The CWE Top 25 - omówienie pod względem projektu

Wiktoria Migasiewicz

1. **Out-of-bonds Write**

   Aby zapobiec zapisywaniu przez program danych poza końcem lub przed początkiem zamierzonego bufora, istnieje warunek sprawdzający czy długość słowa klucza, który ma być wpisany do tablicy nie przekracza jej rozmiaru, jeśli tak program zakańcza się. (We wszelkich działaniach zapisujących dane do tablicy, jednym z warunków jest nieprzekroczenie jej rozmiaru.) Deklarując wszystkie zmienne przypisuję im wartość docelową lub równą 0 i używam przy tym { }.

```
if (keyWord.length() < 25)
    {
        unsigned int j,a={0};
        for(int i={0}; i<4 && a< keyWord.length() ; i++)
            {
                j=0;
                for(j=0;j<5 && a< keyWord.length() ;j++)
                    {
                        tab2[i][j]=keyWord.at(a);
                        a++;
                    }
            }
    }
else
    {
        cout << "Too many signs in key word" << endl;
        exit (0);
    }
```

```
string fileName = {0};
```

2. **Improper Input Validation**

   Aby program weryfikował dane wejściowe czy mają niezbędne do bezpiecznego i prawidłowego przetwarzania dane, program

posiada pętlę i upewnia się czy wprowadzone dane są zgodne z oczekiwaniami, jeśli tak, program egzekwuje się dalej, jeśli nie - wyświetla użytkownikowi komunikat o niepoprawnym wprowadzeniu danych i daje możliwość ponownego wprowadzenia ich. Jeśli sytuacja się powtórzy, program zostaje zakończony bez błędów.

```
char decision = {0};
for (int i = {0}; i < 2; i++)
    {
        cin >> decision;
        cout << endl;
        if (decision == 'M' )
            {
                GetPlaintext (plaintext);
                GetKeyWord (keyWord);
                break;
            }
        else if (decision == 'F')
            {
                ReadingFile (plaintext);
                GetKeyWord (keyWord);
                break;
            }
        else if (decision == 'Q')
            {
                cout << endl << "QUITTING...";
                exit(0);
            }
        else
            {
                cout << "Wrong sign has been entered" << endl << endl << "You have one more try or else the program closes";
                cout << endl << "->";
            }
    }
```

3. **Out-of-bonds Read**

   Aby zapobiec odczytywaniu przez program danych poza końcem lub przed początkiem zamierzonego bufora, chcąc wywołać wartości komórek tabeli, posługuję się funkcją .at() zamiast używać nawiasów kwadratowych - [ ].

```
if( keyWord.at(i) == keyWord.at(a) )
```

4. **Null Pointer Dereference**

   Aby nie spowodować w programie awarii, gdy odwołuje się do wskaźnika o wartości NULL, program wyświetla komunikat o zakończeniu kodowania i zamyka program bez błędów, czy też awarii.

```
//jesli nie ma wskaznika wychodzimy z programu
if (coordinates_of_first == nullptr || coordinates_of_second == nullptr)
   {
       cout << "ERROR - END OF CODING" << endl;
       return "";
```