Lab 5 - Secure Coding

Overview

The objective of this lab is to understand different concepts of vulnerable/buggy situations which get introduced into our programs and how to patch or secure those programs. In particular, you'll be given vulnerable/buggy C code snippets and you'll have to figure out the problem and the source. Then you'd patch that code by writing the correct version that solves the problem without introducing any further bug or vulnerability.

Tasks

Task 01

```c
enum { TABLESIZE = 100 };

static int table[TABLESIZE];

int *f(int index) {
  if (index < TABLESIZE) {
    return table + index;
  }
  return NULL;
}
```

Figure out the source of the problem. Write that in your report and also the corrected version that solves the problem.

Task 02

```c
#include <stddef.h>
#define COLS 5
#define ROWS 7
static int matrix[ROWS][COLS];
```

```
void init_matrix(int x) {
  for (size_t i = 0; i < COLS; i++) {
    for (size_t j = 0; j < ROWS; j++) {
      matrix[i][j] = x;
    }
  }
}
```

Figure out the problem and the reason behind it. Write that in your report and also the corrected version that solves the problem.

Task 03

```
#include <string.h>
#include <stdlib.h>

char *init_block(size_t block_size, size_t offset,
                 char *data, size_t data_size) {
  char *buffer = malloc(block_size);
  if (data_size > block_size || block_size - data_size < offset) {
    /* Data won't fit in buffer, handle error */
  }
  memcpy(buffer + offset, data, data_size);
  return buffer;
}
```

Figure out the problem and the reason behind it. Write that in your report and also the corrected version that solves the problem.

Task 04

```
void clear(int array[]) {
  for (size_t i = 0; i < sizeof(array) / sizeof(array[0]); ++i) {
     array[i] = 0;
   }
```

```
}

void dowork(void) {
  int dis[12];

  clear(dis);
  /* ... */
}
```

Figure out the problem and the reason behind it. Write that in your report and also the corrected version that solves the problem.

Task 05

```
#include <stdio.h>

void func(void) {
  char c_str[3] = "abc";
  printf("%s\n", c_str);
}
```

Figure out the problem and the reason behind it. Write that in your report and also the corrected version that solves the problem.

Task 06

```
#include <stddef.h>

void copy(size_t n, char src[n], char dest[n]) {
   size_t i;

   for (i = 0; src[i] && (i < n); ++i) {
     dest[i] = src[i];
   }
   dest[i] = '\0';
}
```

Hint: *Off-by-One Error*

Figure out the problem and the reason behind it. Write that in your report and also the corrected version that solves the problem.

Submission

Submit the final report following the instructions in each task.