

# Lecture 12: Compiler Checks

Talen en Compilers 2023-2024, period 2

Lawrence Chonavel

Department of Information and Computing Sciences, Utrecht University



# Compilers

```
char* s = "hello",  
while (  
    putchar(*s++)  
);
```

```
.LC0:  
.string "hello"  
main:  
pushq %rbx  
movl $.LC0, %ebx  
.L2:  
movq stdout(%rip), %rsi  
movsbl (%rbx), %edi  
addq $1, %rbx  
call putc  
testl %eax, %eax  
jne .L2  
popq %rbx  
ret
```

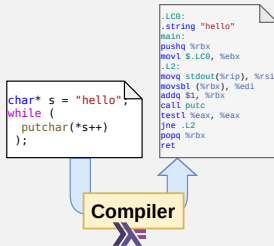
**Compiler**



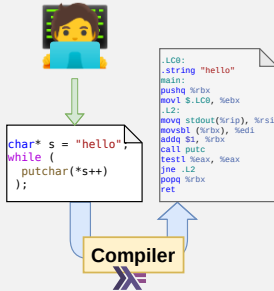
# Human Error



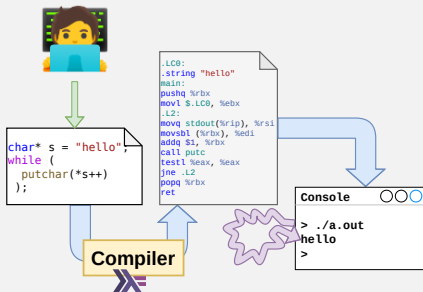
# Programmer Error



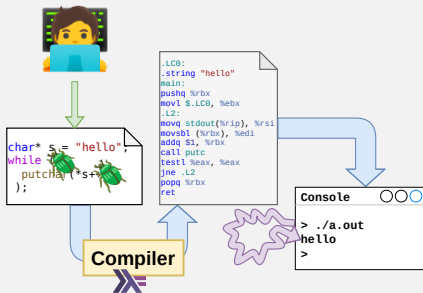
# Programmer Error



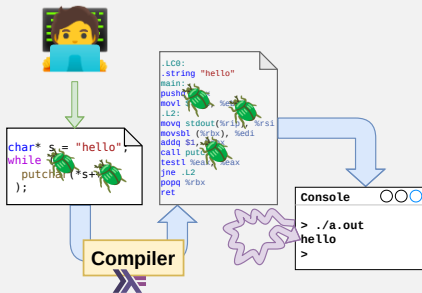
# Programmer Error



# Programmer Error

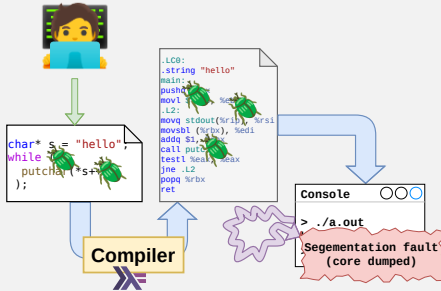


# Programmer Error

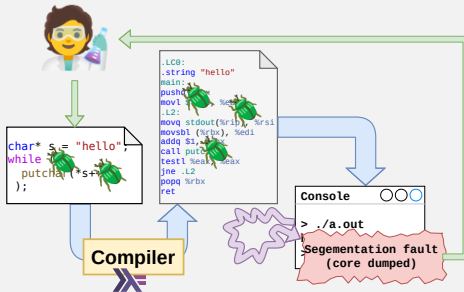




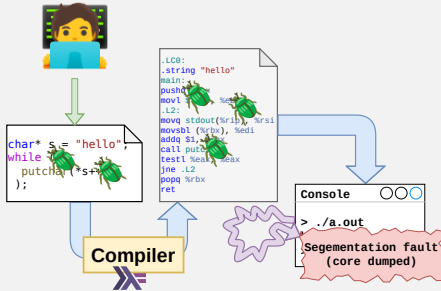
# Programmer Error



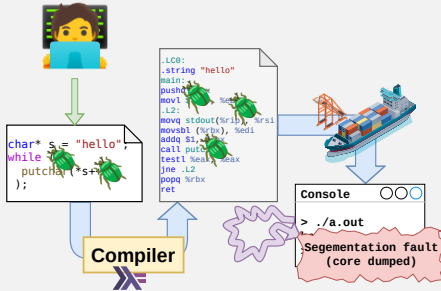
# Programmer Error



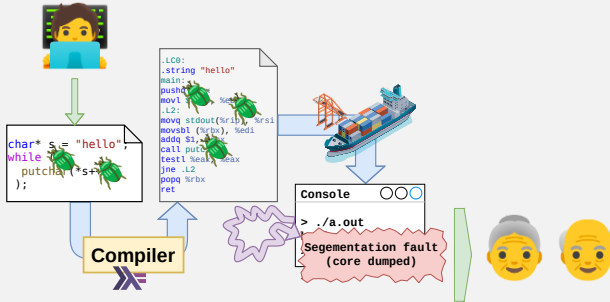
# Programmer Error



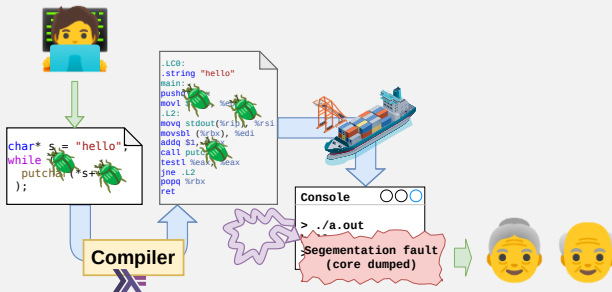
# Programmer Error



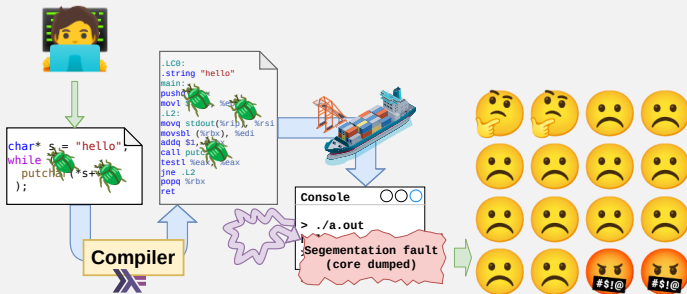
# Programmer Error



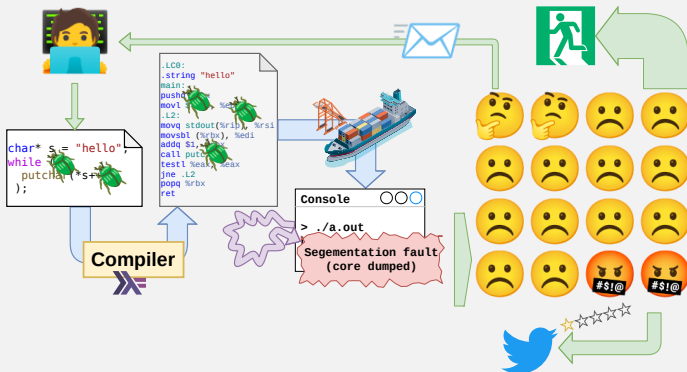
# Consequences



# Consequences

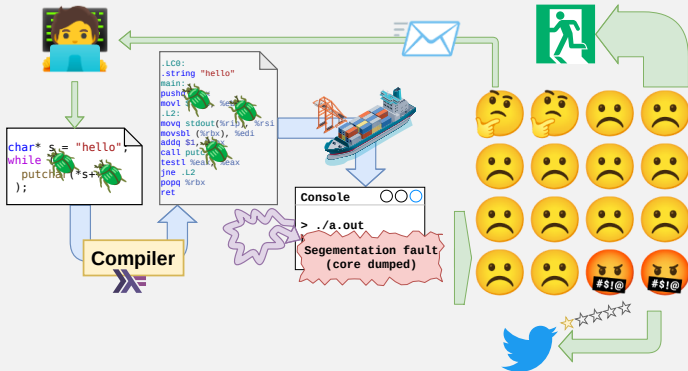


# Consequences

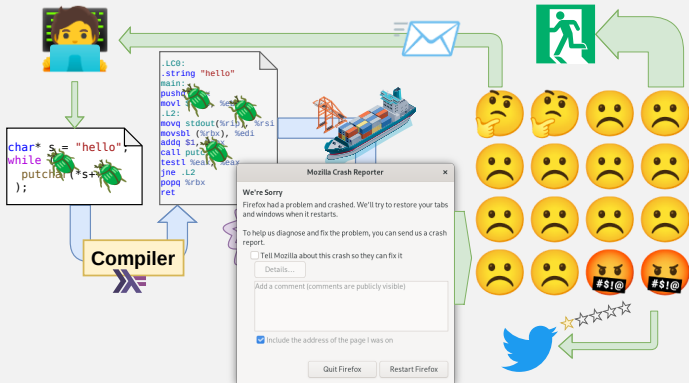




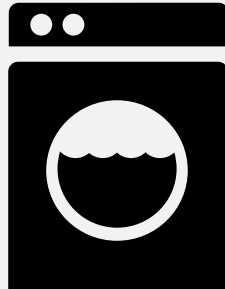
# Error Message Quality



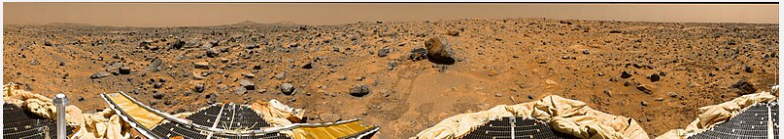
# Error Message Quality



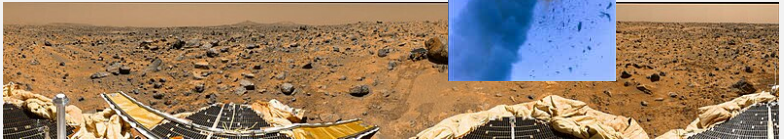
# Error Messages aren't always enough



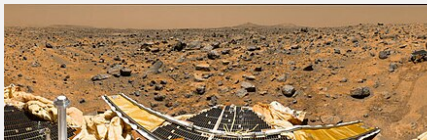
# Error Messages aren't always enough




# Error Messages aren't always enough



# Error Messages aren't always enough




# Error Messages aren't always enough




Ariane V88 self-destructs  
after failed float64 -> int16  
conversion (1996)

[http://www.capcomespace.net/dossiers/espace\\_europeen/ariane/ariane5/AR501/V88\\_AR501.htm](http://www.capcomespace.net/dossiers/espace_europeen/ariane/ariane5/AR501/V88_AR501.htm)



Pathfinder Mars Lander  
goes to sleep after  
priority inversion (1997)

[https://en.wikipedia.org/wiki/Mars\\_Pathfinder#On-board\\_computer](https://en.wikipedia.org/wiki/Mars_Pathfinder#On-board_computer)




6200 "Sudden Unintended Acceleration"  
complaints for Toyota cars (2010)  
"Spaghetti code" suspected

[https://ptolemy.berkeley.edu/projects/chess/pubs/1081/koopman14\\_toyota\\_ua\\_slides.pdf](https://ptolemy.berkeley.edu/projects/chess/pubs/1081/koopman14_toyota_ua_slides.pdf)

The wreckage of a Lexus ES 350 in which four people died in August after it accelerated out of control.




# Error Messages aren't always enough




Ariane V88 self-destructs  
after failed float64 -> int16  
conversion (1996)

[http://www.capcomespace.net/dossiers/espace\\_europeen/ariane/ariane5/AR501/V88\\_AR501.htm](http://www.capcomespace.net/dossiers/espace_europeen/ariane/ariane5/AR501/V88_AR501.htm)



Pathfinder Mars Lander  
goes to sleep after  
priority inversion (1997)

[https://en.wikipedia.org/wiki/Mars\\_Pathfinder#On-board\\_computer](https://en.wikipedia.org/wiki/Mars_Pathfinder#On-board_computer)



6200 "Sudden Unintended Acceleration"  
complaints for Toyota cars (2010)  
"Spaghetti code" suspected


[https://ptolemy.berkeley.edu/projects/chess/pubs/1081/koopman14\\_toyota\\_ua\\_slides.pdf](https://ptolemy.berkeley.edu/projects/chess/pubs/1081/koopman14_toyota_ua_slides.pdf)

The wreckage of a Lexus ES 350 in which four people died in August after it accelerated out of control.






# Error Messages aren't always enough



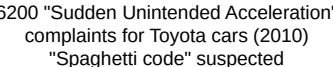
Ariane V88 self-destructs  
after failed float64 -> int16  
conversion (1996)

[http://www.capcomespace.net/dossiers/espace\\_europeen/ariane/ariane5/AR501/V88\\_AR501.htm](http://www.capcomespace.net/dossiers/espace_europeen/ariane/ariane5/AR501/V88_AR501.htm)



Pathfinder Mars Lander  
goes to sleep after  
priority inversion (1997)

[https://en.wikipedia.org/wiki/Mars\\_Pathfinder#On-board\\_computer](https://en.wikipedia.org/wiki/Mars_Pathfinder#On-board_computer)



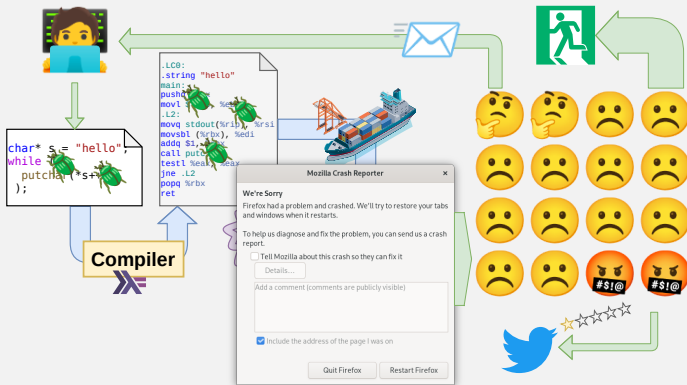
6200 "Sudden Unintended Acceleration"  
complaints for Toyota cars (2010)  
"Spaghetti code" suspected

[https://ptolemy.berkeley.edu/projects/chess/pubs/1081/koopman14\\_toyota\\_ua\\_slides.pdf](https://ptolemy.berkeley.edu/projects/chess/pubs/1081/koopman14_toyota_ua_slides.pdf)

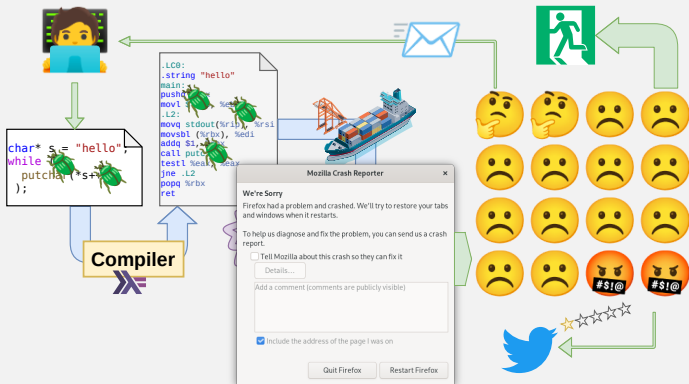
The wreckage of a Lexus ES 350 in which four people died in August after it accelerated out of control.



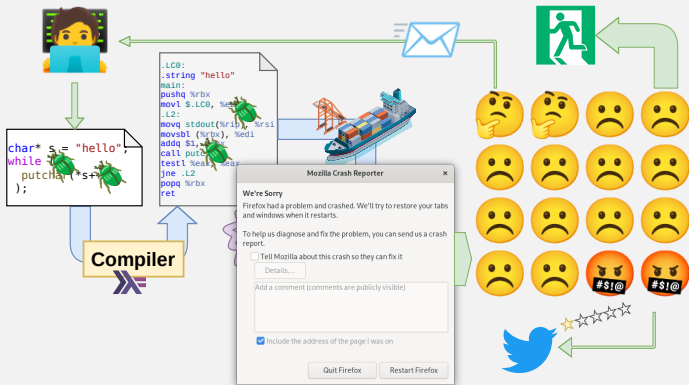
# Fewer Errors



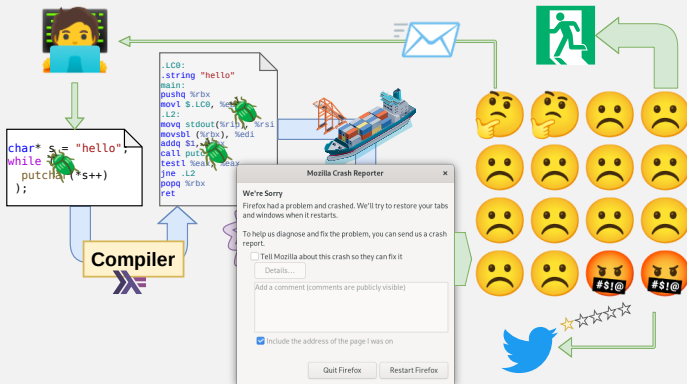
# Fewer Errors



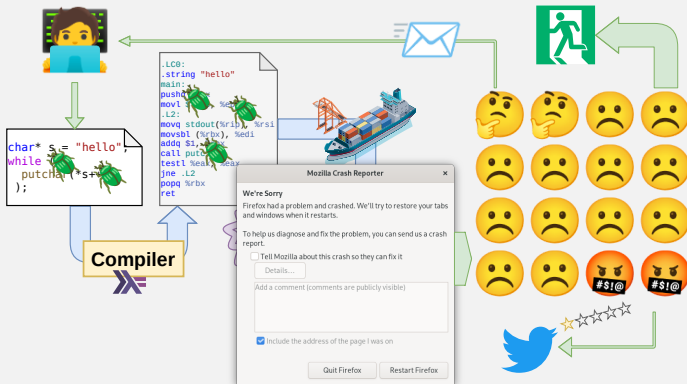
# Fewer Errors



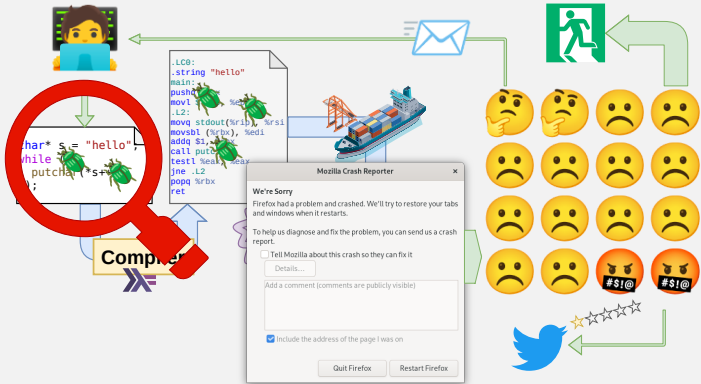
# Fewer Errors



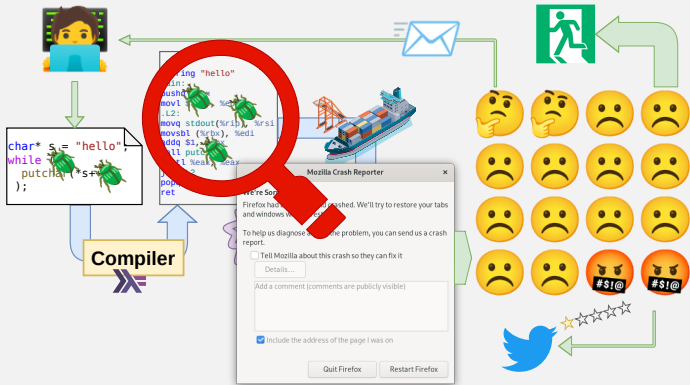
# Where to hunt for



# Where to hunt for

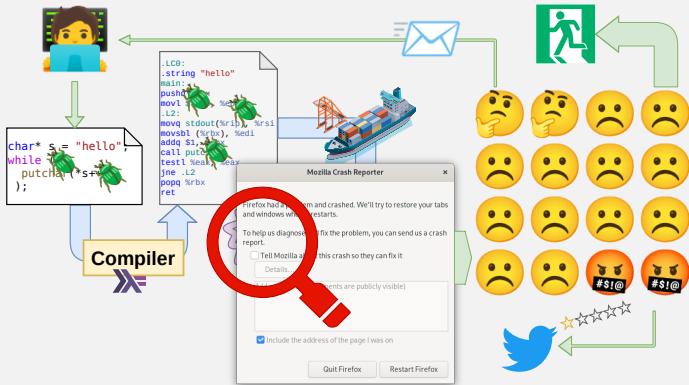


# Where to hunt for

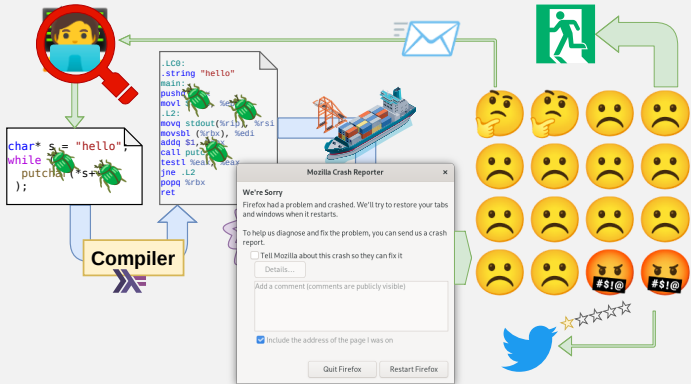




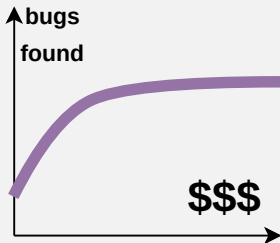
# Where to hunt for



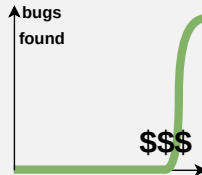
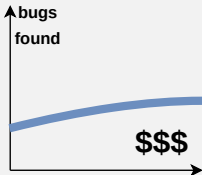
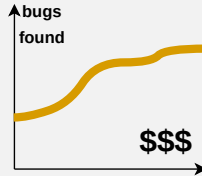
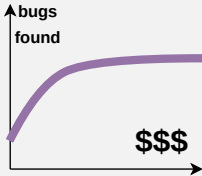
# Where to hunt for



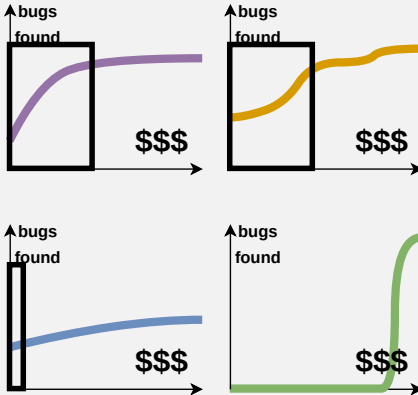
# What to choose?



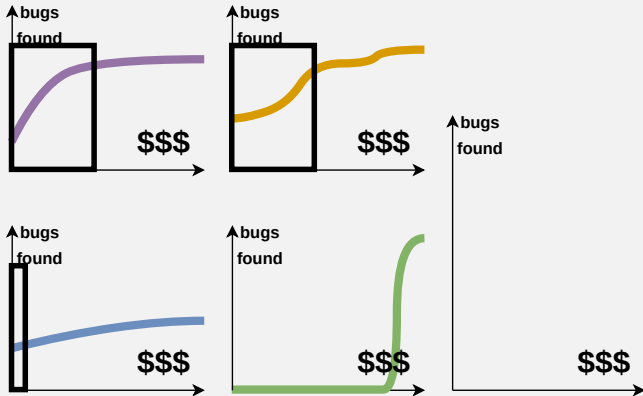
# What to choose?



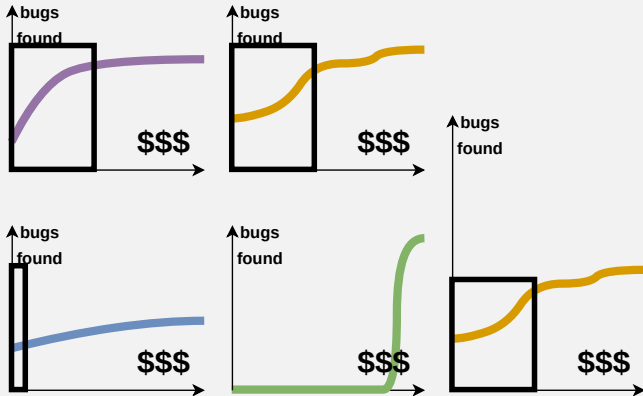
# What to choose?



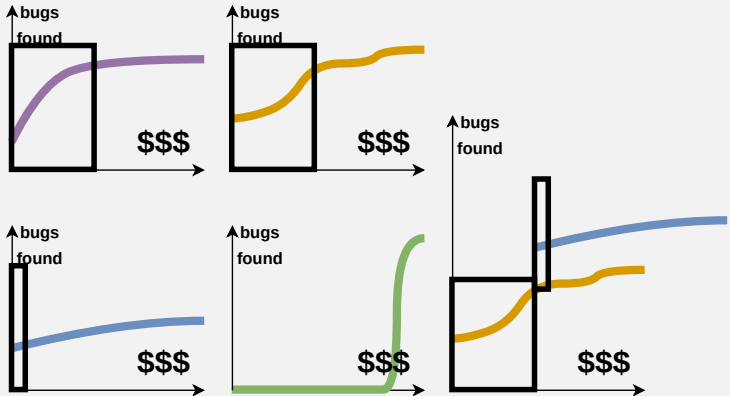
# What to choose?



# What to choose?

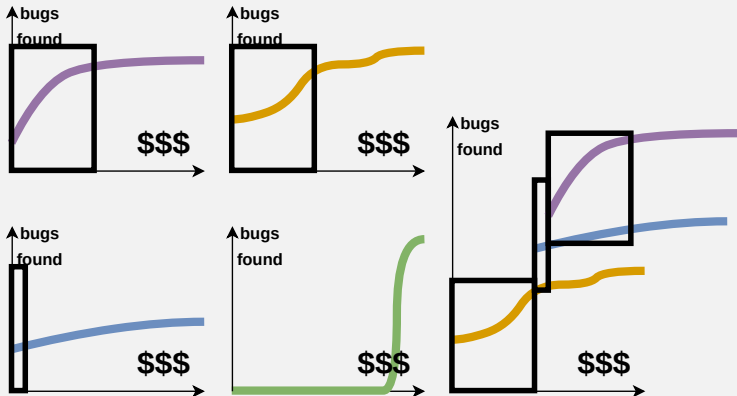


# What to choose?

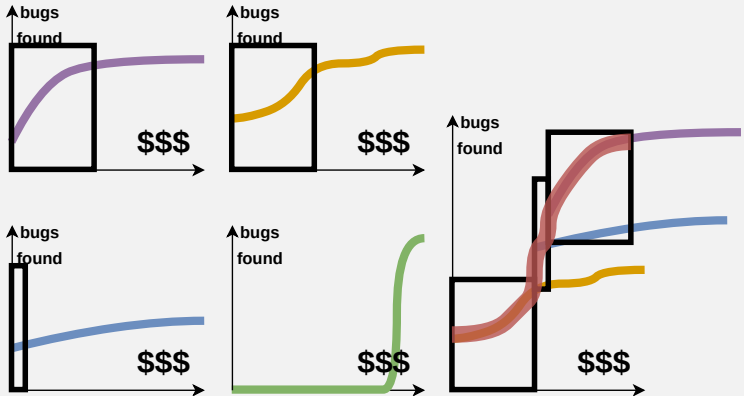




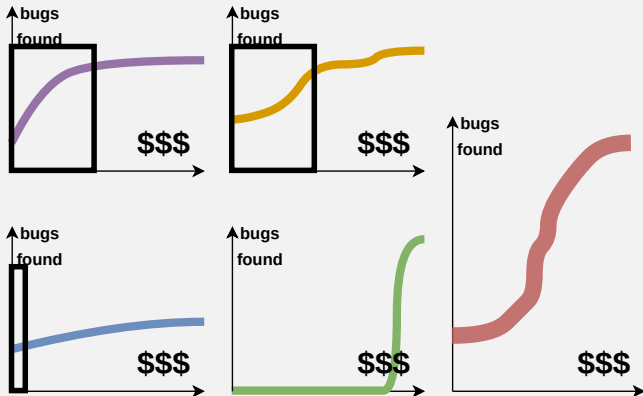
# What to choose?



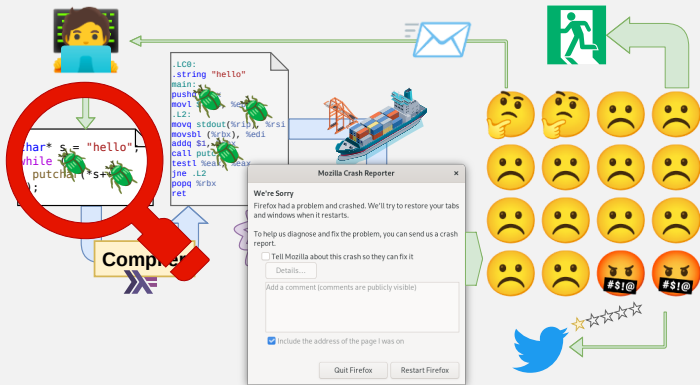
# What to choose?



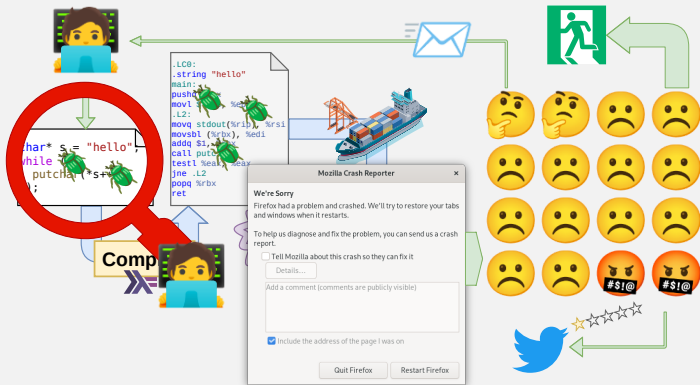
# What to choose?



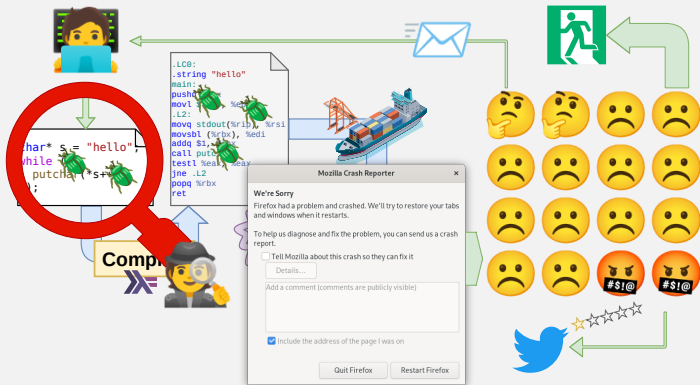
# Who hunts for ?



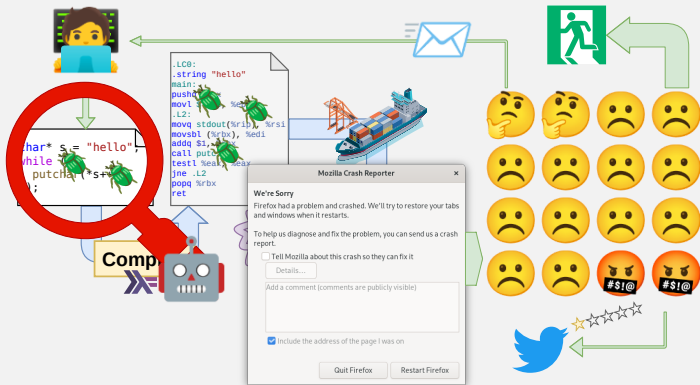
# Who hunts for ?



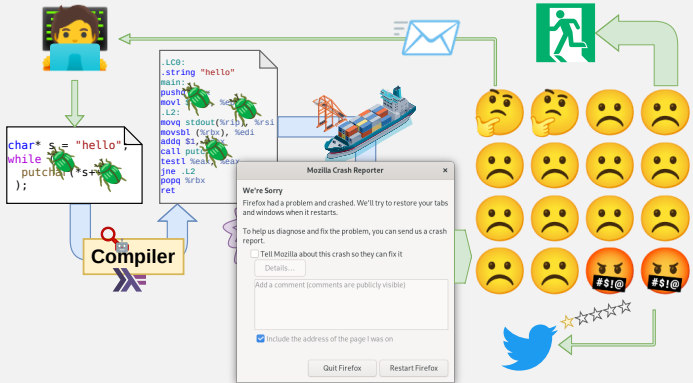
# Who hunts for ?



# Who hunts for ?

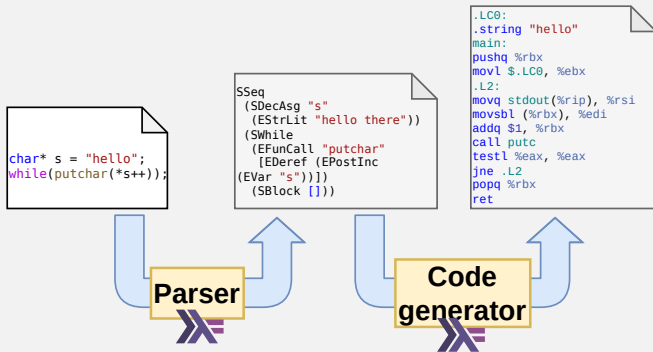


# Compiler checks

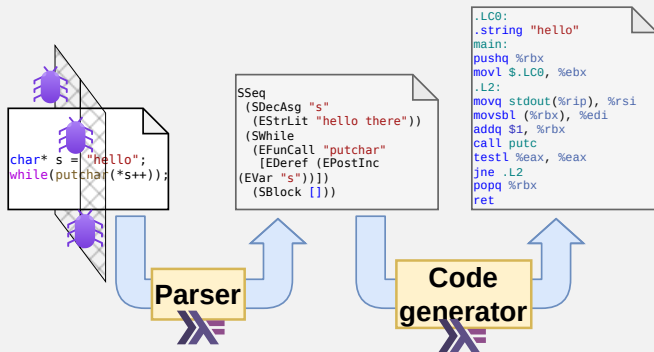




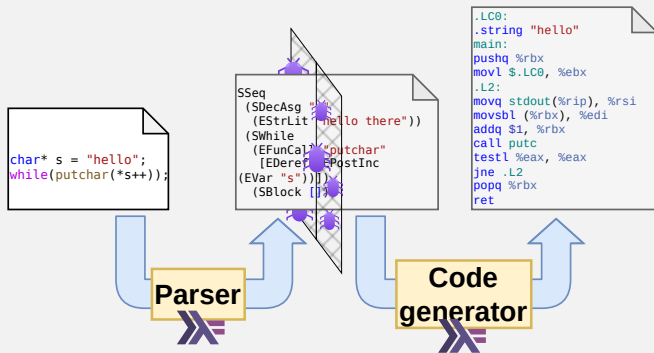
# Compiler checks, but where?



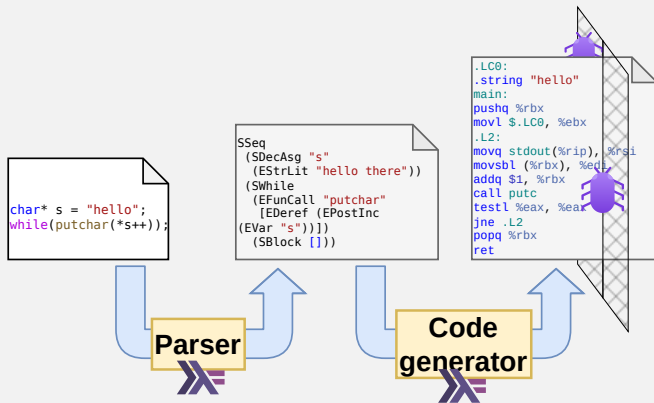
# Compiler checks, but where?



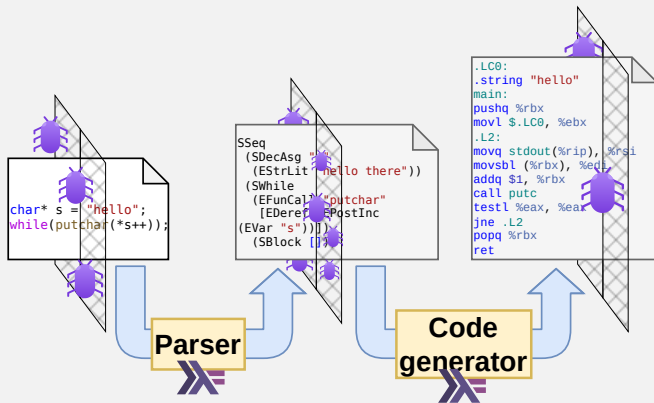
# Compiler checks, but where?



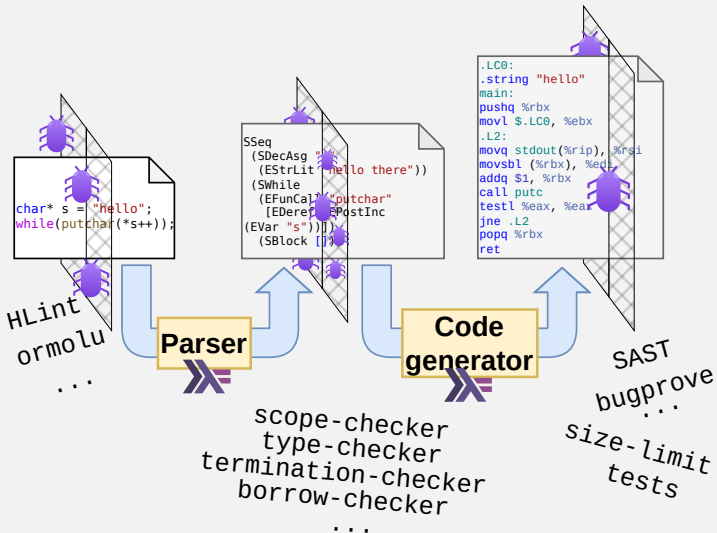
# Compiler checks, but where?



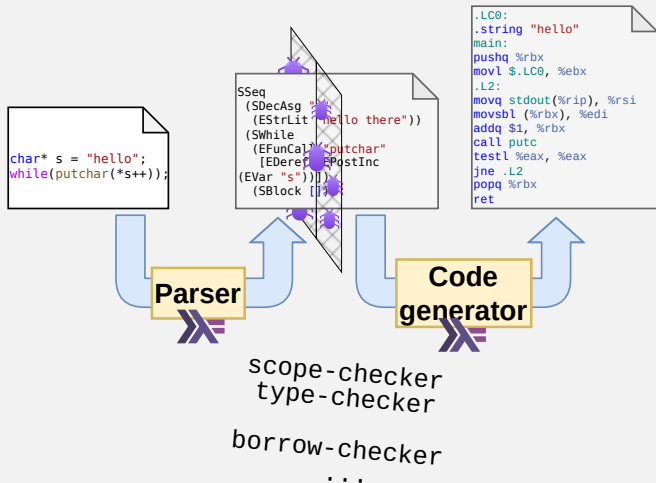
# Compiler checks, but where?



# Compiler checks, but where?



# Compiler checks, but where?



# Example

(live coding)





# Summary

```
check :: Annotation -> Exp -> Bool
```

```
infer :: Exp -> Maybe Annotation
```

```
safeXXX e = infer e >> unsafeXXX e
```



# Summary

```
check :: Annotation -> Exp -> Bool
```

```
infer :: Exp -> Maybe Annotation
```

```
safeXXX e = infer e >> unsafeXXX e
```

```
Valid a b  $\cong$  Either a b
```

```
validate :: Exp -> Valid [ErrorMsg] AnnotatedExp
```

```
safeXXX e = safeXXX' <$> validate e
```



# Summary

