1. Nel contratto attacco.sol, la funzione attack():

   Chiama Aave per ottenere un flash loan da 1000 WETH che restituirà a fine

2. Uso tutti i 1000 WETH presi in prestito per comprarci USDC
   prezzo_WETH = riserva_USDC / riserva_WETH

   La riserva di WETH nella pool aumenta (+1000)
   La riserva di USDC diminuisce (−2.727.273)
   Il prezzo USDC/WETH scende: es. da 3000 → 2479

3. Deposito gli USDC ottenuti e il protocollo valuta con il prezzo manipolato
4. Ottengo più di 1000 WETH iniziali
5. Tengo la differenza e dò indietro i 1000 chiesti all'inizio

riserva_WETH_iniziale = 10.000
riserva_USDC_iniziale = 30.000.000

prezzo_iniziale = riserva_USDC_iniziale / riserva_WETH_iniziale
= 30.000.000 / 10.000
≈ 3.000 USDC per 1 WETH

k = riserva_WETH_iniziale × riserva_USDC_iniziale
= 10.000 × 30.000.000
= 300.000.000.000

Dopo la vendita di 1000 WETH (flash loan):
riserva_WETH_nuova = 10.000 + 1000 = 11.000
riserva_USDC_nuova = k / riserva_WETH_nuova
= 300.000.000.000 / 11.000
≈ 27.272.727 USDC

usdc_ottenuti = riserva_USDC_iniziale - riserva_USDC_nuova
= 30.000.000 - 27.272.727
≈ 2.727.273 USDC

prezzo_nuovo = riserva_USDC_nuova / riserva_WETH_nuova
= 27.272.727 / 11.000
≈ 2.479 USDC per 1 WETH

Depositi i 2.727.273 USDC come collaterale nel protocollo di lending.
Il protocollo calcola il valore del collaterale in WETH usando il prezzo manipolato:

valore_collaterale_in_WETH = usdc_ottenuti / prezzo_nuovo
= 2.727.273 / 2.479
≈ 1100 WETH

Prestito ricevuto: il protocollo, privo di controllo LTV, ti dà l'intero valore → 1100 WETH!

Guadagno netto di circa 1100-1000 = 100WETH