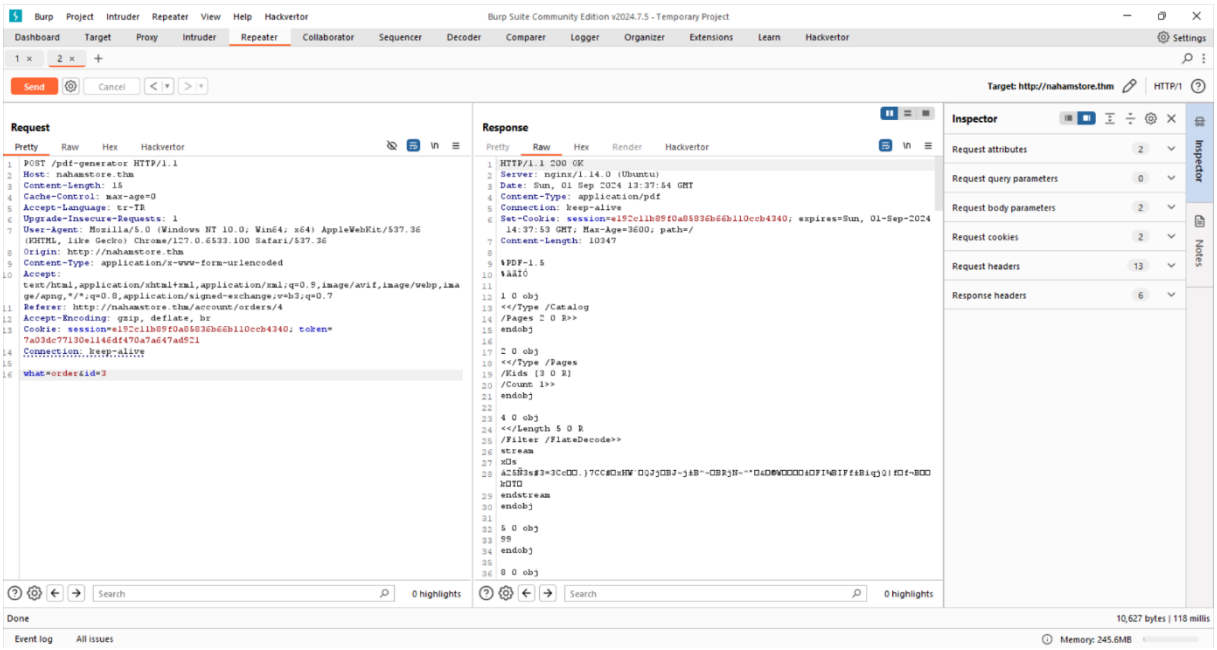
Tek tek biraz böyle bakalım arayalım new york daki adresi.



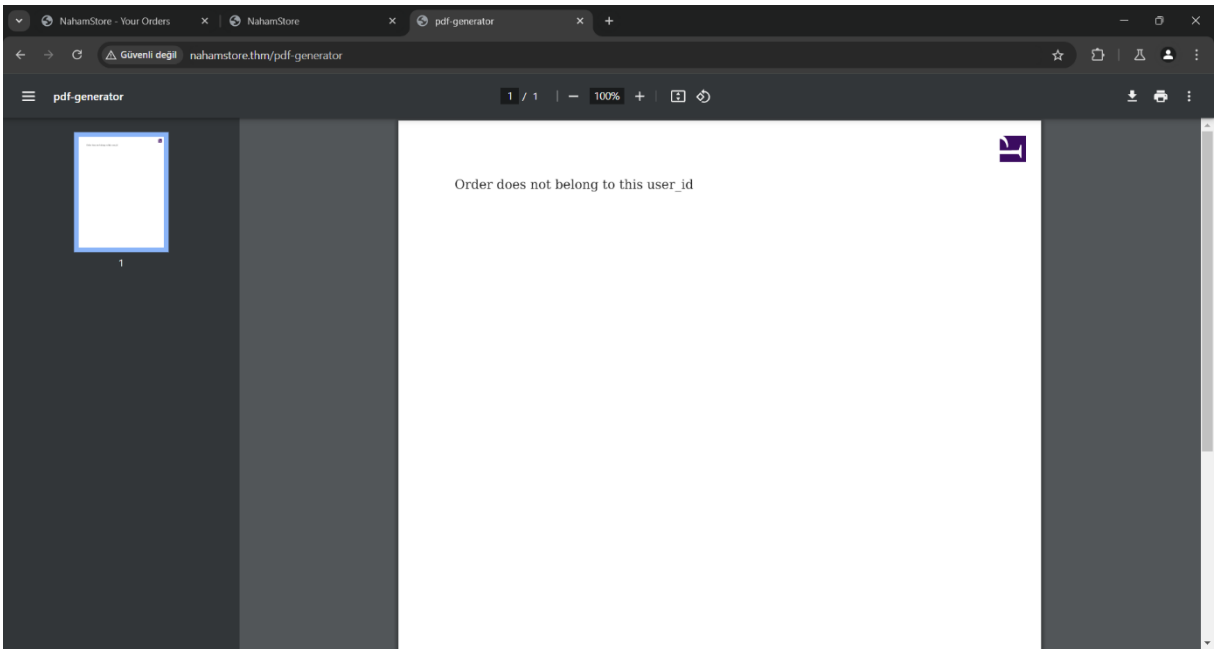
Ve id=3 te bulduk ilk satırı isteniliyordu bizden 160 Broadway olucak cevap.Şimdi ikinci kısmı bulmaya çalışalım ikinci kısımda bizden tarih saat falan isteniliyordu bunu bulmak için şipariş verelim bi tane.



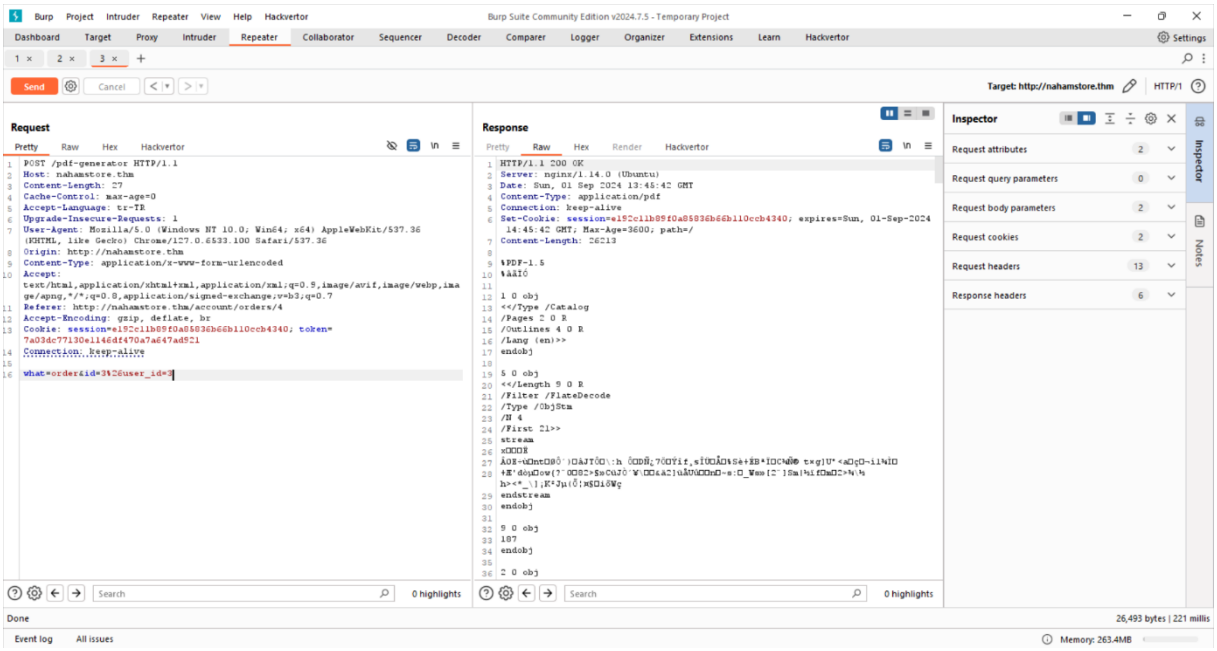
Burda siparişi oluşturduk ve tarih falan çıktı ama burda bir şey bulamadık değiştirebileceğimiz o yüzden pdf tuşuna basıp izliyoruz.



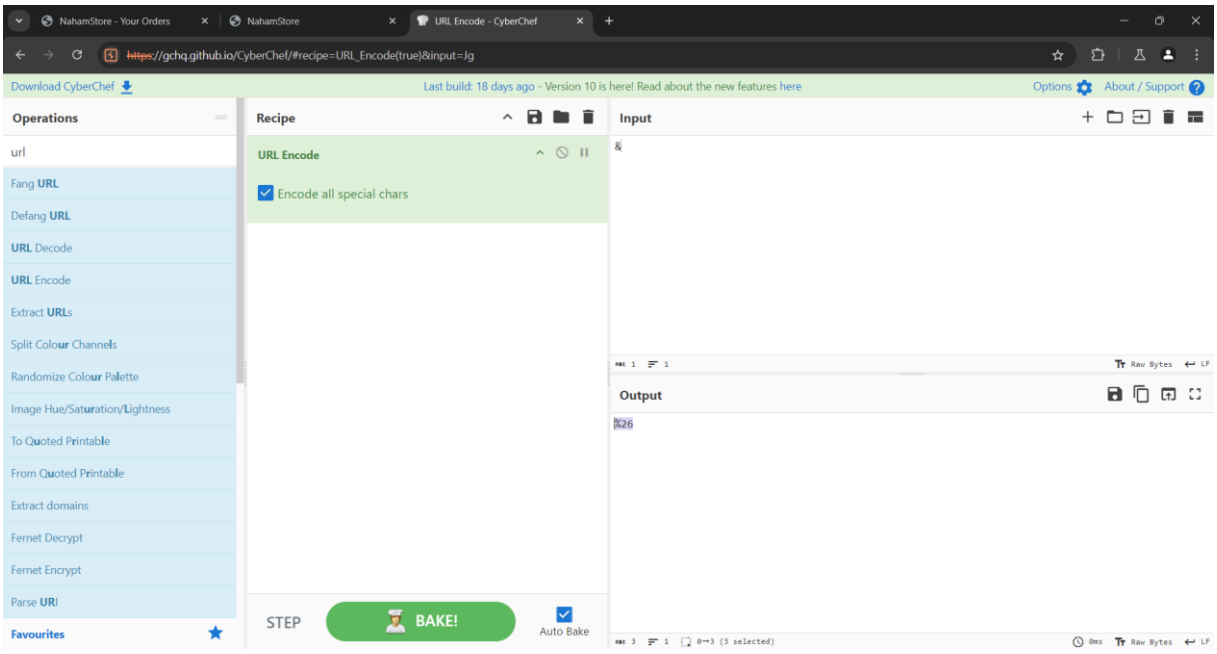
Parametremizi bulduk ve hemen 3 ile değiştirdik ama bize bir hata döndü.

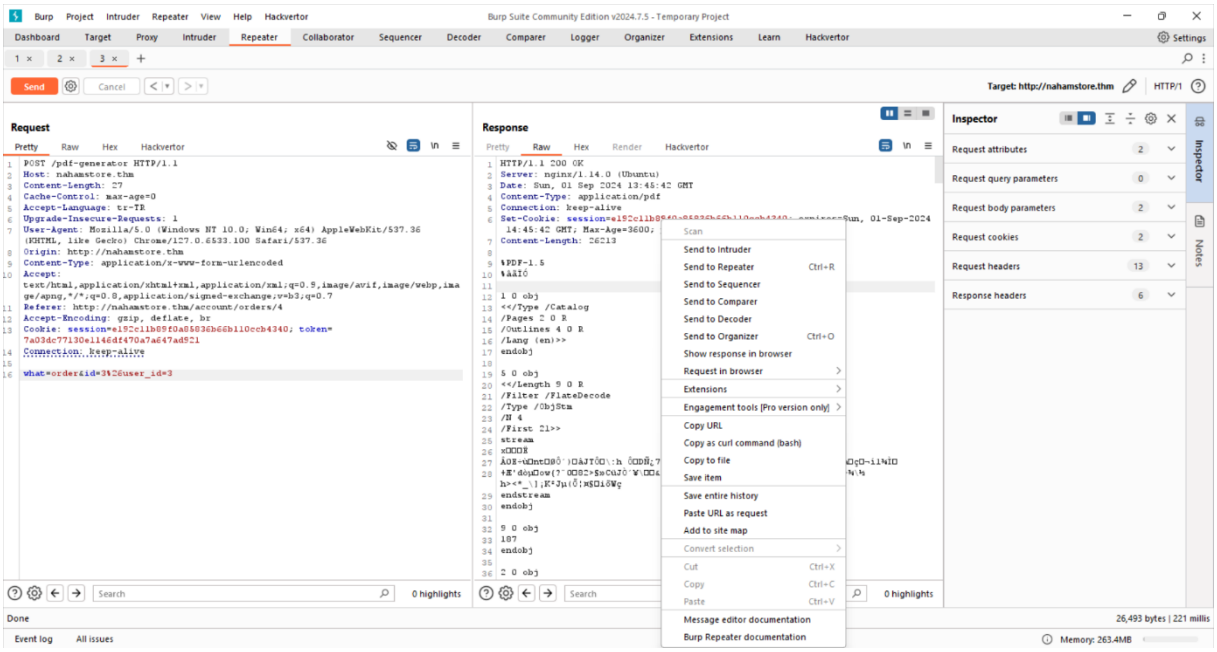


Bunu atlatmak için user_id ekleyip gönderelim.



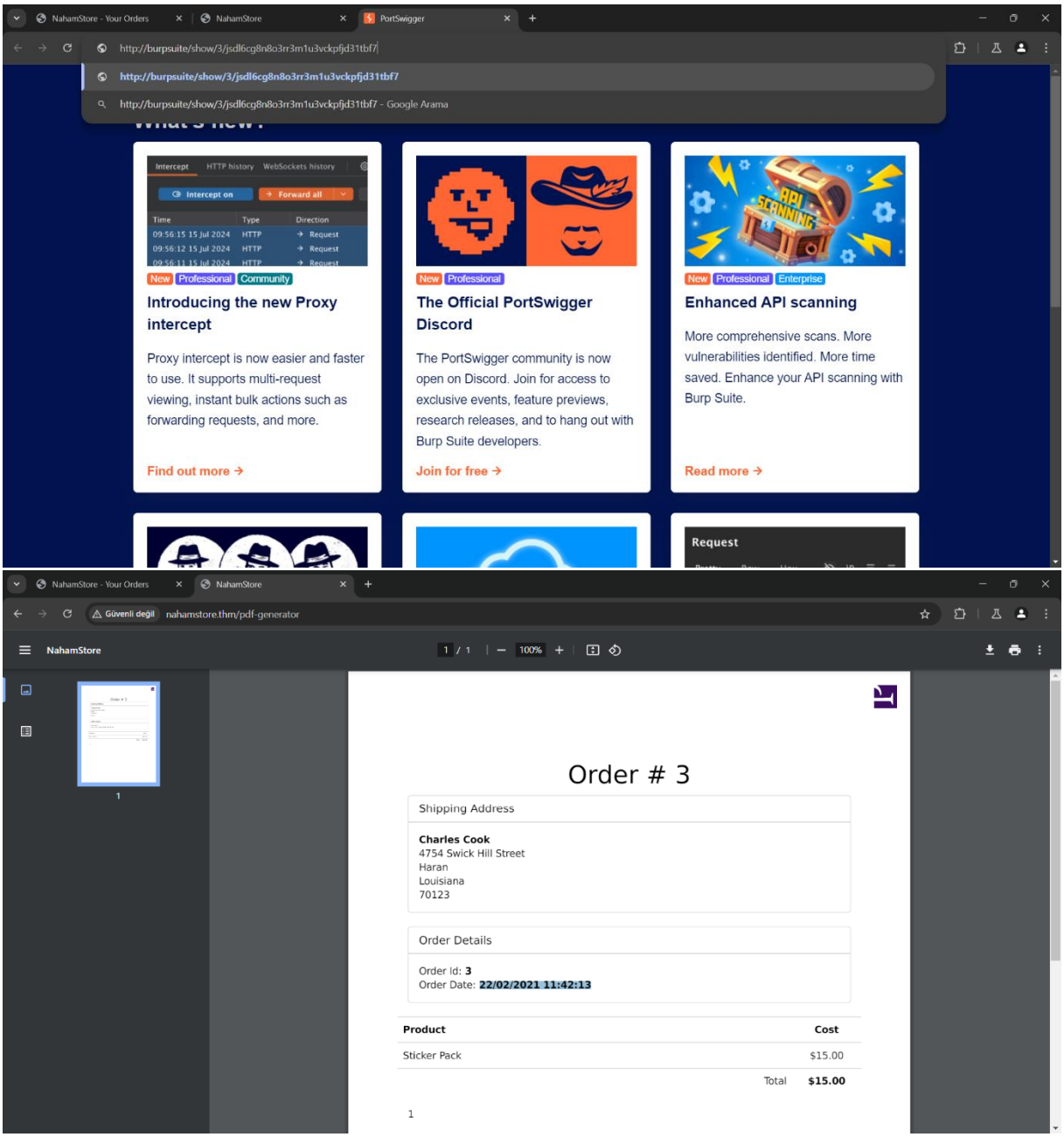
Burda &user_id=3 ekledik parametreye çalışmadı ondan dolayı & işaretini url encode yaptık %26 oldu bunu kullanarak yani son hali ” what=order&id=3%26user_id=3 “ şeklinde oldu ve bunu gönderince sayfamızı açınca tarih karşımıza çıkacak.İlk resim %26 yı nerden bulduğum.





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 bunuda bulduk ve idor labını tamamlamış olduk.