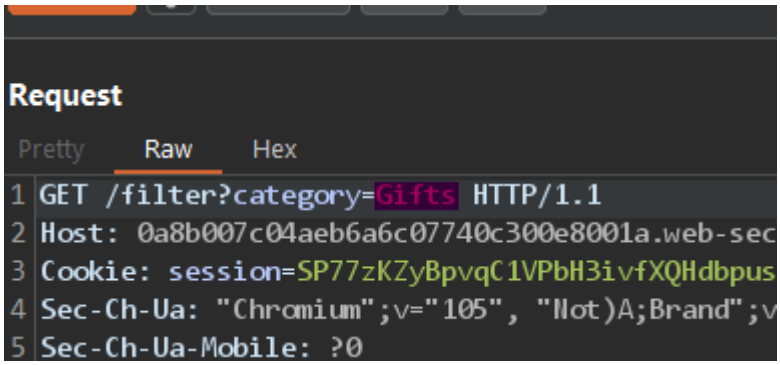
SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

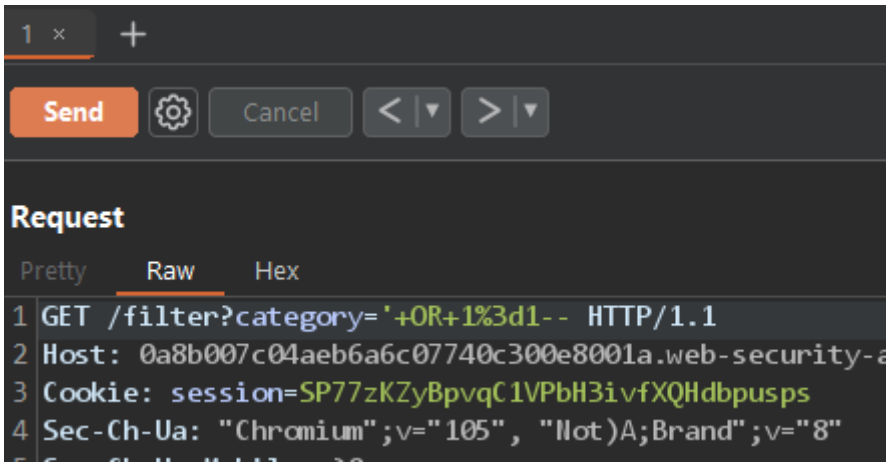
As per the previous lab, we can use the classic '1=1-- to bypass the category filters. This will allow us to view all the hidden products on the website.

This can be done directly in the URL bar or Burp. I prefer repeater beacuse I paid a small forture for it so I'm getting my monies worth :P

Capture a Category Filter Request and Send to Repeater



Adding the Classics, followd by URL encoding



Smashed It