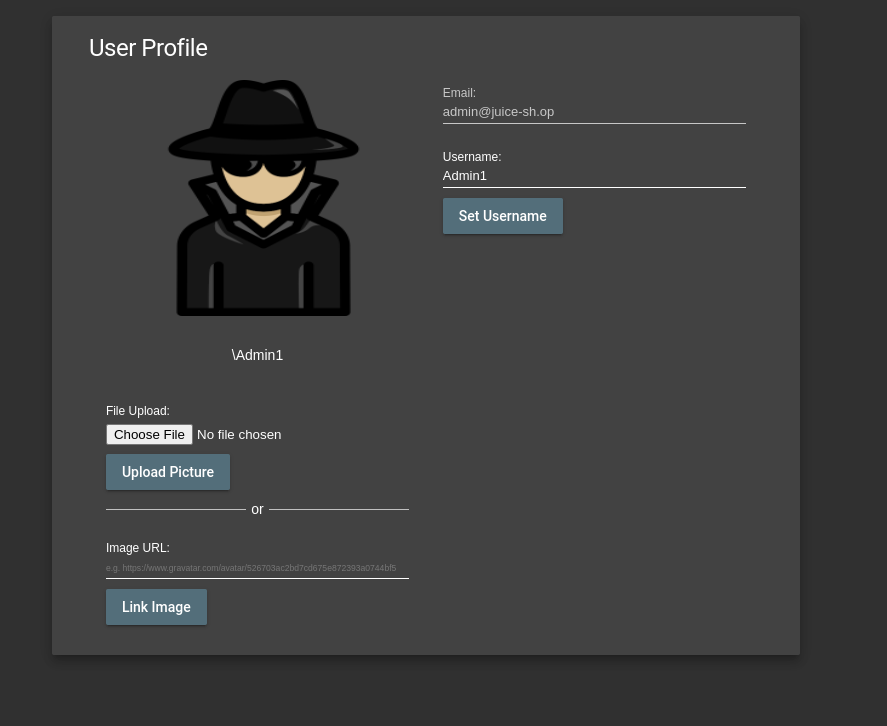
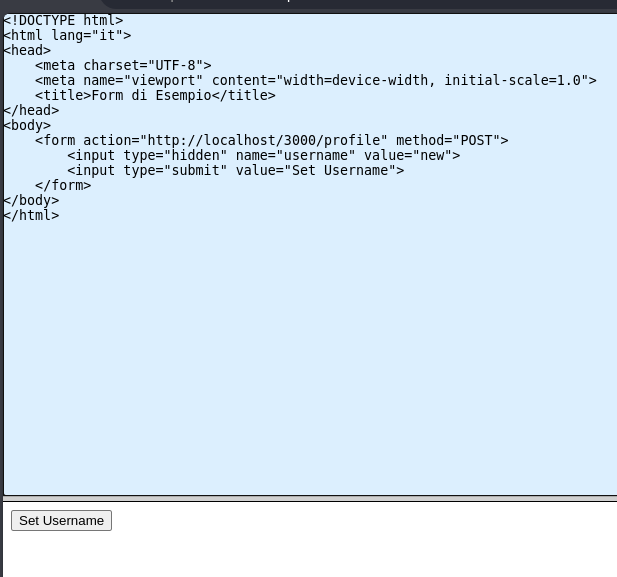
**Broken Access Control**

**CSRF Token (Non funziona su Docker):**

È presente una problematica relativa al cambio dell'username utente, se ci rechiamo nella pagina di utente (/profile) ci si aprirà questa pagina:



Qui c’è la possibilità di cambiare l’username dell’utente, ma non è presente un CSRF Token che controlla se la richiesta viene da una fonte, o utente, legittima. Quindi è possibile cambiare l’username anche da una fonte esterna, rechiamoci sul sito <https://htmledit.squarefree.com/> che ci permette di creare qualsiasi cosa usando html, l’idea è di creare la form e fare il submit da questa fonte in modo che possiamo cambiare l’username:

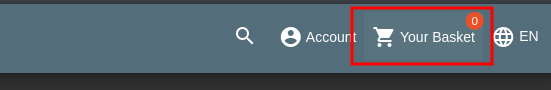


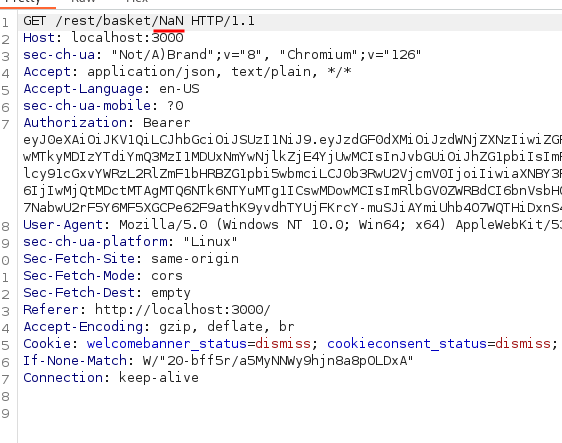
Ora proviamo se funziona cliccando sul button per fare il submit:

(in aggiornamento, funziona solo utilizzando una versione vecchia di firefox 81.0 che sto cercando di recuperare)

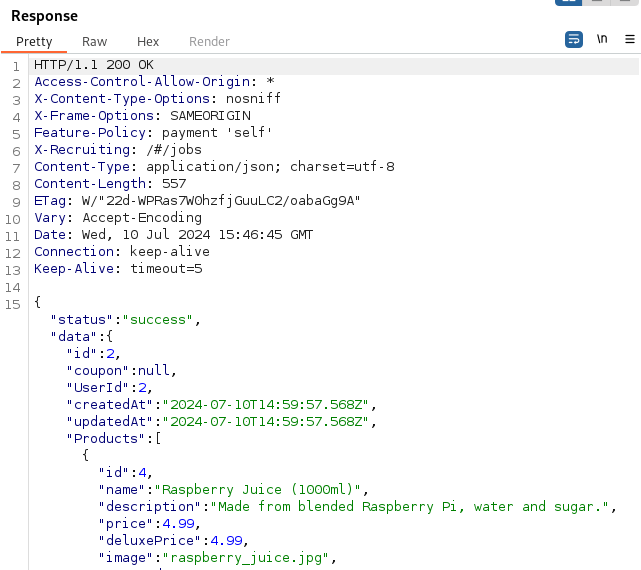
**Basket di altri utenti:**

E’ possibile vedere il carrello degli altri utenti, per farlo possiamo utilizzare burp e intercettare la richiesta. Attiviamolo e clicchiamo su “Baskets” o se si è loggati “Your Basket”:

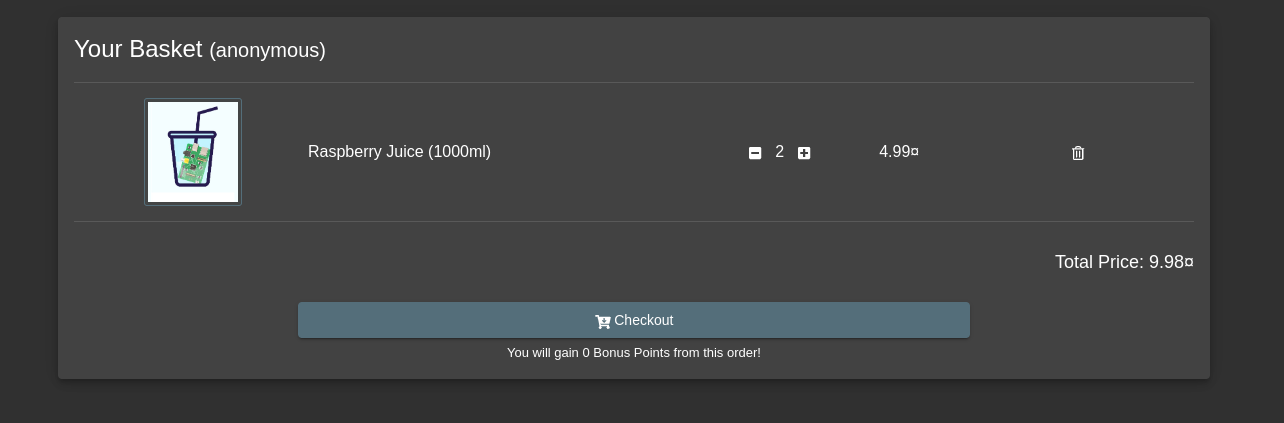


Rechiamoci su burp e vediamo come è strutturata la richiesta:  
  


Vediamo che nella richiesta viene passato un parametro, nel mio caso è NaN (not a number) quindi decido di mandare la richiesta al repeater e cambiarla mettendo un numero diverso:  

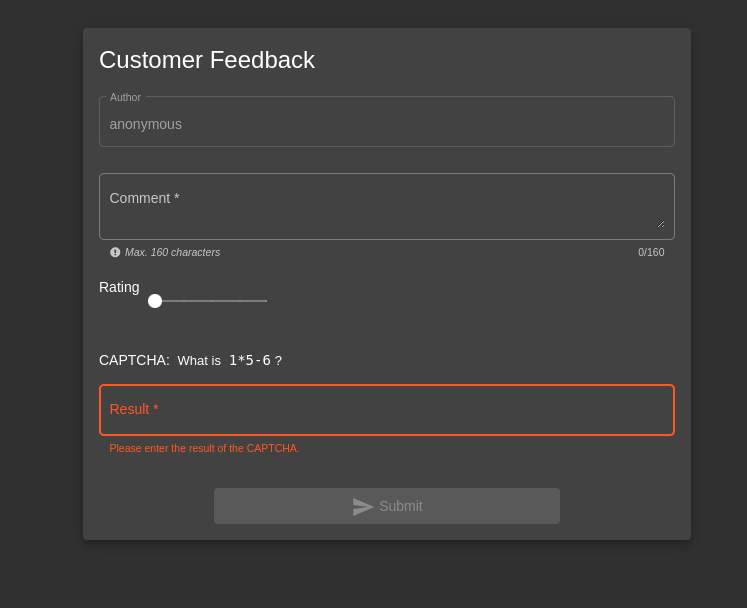

E ricevo questa risposta:  
  


A quanto pare sono riuscito a vedere il carrello dell’utente 2. Mando la richiesta di burp al browser e vediamo la visualizzazione della pagina html:

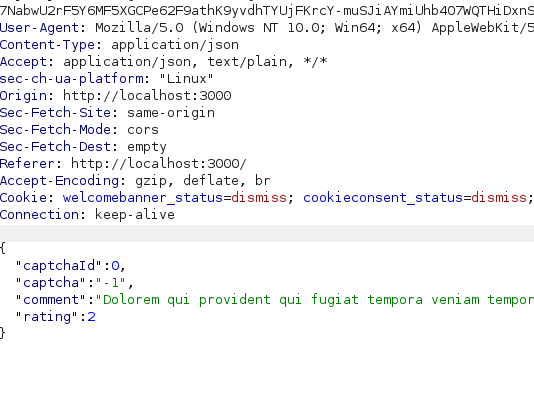


**Feedback spacciandosi per un altro utente:**

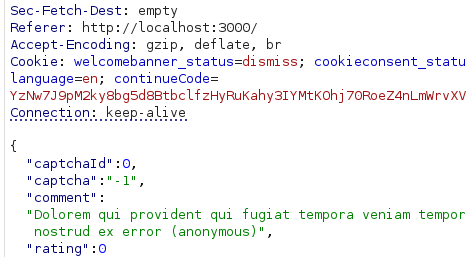
Nella pagina “/contact” è possibile lasciare un feedback:



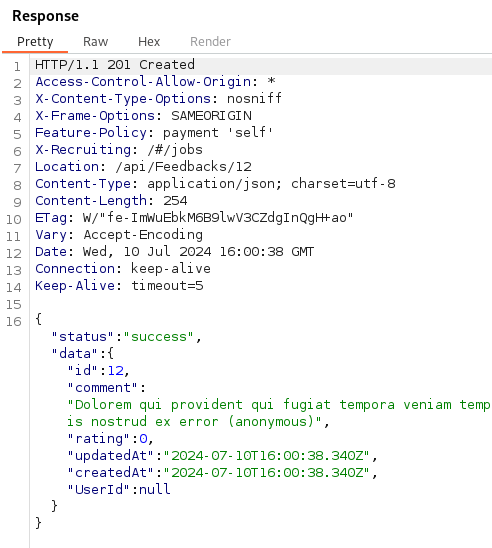
Da interfaccia non è possibile scrivere l’autore e neanche inserire il rating a 0, allora provo a intercettare la richiesta con burp:



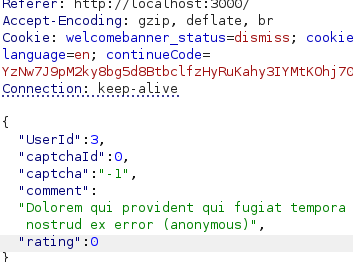
Posso cambiare il rating, ma non l’utente che inserisce il feedback. Mando quindi la richiesta al repeater e provo a inviarla mettendo un rating di 0:

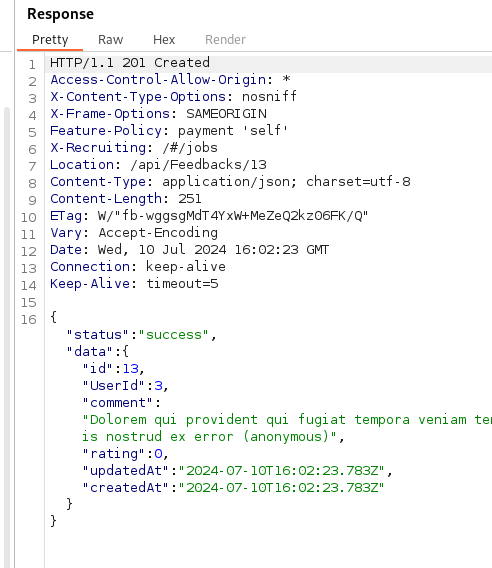


E questa è la risposta:

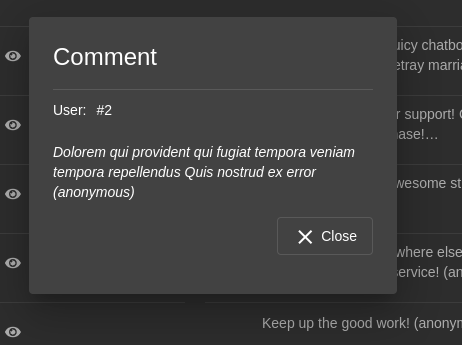


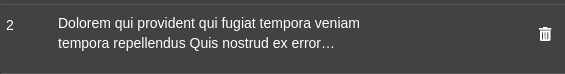
Vedo nella risposta un ***UserId*** impostato a null, provo a cambiare la richiesta nuovamente aggiungendo il campo inserendo un id diverso:



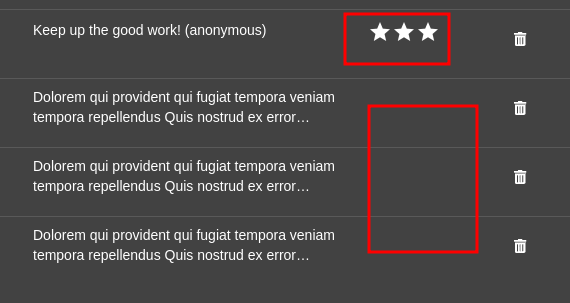


Mi dice che la richiesta è andata a buon fine e sembra che sia cambiato anche lo UserId visto che prima era a null e adesso a 3, andiamo a vedere se la vediamo nella pagina, per vedere il feedback ci dobbiamo recare alla pagina /administration:



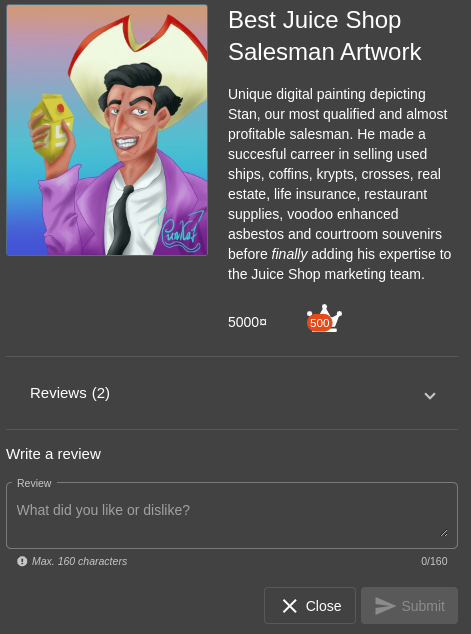


A quanto pare per la logica dell’applicazione l’id che abbiamo messo (3) in realtà si riferisce all’utente 2 ma comunque siamo riusciti da utenti estranei a inserire un feedback spacciandoci per un utente qualsiasi e siamo riusciti anche a inserire il feedback con 0 stelle anche se dall’interfaccia web non era possibile.



**Recensioni di prodotti spacciandosi per altri utenti:**

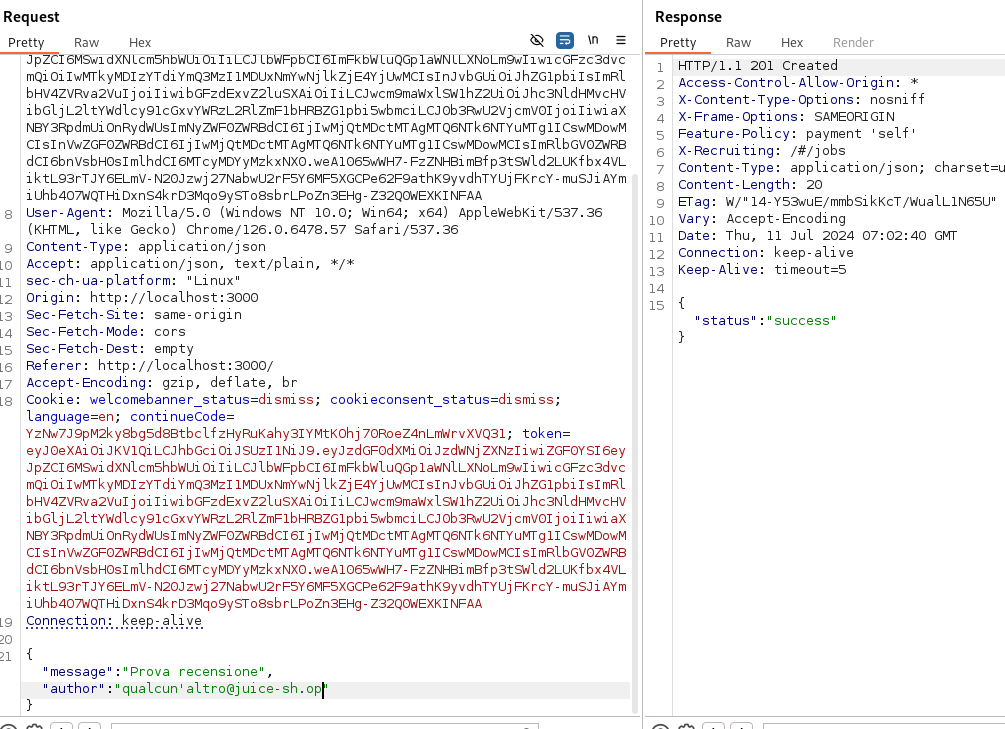
È possibile scrivere recensioni spacciandosi per altri utenti, apriamo un prodotto qualsiasi e vedremo che possiamo scrivere una recensione:



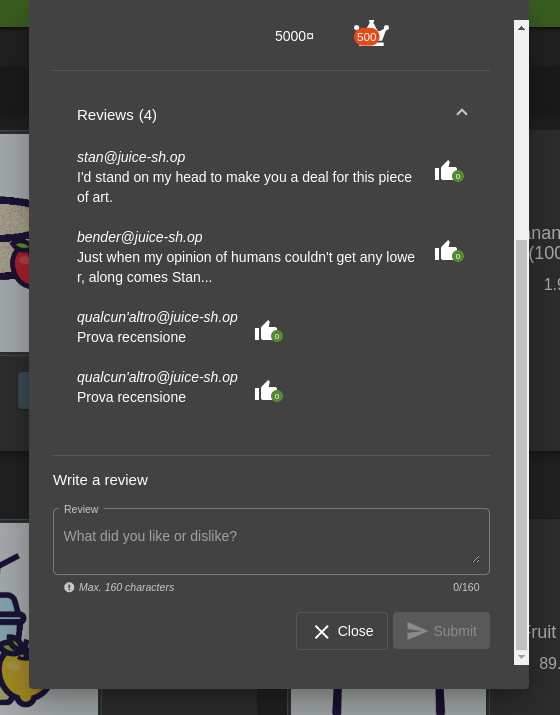
Scriviamo qualcosa e utilizziamo burp per intercettare la richiesta:



Ecco la richiesta, per capire come scriverla come altri utenti la mando al repeater e faccio varie prove:



Sembra che sia andata a buon fine, ora la provo a inviare veramente e vediamo il risultato:



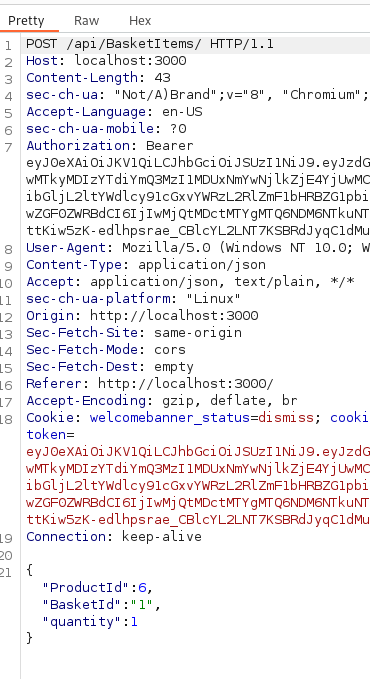
Ed è andata correttamente.

**Aggiungere prodotti ai carrelli di altri utenti:**

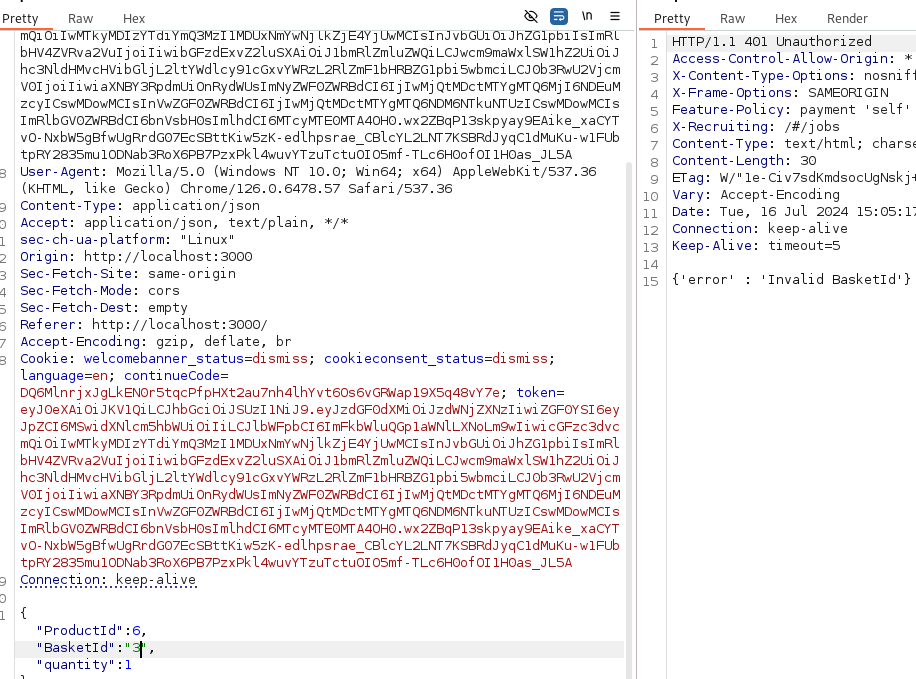
È possibile aggiungere prodotti a carrelli di altri utenti utilizzando un utente differente da quello che ha il carrello, per prima cosa per capire come fare controllo come funziona l’aggiunta del prodotto al basket:



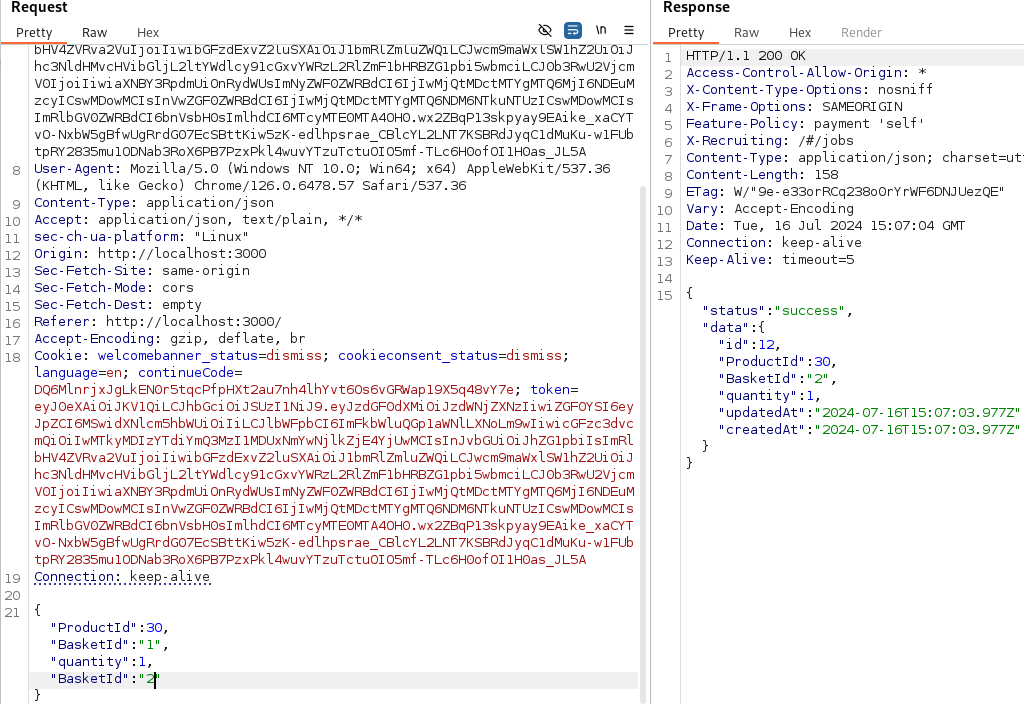
Viene richiamato prima il carrello (1 che è quello dell’utente admin che sto usando) e successivamente viene aggiunto



Questa è la richiesta che si occupa di aggiungere il prodotto al basket indicato, cambiamo quindi il basketId e mandiamo la richiesta a buon fine:



Mi dice che è sbagliato l’id del basket, allora dopo svariati tentativi ho provato questo:



Aggiungendo 2 volte il campo basketId e cambiandone il valore è possibile quindi aggiungere prodotti ad un basket di un’altro utente.