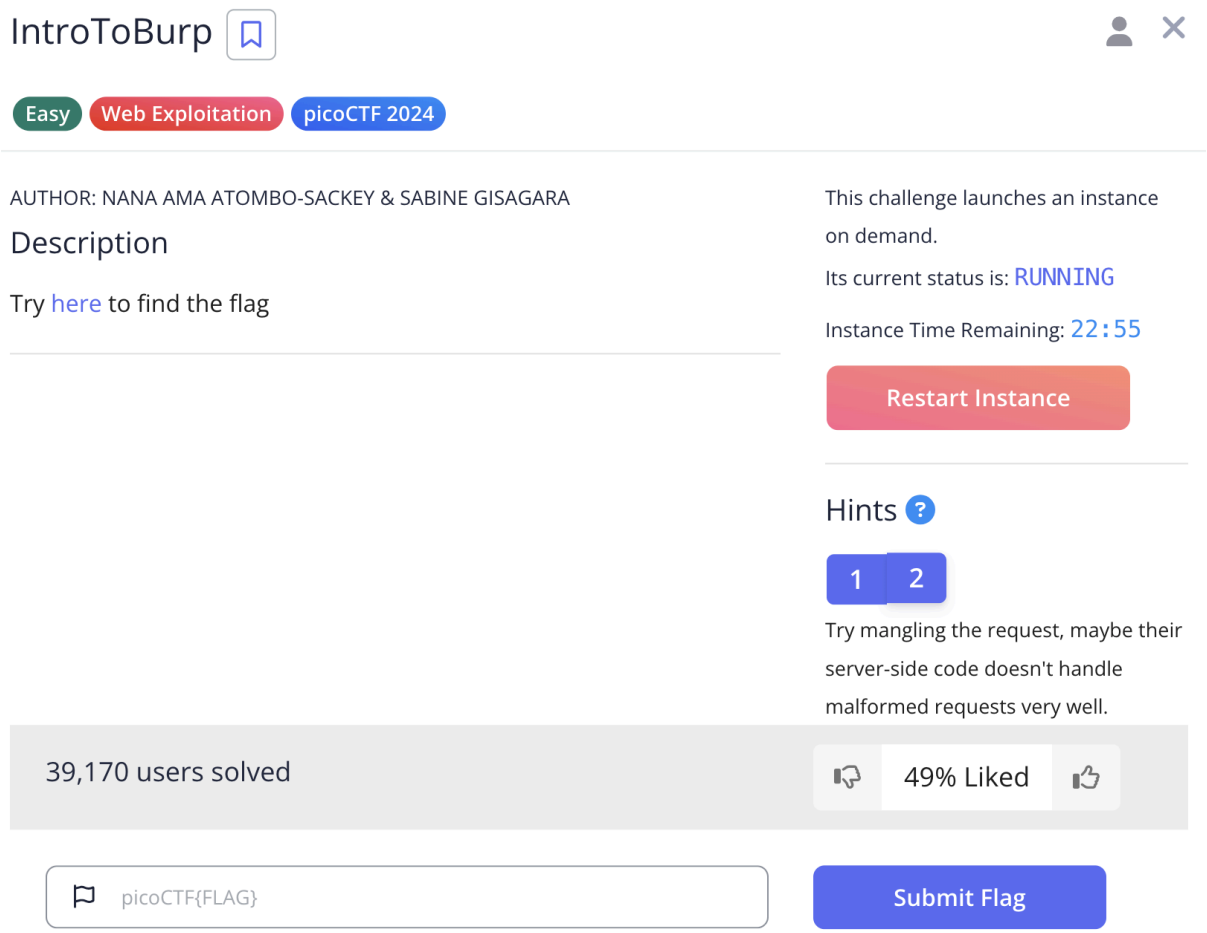


Hint :

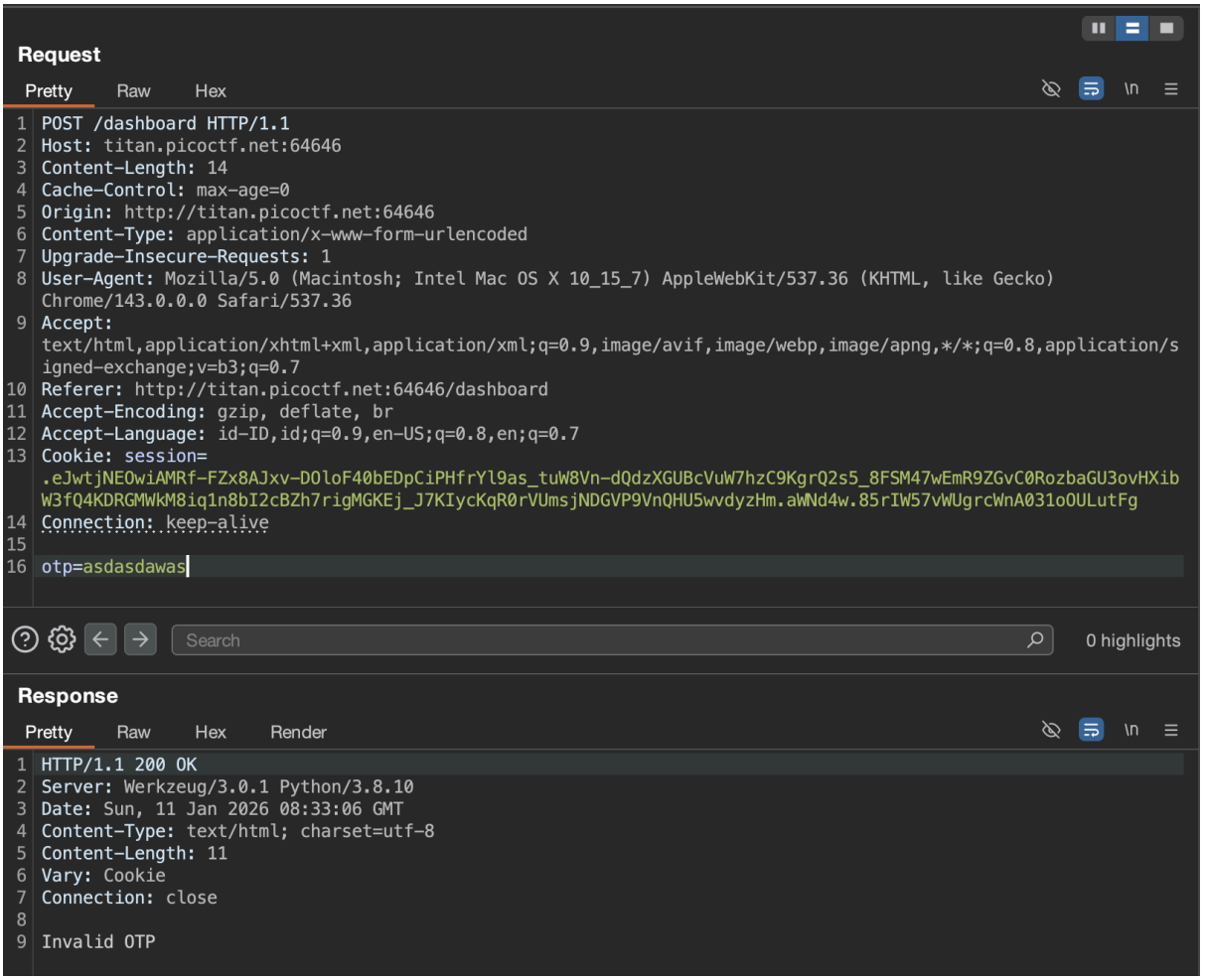
1. Intercept dengan Burpsuite
2. Coba untuk merubah apa yang ada pada isi request

Solusi :

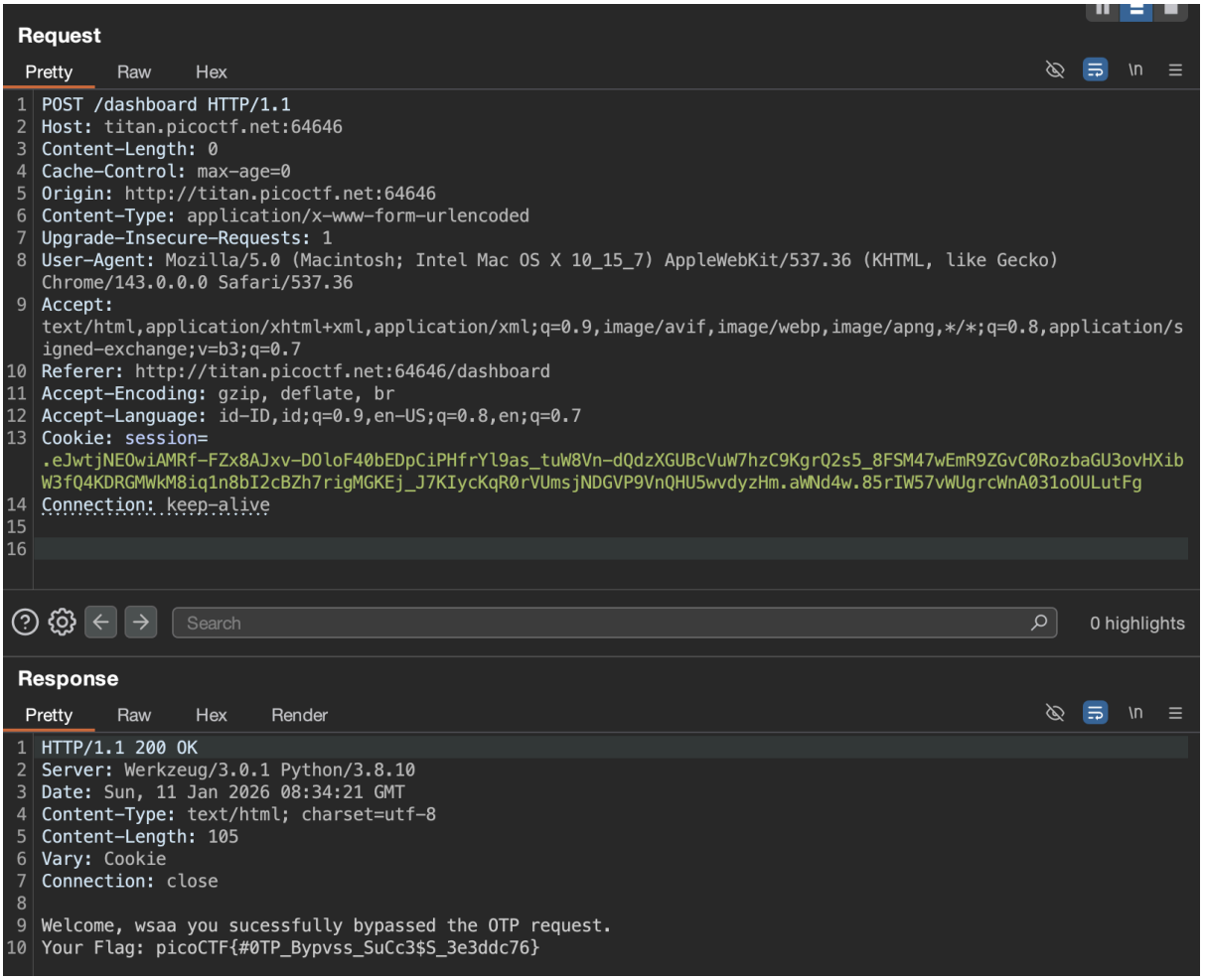
Kami membuka url pada tulisan here dan mendapatkan tampilan :

Kami coba untuk registrasi dengan memencet tombol Register setelah itu muncul permintaan OTP. Kami menyadari bagaimana cara kita dapat OTP? disitu kami stuck dan coba untuk menggunakan Burpsuite.

Setelah registrasi muncul tampilan diatas. disini kita putuskan untuk langsung menggunakan Burpsuite -> Send to repeater.



Kami langsung coba untuk send dan melihat repons dari requestnya dan terlihat kalau OTP tidak valid. kami penasaran bagaimana jika otp ditiadakan dengan menghapus otp=..... pada request. Ternyata kami mendapatkan flagnya.



Flag : picoCTF{#0TP_Bypvss_SuCc3$S_3e3ddc76}