Pico CTFs Write Ups week 11:

1. Cookies:
    a. Used Burp Suite and opened the browser to http://mercury.picoctf.net:21485/.
    b. After inspecting it, there was a cookie with a value of -1, if I changed the value the page would respond with an actual cookie name, for example, if I entered the value 7 the webpage would return "sugar cookies".
    c. To check the different responses, I could get I sent the response to the "Intruder" tab in Burp suite and planted a "payload" with different numbers from -1 to 40
    d. This resulted in a long list of responses, most of them were of length 1930-1950
    e. However, there was one with length 1265, after checking the response, it had the flag.
    f. picoCTF{3v3ry1_l0v3s_c00k135_94190c8a}
2. logon:
    a. Used Burp suite and opened the browser on http://jupiter.challenges.picoctf.org:15796.
    b. The problem asks you to log in as Joe but that’s not necessary, after playing around you can actually create a new account on the website since it won't check the password.
    c. After intercepting the response, it actually creates three cookies, one for password, one for username, and one for admin.
    d. The admin is set to false, however, it can be easily changed to "True" and after that, the page will give you the flag.
    e. picoCTF{th3_c0nsp1r4cy_l1v3s_6edb3f5f}