03

Pickle e segurança

Vimos que é possível utilizar o `pickle` para serializar objetos Python que podem ser lidos pelo programa. Porém, devemos tomar um certo cuidado com seu uso.

Pelo fato de estarmos serializando um objeto Python, pode ser que códigos maliciosos sejam carregados e executados no programa. Logo, uma regra importante a ser seguida é: não carregar um arquivo `pickle` cuja origem possa estar comprometida e trazer algum risco à aplicação.

Neste post do blog da Synopsys (https://www.synopsys.com/blogs/software-security/python-pickling/) (em inglês), é tratado um pouco sobre o `pickle` e como usá-lo de forma segura, caso estejam interessados, é recomendo a leitura.