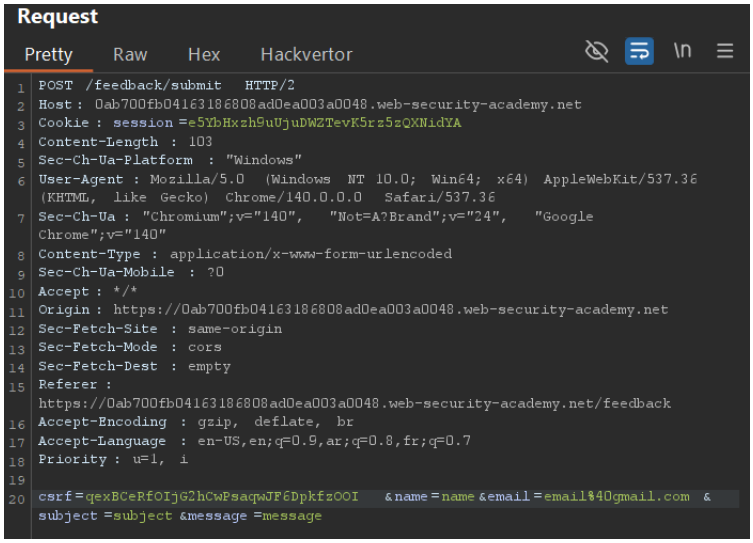
Blind OS command injection with time delays

1. This lab contains a blind OS command injection vulnerability in the feedback function.

2. The application executes a shell command containing the user-supplied details. The output from the command is not returned in the response.

3. I go to feedback form directly and submit it and intercept this request and pass it to repeater. This is the request:



4. I tried to inject this payload: **ping 127.1** into all variables that sent in request and all of them respond with 200 OK but the command didn't execute except the email, it responded with 500 internal server error. I think it's vulnerable, but the command is not right. So, I will try to manipulate the payload and inject it into the email variable.

   Note: I knew that the command didn't execute because this command sends four packets, each packet takes around 1 second and the response takes around one or two seconds

5. After many trials, I think the original command seems like: `<myInput> -n` So when I inject my payload: `|| ping+-c+10+127` the command will be: `email || ping -c 10 127 -n` and this is syntax error. So, I need to separate my command and the original command.

6. I manipulated my payload to be: `|| ping+-c+10+127 ||` and finally the response took 10 seconds, and the lab solved.