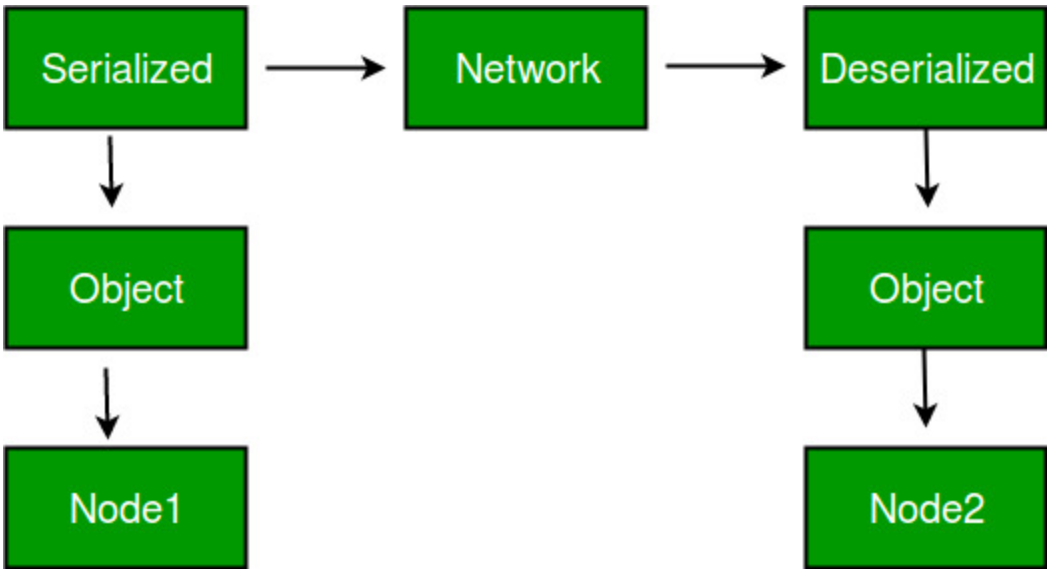
sérialisation

Qu'est-ce que la « sérialisation » ?

La sérialisation dans un résumé est le processus de conversion de données - en particulier d'« objets » dans les langages de programmation orientée objet (POO) tels que Java - en formatage de niveau inférieur appelé « flux d'octets », où elles peuvent être stockées pour une utilisation ultérieure, par exemple dans des fichiers, des bases de données et/ou parcourues sur un réseau. Il est ensuite converti ultérieurement de ce « flux d'octets » en « Objet » de niveau supérieur. Cette conversion finale est connue sous le nom de « désérialisation »



(gentiment pris de https://www.geeksforgeeks.org/classes-objects-java/)

Alors, qu'est-ce qu'un « Objet » ?

Les « objets » dans un contexte de programmation peuvent être comparés à des exemples réels. Simplement, un « Objet » n'est que cela : une chose. Les « objets » peuvent contenir différents types d'informations telles que des états ou des caractéristiques. Pour établir une corrélation avec un exemple réel...Prenons une lampe.

Une lampe est un excellent « objet ». Une lampe peut être allumée ou éteinte, la lampe peut avoir différents types d'ampoules - mais en fin de compte, c'est toujours une lampe. Le type

d'ampoule utilisé et le fait que la lampe soit « allumée » ou « éteinte » dans ce cas sont tous stockés dans un « Objet ».

Comment pouvons-nous exploiter ce processus ?

Une attaque de « sérialisation » est l'injection et/ou la modification de données tout au long de l'étape du « flux d'octets ». Lorsque l'application accède ultérieurement à ces données, un code malveillant peut entraîner de graves conséquences... allant de DoS, fuite de données ou attaques beaucoup plus néfastes comme être « enraciné » ! Pouvez-vous voir où cela va...?