Practical exercise: password checker

zaterdag 10 december 2022 11:50

The following two lines of code:

```
char test[2];//Should hold the result of the test at the first index
char userInput[10];
```

create two variables on the stack; since the stack grows starting from the bottom, we have that the variable test is stored on the bottom, while the variable userInput is stored immediately above that. Furthermore, we note that this program has a buffer overflow vulnerability; when more characters are put into the userInput during the scanf operation than the variable can hold, they flow over into the next variable, which, in this case, is test. Thus, when we set the eleventh character of the input to 1, we are effectively setting the first element of the test variable to 1; this makes the if-statement later on in the program evaluate to true, and makes the program effectively accept the password.

input	123456789	1234567890	12345678901
userInput[0]	1	1	1
userInput[1]	2	2	2
userInput[2]	3	3	3
userInput[3]	4	4	4
userInput[4]	5	5	5
userInput[5]	6	6	6
userInput[6]	7	7	7
userInput[7]	8	8	8
userInput[8]	9	9	9
userInput[9]	\0	0	0
test[0]		\0	1
test[1]			\0