Recommender systems are not robust and are vulnerable to adversarial attacks (noises).

- Example 1, Vulnerability of a multimedia recommender system:

  **Motivation**

  **Performance of AMF**

  Top-K recommendation evaluation (K=100)
  - Comparing with the baselines, AMF achieves the best results in most cases.
  - AMF exhibits an average improvement of 2.9% over NeuMF, an expressive deep learning model. However, AMF is just a small MF model with fewer parameters.
  - AMF betters IRGAN by 5.5% on average, and AMF is more efficient and much easier to train than IRGAN.

  **Robustness of AMF**

  APR makes the model become less sensitive to adversarial perturbations. The table compares the relative decrease in NDCG@100 of MF trained by BPR and APR.

  **Experiment results:**
  When MF-BPR converges, further training it with APR (i.e., AMF) leads to significant improvements: