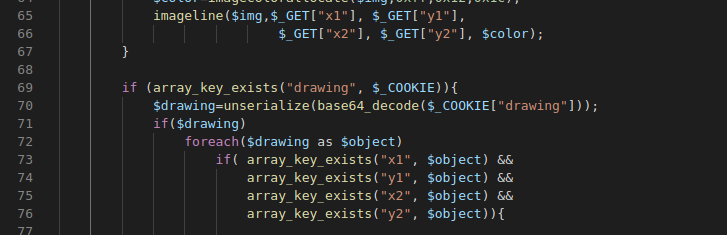
NATAS26 – SERIALIZE ATTACK

Natas26 labını çözmeden önce serialize attack nedir ve nasıl çalışır bununla ilgili bir kaç bilgi vermek gerekir(<https://portswigger.net/web-security/deserialization/>).

Natas26 nın kaynak kodlarını incelediğimizde cookie de drawing değişkinini serialize edip tutuyor ve onu kodun bir kaç yerinde unserialize edip okuyor.



Biz buradaki cookie değerine yukarıda bulunan Logger classının serialize edilmiş halini verirsek 70. satırda unserialize edecek ve kod satırında serialize ettiğimiz kod parçacığı çalışacak. Bunun için bir payload hazırlayıp cookie de gönderiyoruz.

natas26\_payload.php kodunu çalıştırıyoruz ve url encode ederek gönderiyoruz.