Buffer Overflow Attacks

What is the idea?

- Injecting wrong data input in a way that it will be interpreted as instructions

How data can become instructions?

- Because the data and instructions are the same thing binary values in memory

When was it discovered for the first time?

➡ Understood as early as 1972, first severe attack in 1988

Buffer Overflow Attacks

What is the idea?

➡ Injecting wrong data input in a way that it will be interpreted as instructions

How data can become instructions?

➡ Because the data and instructions are the same thing binary values in memory

When was it discovered for the first time?

➡ Understood as early as 1972, first severe attack in 1988

What you need to know

- understand C functions
- familiar with assembly code
- understand the runtime stack and data encoding
- know how systems calls are performed
- understand the exec() system call