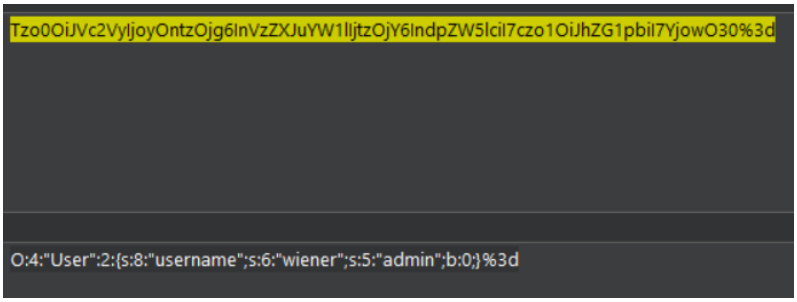
Modifying serialized objects

1. This lab uses a serialization-based session mechanism and is vulnerable to privilege escalation as a result.

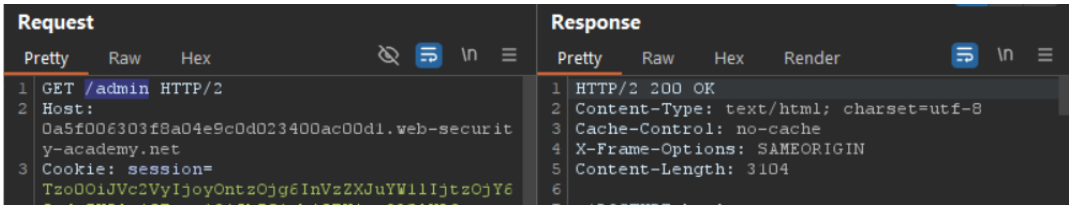
2. While browsing the web application and observing the requests, I found a session variable sent in cookies like this:

After decoding this session, I found that this is a serialized object that contains the username and his admin role (true or false).



3. I changed my admin role from 0 to 1 and encode it back and replace it with my session in the request and sent it.

4. Now, I am an admin and I have access on admin panel.



5. I request this URL /admin/delete?username=carlos and delete carlos user successfully.