malicious input

type checker

string

badstring pfstr

badString

pfstr

fgets(FILE *)

checkpt(badstr)

printf(pfstr, ...)

Y N

10 16

Strongly typed

- Cannot violate type system

double printf(int, char, long);

not known

(char*) 3

?

Segfault

bad deref — NULL

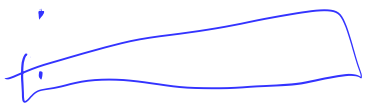
— uninit

Compile

nullable<T>

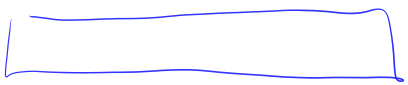
```
null? x {
}{
}
if (x is null) {
    // no **x allowed
} else {
    // *x allowed
}
```

```
int *x;
```



nullable

```
x = malloc(24);
```



nullable (error)

runtim

Check

```
test    %rax, %rax
Je      Bad mem
Mov     (%rax), %rdx
```

bad mem:
    NullPointerExc
    throw an exception

index bounds

if (i ≥ a.length)
    then new IOBE
a[i]

Memory

null

index / overflow

memory leak — GC

malloc

no

free

use after free — GC

borrow

Ownership

1 func owns each address at a time

Code owns heap memory

```
f( ) {
    x = malloc
    g(x)
    free(x)
}
```

```
borrow
g(int *x) {
}
```

Rust

non-rust laws

✓ ask me anything