

ВЗЛОМ СТЕКА.

Напарник – Антон Манакин.

Обоюдный взлом был проведён в формате поиска багов и их исправления.

Что было найдено у меня:

- *Основной баг:* можно нарочно поменять элементы в каждом из буферов по своему и перезаписать все хэши на нужные при помощи функций хеширования, и программа ничего с этим не сделает.

```
printf("CAGE[2] = %lg\n", cage_copy->stack->buffer[3]);
printf("STACK[2] = %lg\n", Anna->stack->buffer[3]);

printf("HASH ANNA STACK = %li\n", Anna->stack->hash_stack);
printf("HASH ANNA BUFFER = %li\n", Anna->stack->hash_buffer);
printf("HASH COPY STACK = %li\n", cage_copy->stack->hash_stack);
printf("HASH COPY BUFFER = %li\n", cage_copy->stack->hash_buffer);

cage_copy->stack->buffer[2] = 10.1;
Anna->stack->buffer[2] = 10.1;

cage_copy->stack->hash_buffer = hashing_buffer(cage_copy);
cage_copy->stack->hash_stack = hashing_stack(cage_copy);

Anna->stack->hash_buffer = hashing_buffer(Anna);
Anna->stack->hash_stack = hashing_stack(Anna);

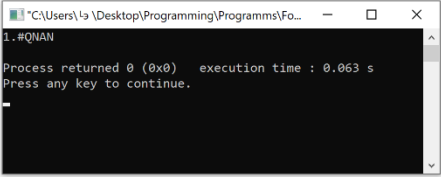
for (int i = 1; i <= 10; i++)
{
    stack_pop(&Anna, &value);
    printf("VALUE[%i] = %lg\n", i, value);
}
stack_destruct(&Anna);
```

Можно исправить при помощи идентификатора static у функций и копирующей структуры стека, но при формате хранения в файле типа header я не представляю, как это сделать.

Комментарий напарника: При изменении сначала нужно изменить хэш буфера, а потом хэш структуры, иначе в новом хэше структуры будет старое значение хэша буфера.

- *Баг транзакций:* Не учитывались все случаи транзакций. Некоторые были добавлены, при всех остальных случаях выдаётся ошибка вторжения.
- *Невнимательный баг:* при попытке удалить последний элемент пустого стека, удалялась канарейка и программа не вылетала.

```
1... #include <stdio.h>
2... #include <stdlib.h>
3... #include <math.h>
4... #include "Stack.h"
5
6 int main()
7 {
8     Stack *pain = stack_new(10);
9
10    double a;
11
12    stack_pop(&pain, &a);
13    printf("%lg\n", a);
14
15    stack_destruct(&pain);
16
17    return 0;
18 }
19
```



Описание проблемы: В проверке на пустоту стека в функции `stack_pop` не учитывалось, что там всегда лежат две канарейки и длина всегда должна быть не меньше 1.

```
if ((*that_stack)->stack->length <= 0)
{
    ASSERTION(STACK_UNDERFLOW);
    stack_dump((*that_stack), STACK_UNDERFLOW, STACK_POP);
    return STACK_UNDERFLOW;
}
```

Описание проблемы: В проверке на пустоту стека в функции `stack_pop` не учитывалось, что там всегда лежат две канарейки и длина всегда должна быть больше 1.

Проблема исправилась проверкой длины, уменьшенной на 1.