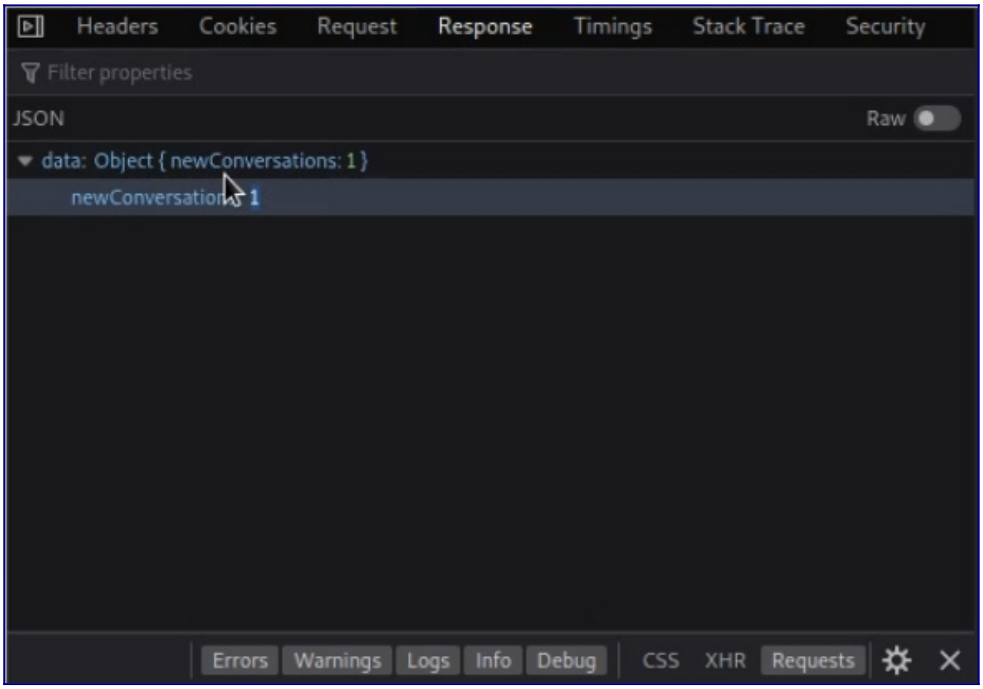
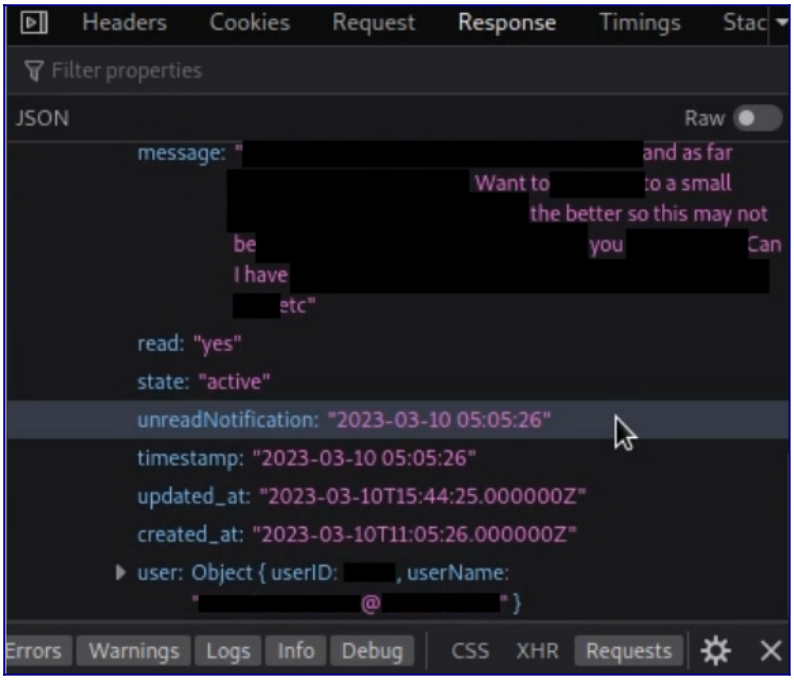
How I Hacked A Social Media E-Commerce Site Accessing Anyone’s Messages & Credit Card Information

Brent Elisens
@sixie6e
Dec 29, 2023

The function that retrieves user messages starts with an OPTIONS request of 0 bytes. It is immediately followed by a GET request to retrieve how many unread messages I have. The response is a JSON object showing how many, but none of the message content. Altering the user/conversation IDs of the GET request I get varying responses of this:



So then I started on the OPTIONS request and by doing the same thing, with random user/conversation IDs, the JSON response included the message content this time:



Next I started changing the host/URL values on the GET request and by doing the same thing, with random user/conversation IDs, the JSON response included the credit card information: