Ćwiczenia 05 - BSI

Autorzy:

Szymon Jakóbiak

Mikołaj Noga

22.11.2021

Wybrany przez nas język programowania do wykonania następującego ćwiczenia to ***Java***.

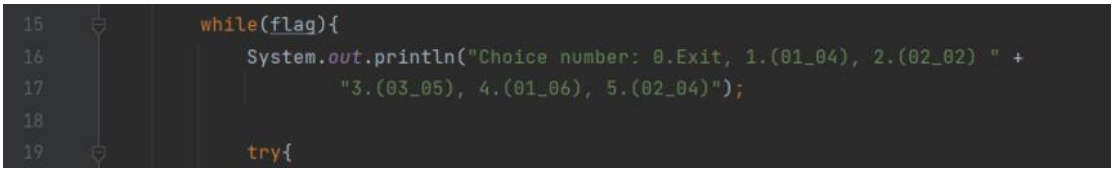
Analiza repozytorium opiera się o standard ***CERT Oracle Secure Coding Standard***.

Badane repozytorium: https://github.com/MikolajNoga/BSI

Naruszenia CERT w badanym repozytorium:

1. ERR02-J - wykryty na linii 15 w klasie **Main.java**

Wycinek wykrycia naruszenia z narzędzia SonarQube



Wycinek miejsca w kodzie, w którym występuje naruszenie

Noncompliant Code Example

```
System.out.println("My Message");  // Noncompliant
```

Compliant Solution

```
logger.log("My Message");
```

See

- CERT, ERR02-J. - Prevent exceptions while logging data

Przykład rozwiązania problemu

W przypadku naszej aplikacji użycie loggera nie jest wszędzie możliwe, ponieważ potrzebujemy komunikacji z użytkownikiem, natomiast logger może tylko informować użytkownika.

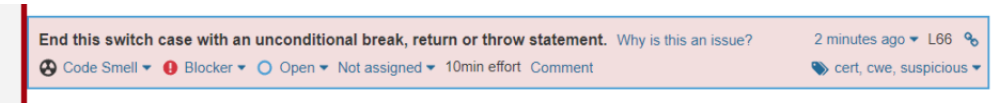
W linijce 98 można użyć loggera stosując następujący kod:

logger.log(Level.INFO, "You provided wrong type of variable");

logger.log(Level.INFO, e.getMessage());

Logger logger = Logger.getLogger(String.valueOf(Main.class));

2. MSC17-C - wykryty na linii 66 w klasie **Main.java**



Wycinek miejsca w kodzie, w którym występuje naruszenie

```
15        while(flag){
16            System.out.println("Choice number: 0.Exit, 1.(01_04), 2.(02_02) " +
17                    "3.(03_05), 4.(01_06), 5.(02_04)");
18
19            try{
```

Wycinek miejsca w kodzie, w którym występuje naruszenie

```
switch (myVariable) {
  case 1:
    foo();
    break;
  case 2:  // Both 'doSomething()' and 'doSomethingElse()' will be executed. Is it on purpose ?
    doSomething();
  default:
    doSomethingElse();
    break;
}
```

Compliant Solution

```
switch (myVariable) {
  case 1:
    foo();
    break;
  case 2:
    doSomething();
    break;
  default:
    doSomethingElse();
    break;
}
```

Przykład rozwiązania problemu

3. MSC13-C - wykryty na linii 316 w klasie **Main.java**

Wycinek miejsca w kodzie, w którym występuje naruszenie

Noncompliant Code Example

```
i = a + b; // Noncompliant; calculation result not used before value is overwritten
i = compute();
```

Compliant Solution

```
i = a + b;
i += compute();
```

Przykład rozwiązania problemu

- MITRE, CWE-563 - Assignment to Variable without Use ('Unused Variable')
- CERT, MSC13-C. - Detect and remove unused values
- CERT, MSC56-J. - Detect and remove superfluous code and values

Wykrycie błędu