From: **Richie Prieto** richie.nprieto@gmail.com
Subject: Broken Access Control - IDOR
Date: 15 July 2022, 11:13
To: florencia.presta.87@gmail.com

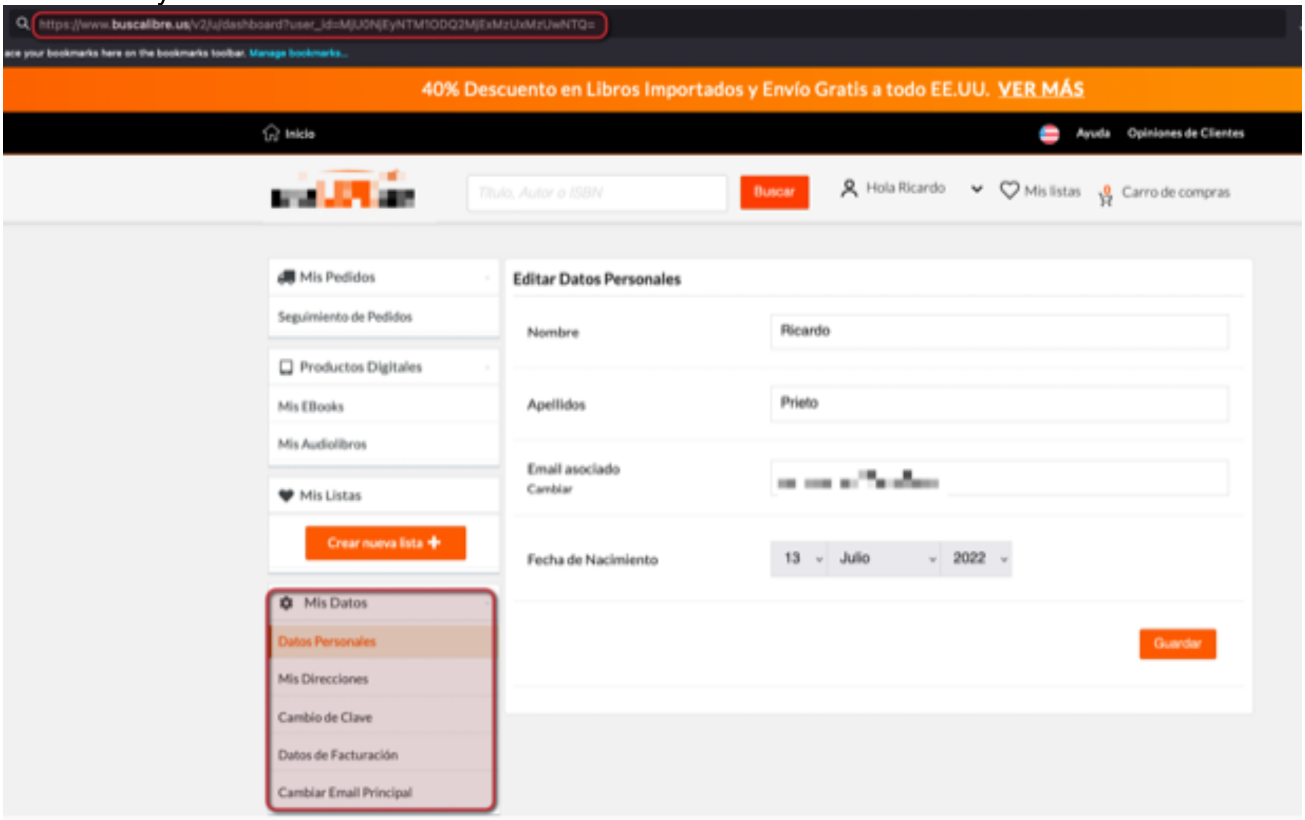
Hello Micaela, my name is Ricardo Prieto and I'm an Information Security professional and client of your company as well. I write to you directly because is the only email I found of your department.
Basically, while using your site to buy a book, I came across with something unexpected. I found a vulnerability in your shopping web application that allows me to switch to other customer's carts by changing my user ID in the URL (I noticed it's base64 encoded).

The most critical thing about this, is actually that I was also able to access other clients private information by applying a exploiting a regular IDOR + decode/encoding. This make me very concern about all the private information that can be easily disclosed, so I'm really interested in help you and your tech team, to solve this issue as soon as possible.

Some information that I was able to access:

- First name
- Last name
- Address
- Email
- Cell phone number™
- Latest purchases

I'll let you some screenshots below:

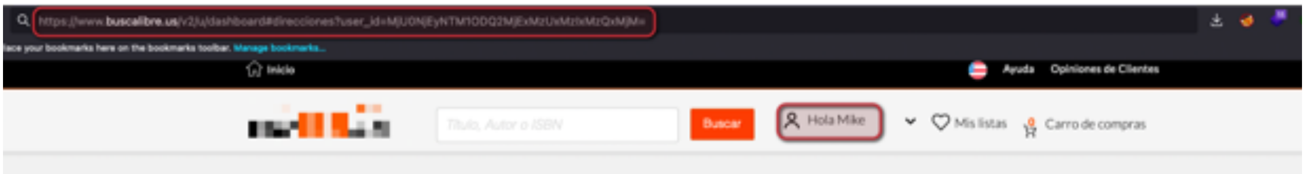


https://www.buscalibre.us/v2/u/dashboard?user_id=MjU0NjEyNTM1ODQ2MjExMzUxMzUwNTQ=

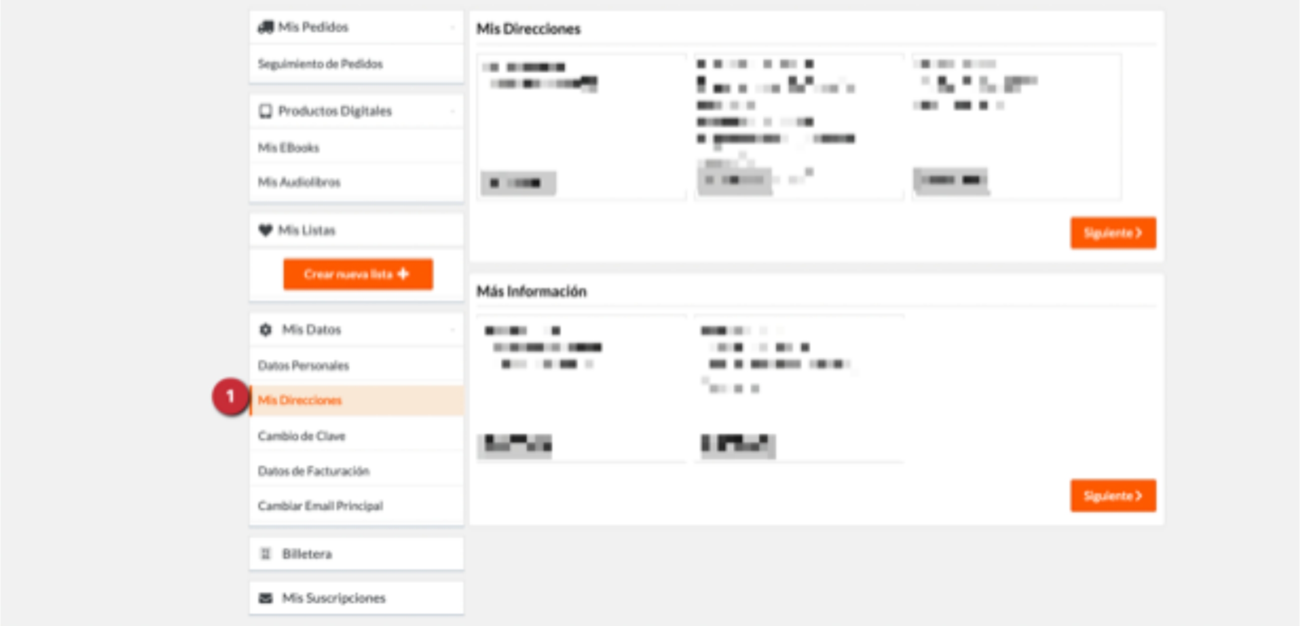
Editar Datos Personales

Nombre: Ricardo
Apellidos: Prieto
Email asociado (Cambiar): [redacted]
Fecha de Nacimiento: 13 Julio 2022

Switching into another account:



https://www.buscalibre.us/v2/u/dashboard#direcciones?user_id=MjU0NjEyNTM1ODQ2MjExMzUxMzIxMzQxMjM=



IMHO I would suggest you change the HTTP method from GET to POST and would also try to avoid direct object references or at least improve the obfuscation mechanism (currently a regular Base64 encoding).
Perhaps applying a salt value in a better hashing algorithm like SHA256 or SHA512 can improve the current state way more.

Micaela, please do not hesitate to contact me if you require further information, I will be happy to help you.
Best,

Ricardo Prieto