SOSA - LAB3, Ivan Futivić

Opis eventualnih promjena obavljenih na kodu iz Dodatka A

- U funkciju perform_division dodana dokumentacija koja ukazuje na to da kad ulazne vrijednosti nisu brojevi funkcija mora vraćati "nan"
- U funkciji login_success dodana dokumentacija da funkcija u slučaju lošeg parsiranja broja ili u slučaju evaluacije neispravnog izraza vraća "nan"
- Dio koda je izvučen u funkciju main kako bi ga bilo lakše testirati
- Funkcija main umjesto "exit(0)" poziva return

Opis razvijenih testova

- Napisani su testovi za:
    - klasu OperationsManager i funkciju perform_division
    - funkciju login_success
    - funkciju main

- Testovi za funkciju perform_division:
    - Obično dijeljenje cijelih brojeva
        - Prošao
    - Dijeljenje s negativnim cijelim brojem
        - Prošao
    - Dijeljenje s nulom
        - Pao
        - Dijeljenje s nulom rezultirao iznimkom, očekivan rezultat je "nan"
    - Dijeljenje koje rezultira decimalnim brojem s beskonačno decimalnim mjesta
        - Prošao
    - Dijeljenje u slučaju kad su ulazni argumenti stringovi
        - Pao
        - Rezultira iznimkom tijekom parsiranja stringova u float, očekivan rezultat je "nan"
    - Dijeljenje sa "nan"
        - Prošao
    - Dijeljenje sa "inf" i "-inf"
        - Prošao

- Testovi za funkciju login_success:
  - Korištenje ispravih vrijednosti
    - Prošao
  - Korištenje stringova u inputu
    - Pao
    - Rezultira iznimkom tijekom parsiranja stringova u float, očekivan rezultat je "nan"
  - Upisivanje vrijednosti koje rezultiraju dijeljenjem s nulom
    - Pao
    - Dijeljenje s nulom rezultirao iznimkom, očekivan rezultat je "nan"
  - Upisivanje matematičkom izraza u kojem se dijeli s nulom
    - Pao
    - Dijeljenje s nulom rezultirao iznimkom, očekivan rezultat je "nan"
  - Korištenje stringova u matematičkom izrazu
    - Pao
    - Rezultira iznimkom u eval funkciji
- Testovi za funkciju main:
  - Login s ispravnim korisničkim imenom i lozinkom
    - Prošao
  - Login s neispravnim korisničkim imenom
    - Prošao
  - Login s neispravnom lozinkom
    - Prošao

Bandit

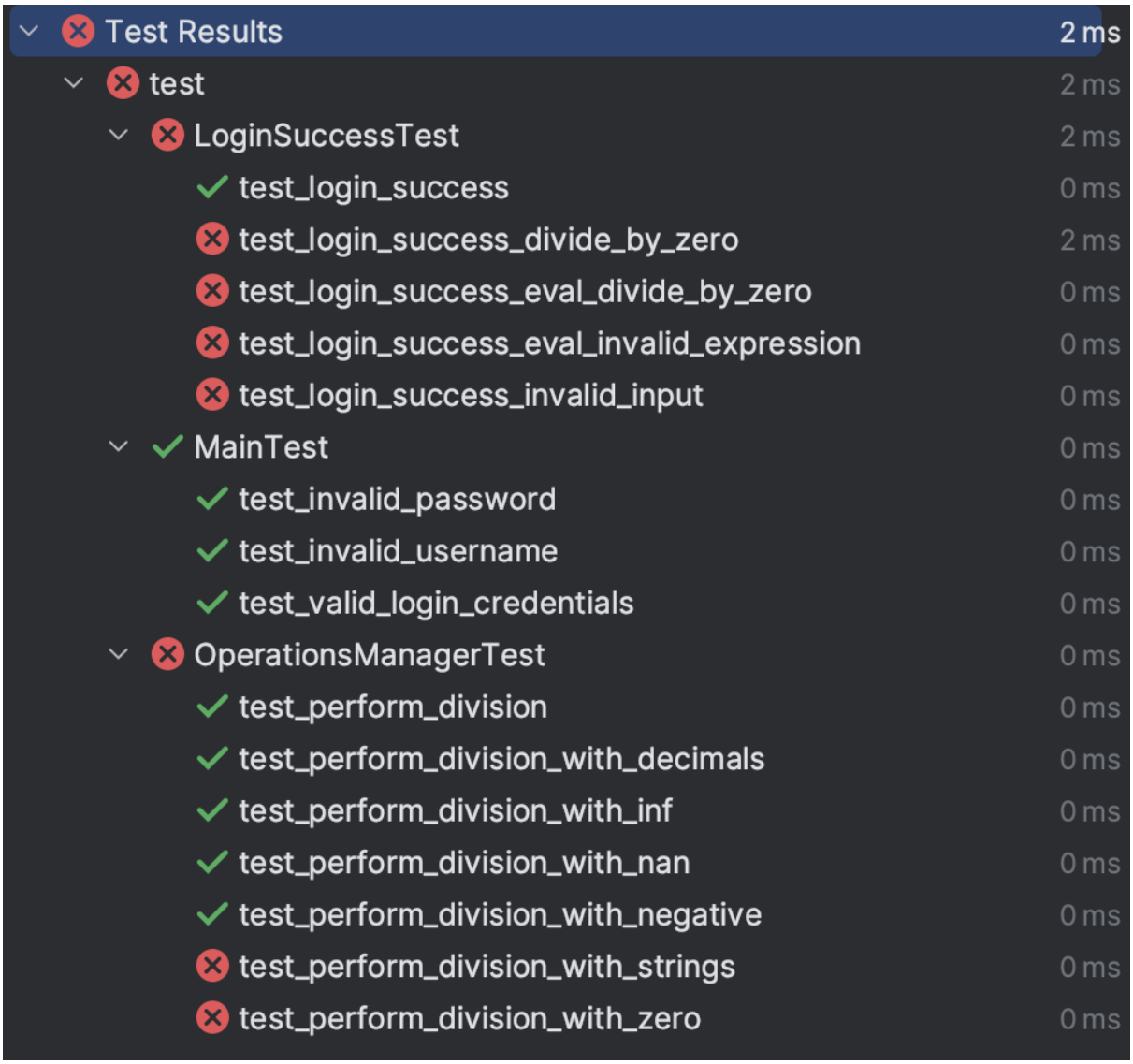
- Instaliran s "pip3 install bandit"
- Pokrenuto s "bandit -r ."
- Nije pronašao probleme s validacijom inputa i argumenata funkcije
- Pronašao dva sigurnosna problema:
  - "Use of possibly insecure function - consider using safer ast.literal_eval"
    - Ranjivost **CWE-78**
    - Obični "eval" ne provodi neutralizaciju specijalnih elemenata u ulazu, preporučuje se koristiti ast.literal_eval
  - "Possible hardcoded password: '123'"
    - Ranjivost **CWE-259**
    - Nije pametno čuvati lozinke u kodu u jasnom tekstu. Preporučuje se koristiti hashing i usporediti hash ulaza s hashom ispravne lozinke

```
Run started:2023-05-31 16:47:47.696965

Test results:
>> Issue: [B307:blacklist] Use of possibly insecure function - consider using safer ast.literal_eval.
   Severity: Medium   Confidence: High
   CWE: CWE-78 (https://cwe.mitre.org/data/definitions/78.html)
   More Info: https://bandit.readthedocs.io/en/1.7.5/blacklists/blacklist_calls.html#b307-eval
   Location: main.py:24:21
23      expression = input("Enter a mathematical formula to calculate: ")
24      print("Result:", eval(expression))
25
--------------------------------------------------
>> Issue: [B105:hardcoded_password_string] Possible hardcoded password: '123'
   Severity: Low   Confidence: Medium
   CWE: CWE-259 (https://cwe.mitre.org/data/definitions/259.html)
   More Info: https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_password_string.html
   Location: main.py:31:37
30
31      if user != "root" or password != "123":
32          print("Wrong username or password!")
--------------------------------------------------
Code scanned:
    Total lines of code: 29
    Total lines skipped (#nosec): 0
    Total potential issues skipped due to specifically being disabled (e.g., #nosec BXXX): 0

Run metrics:
    Total issues (by severity):
        Undefined: 0
        Low: 1
        Medium: 1
        High: 0
    Total issues (by confidence):
        Undefined: 0
        Low: 0
        Medium: 1
        High: 1
Files skipped (0):
```

Ispis alata Bandit (bandit_report.txt)



Rezultati pokretanja testova (test_run.txt)