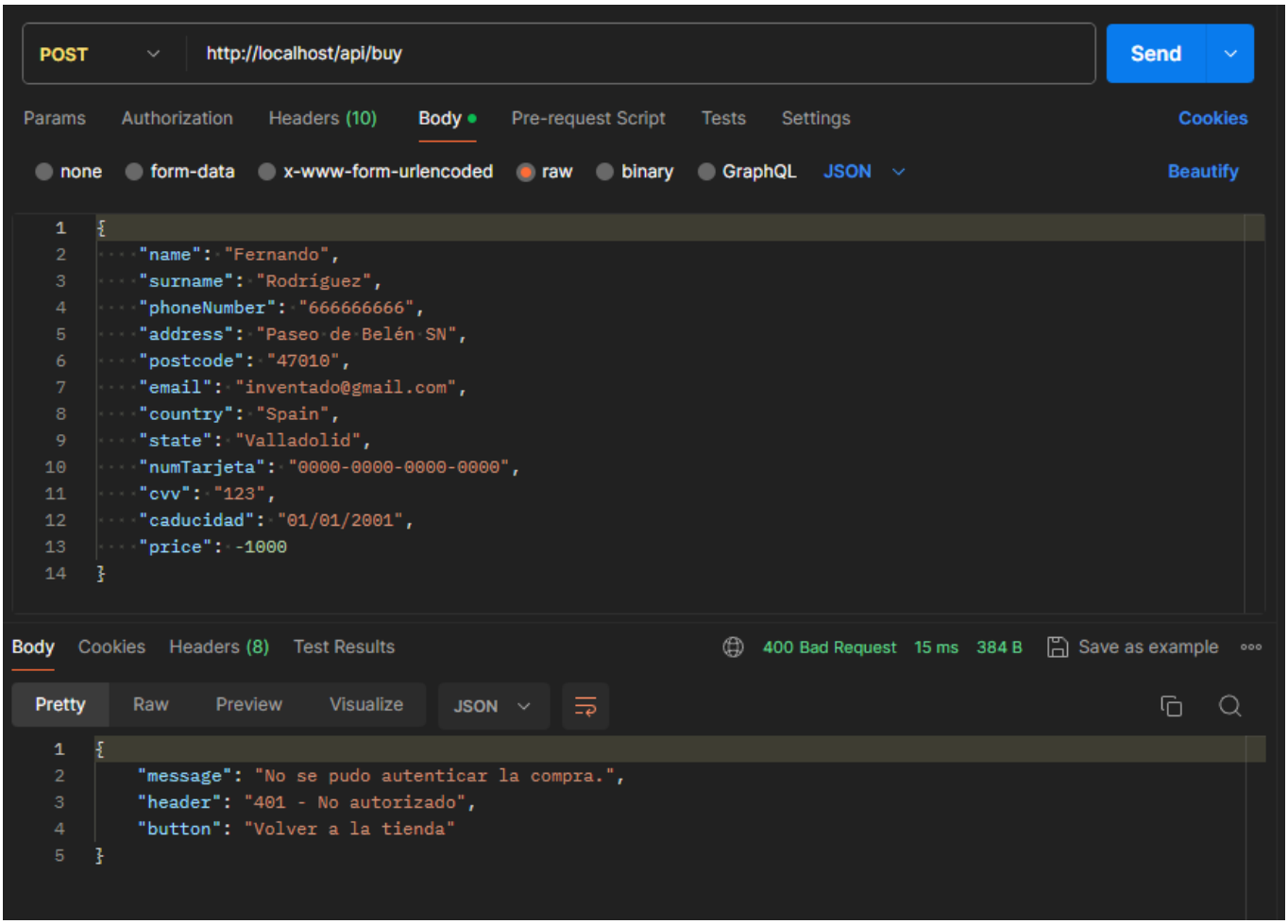
Writeup - ¡Hazte millonario!

Este reto consiste en conseguir que una compra te salga con saldo negativo. Para este reto, utilizaremos `Postman`, aunque se puede hacer con `cURL` o cualquier otro programa que permita realizar peticiones HTTP.

Si miramos la pestaña `Red` de las opciones de desarrollador, podemos ver como lo que se envía al `endpoint` es un JSON que contiene un campo llamado `price`:

Por tanto, para hacernos millonarios, hemos de conseguir que este `price` sea negativo. Para ello, podemos intentar modificar el precio usando `Postman`:

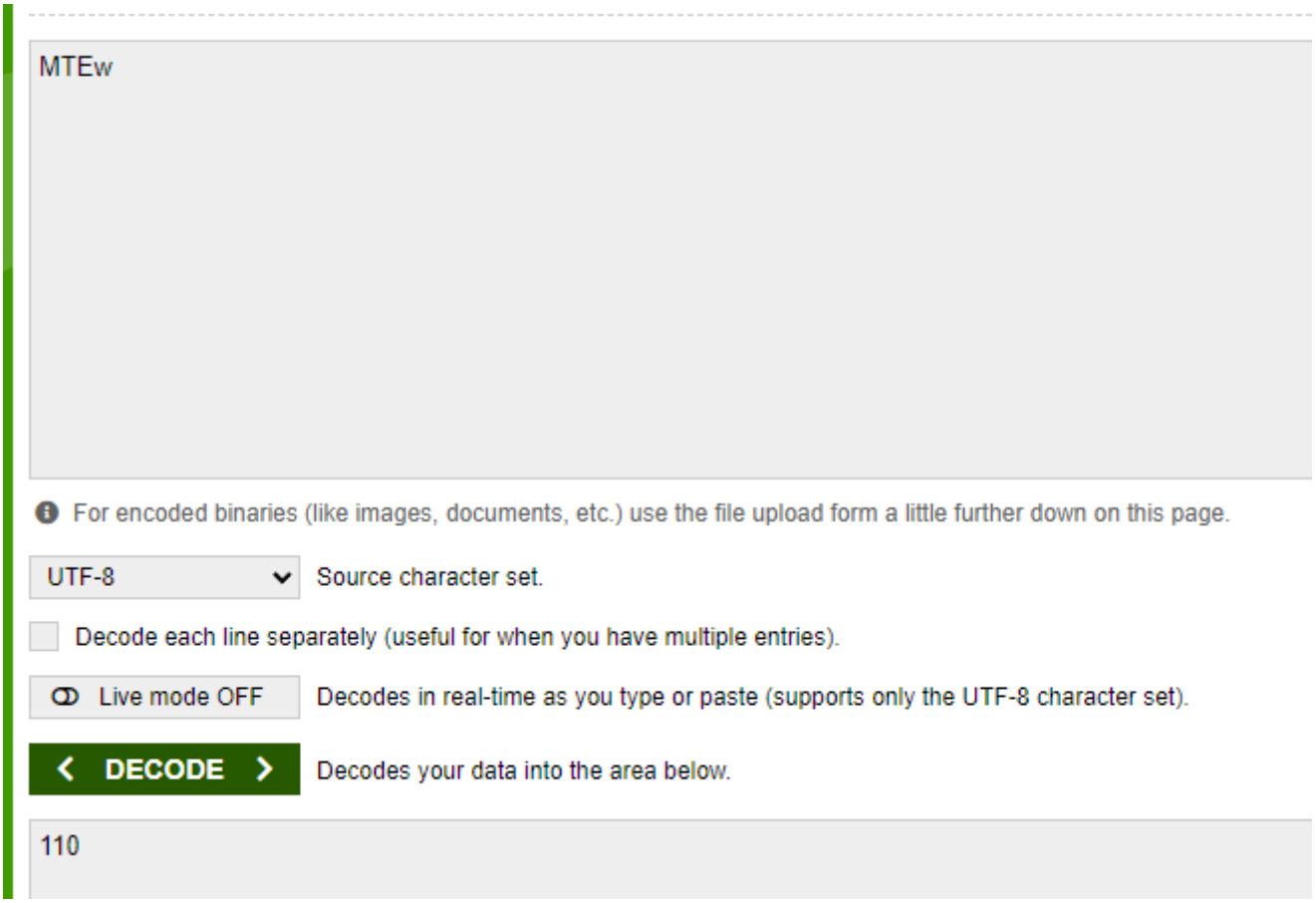


Sin embargo, el servidor nos devuelve un código `401`, lo que quiere decir que no estamos autorizados para realizar dicha compra. Aquí, si nos fijamos en el encabezado de la petición que hicimos desde el navegador:

Vemos que existe una Cookie llamada `transAuth`. Debido a que el error `401` indica que no estamos autorizados, igual la cookie de `transAuth` indica si estamos autorizados a realizar la compra.

Ahora, he realizado una compra de 110€, y he visto que la Cookie ha cambiado. Sin embargo, si hago una compra del mismo precio, el valor de la Cookie se mantiene, por tanto, podemos suponer que el valor de la Cookie varía en función del precio.

Si probamos a decodificar la Cookie de `Base64` (*típicamente las Cookies están codificadas de esta forma*), podemos ver que el valor de la Cookie se corresponde con el precio total de la compra:



Por tanto, si queremos hacernos millonarios, simplemente codificamos `-1000000` en `Base64` y lo añadimos como Cookie a la petición:

Encode to Base64 format

Simply enter your data then push the encode button.

-1000000

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Destination character set.

LF (Unix) Destination newline separator.

Encode each line separately (useful for when you have multiple entries).

Split lines into 76 character wide chunks (useful for MIME).

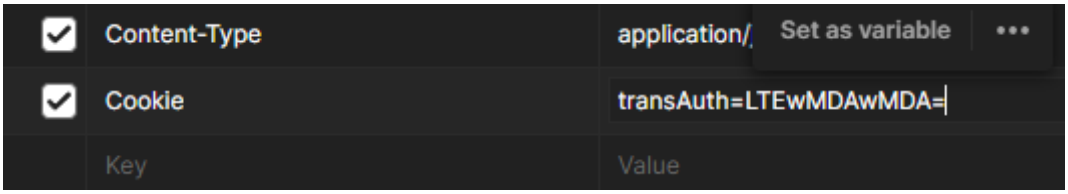
Perform URL-safe encoding (uses Base64URL format).

Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

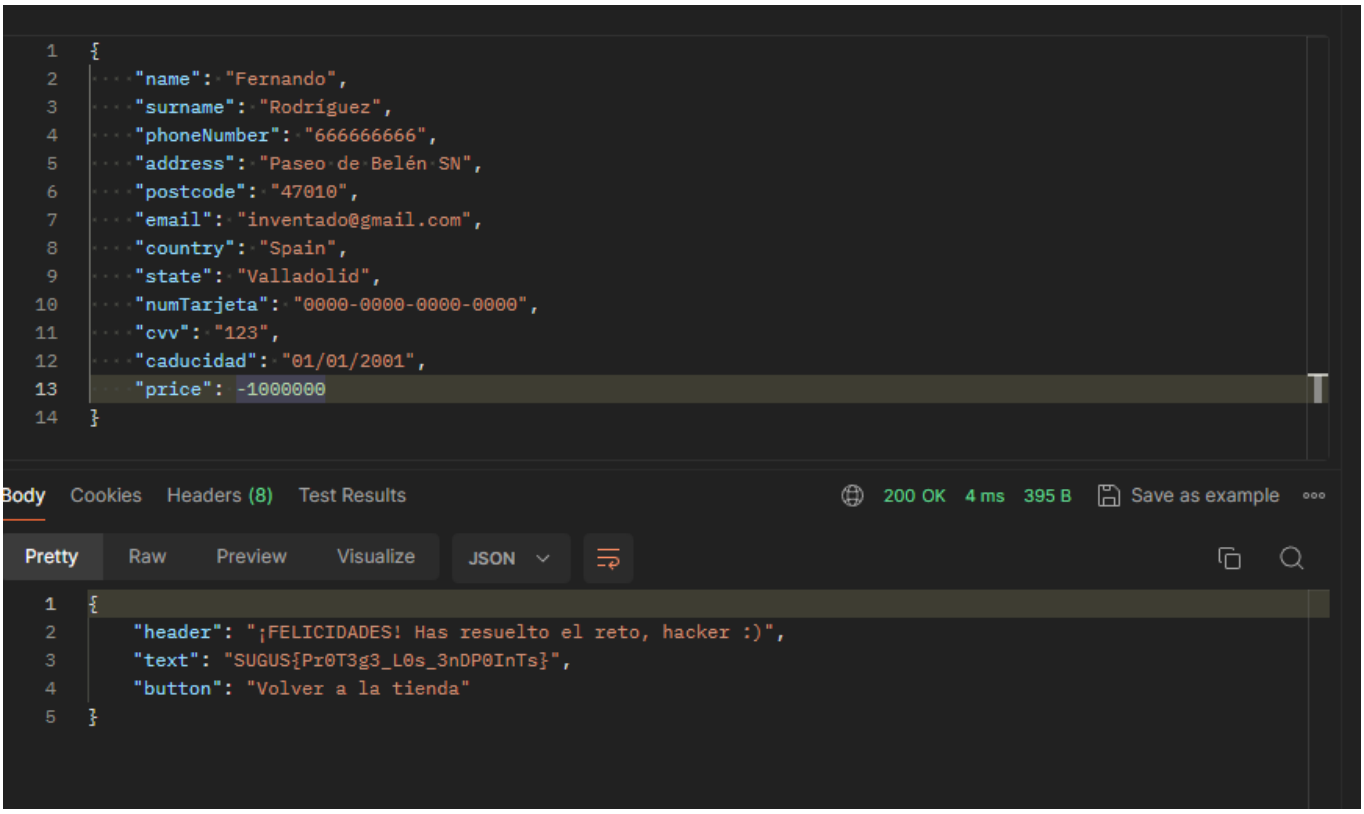
ENCODE Encodes your data into the area below.

LTEwMDAwMDA=

En `Postman`, añadimos la Cookie a la cabecera de la petición HTTP:



Una vez hecho esto, ¡ya somos millonarios!


{
"name": "Fernando",
"surname": "Rodríguez",
"phoneNumber": "666666666",
"address": "Paseo de Belén SN",
"postcode": "47010",
"email": "inventado@gmail.com",
"country": "Spain",
"state": "Valladolid",
"numTarjeta": "0000-0000-0000-0000",
"cvv": "123",
"caducidad": "01/01/2001",
"price": -1000000
}
Body
Cookies
Headers (8)
Test Results
200 OK
4 ms
395 B
Save as example
Pretty
Raw
Preview
Visualize
JSON
{
"header": "¡FELICIDADES! Has resuelto el reto, hacker :)",
"text": "SUGUS{Pr0T3g3_L0s_3nDP0InTs}",
"button": "Volver a la tienda"
}