# GoSonar: Detecting Logical Vulnerabilities in Memory Safe Language Using Inductive Constraint Reasoning

**Md Sakib Anwar**
anwar.40@osu.edu

Carter Yagemann
yagemann.1@osu.edu

Zhiqiang Lin
zlin@cse.ohio-state.edu

IEEE S&P 2025

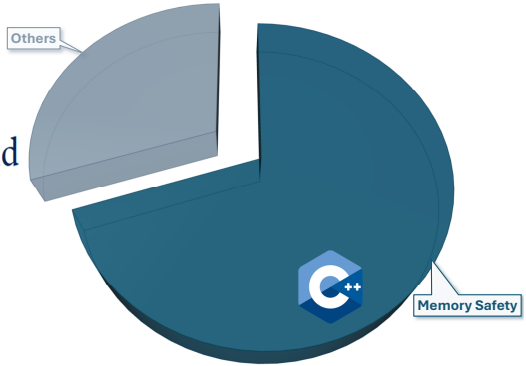

# A National Cybersecurity Imperative

FEBRUARY 26, 2024

## Press Release: Future Software Should Be Memory Safe

ONCD ▸ BRIEFING ROOM ▸ PRESS RELEASE

**Leaders in Industry Support White House Call to Address Root Cause of Many of the Worst Cyber Attacks**




**CVE Root Cause Distribution**

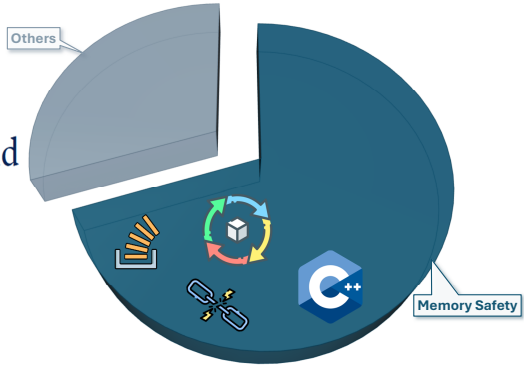
# A National Cybersecurity Imperative

FEBRUARY 26, 2024

## Press Release: Future Software Should Be Memory Safe

ONCD ▸ BRIEFING ROOM ▸ PRESS RELEASE

**Leaders in Industry Support White House Call to Address Root Cause of Many of the Worst Cyber Attacks**




**CVE Root Cause Distribution**

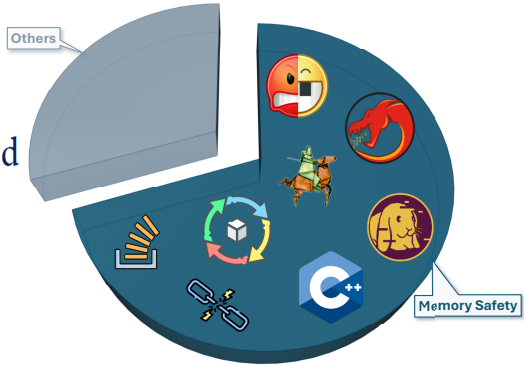
# A National Cybersecurity Imperative

FEBRUARY 26, 2024

## Press Release: Future Software Should Be Memory Safe

ONCD ▸ BRIEFING ROOM ▸ PRESS RELEASE

**Leaders in Industry Support White House Call to Address Root Cause of Many of the Worst Cyber Attacks**




**CVE Root Cause Distribution**

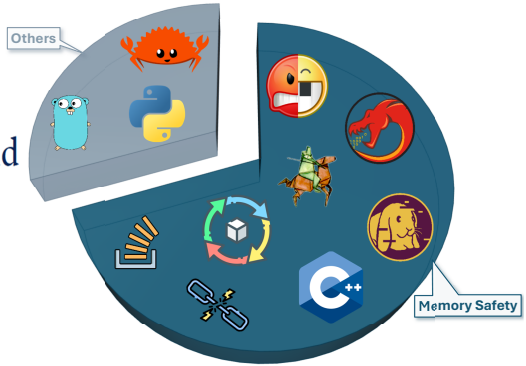
# A National Cybersecurity Imperative

FEBRUARY 26, 2024

## Press Release: Future Software Should Be Memory Safe

ONCD ▸ BRIEFING ROOM ▸ PRESS RELEASE

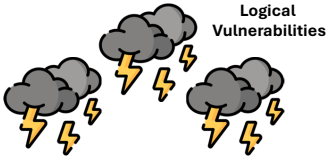
**Leaders in Industry Support White House Call to Address Root Cause of Many of the Worst Cyber Attacks**



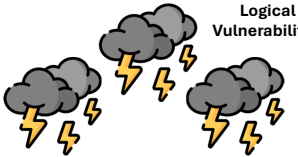

**CVE Root Cause Distribution**

# Memory Safety $\neq$ Secure

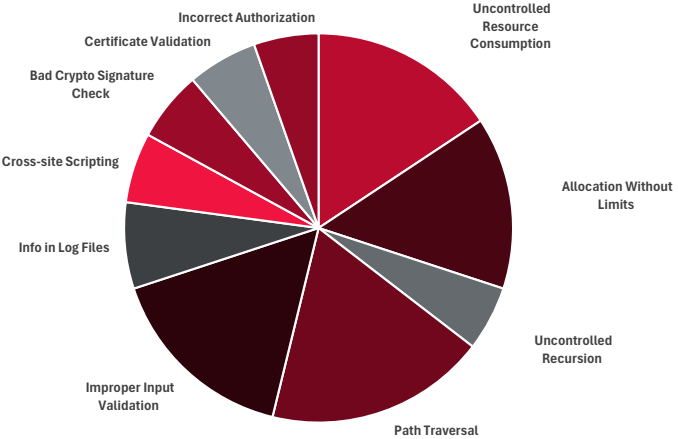
# Memory Safety $\neq$ Secure




# Memory Safety $\neq$ Secure

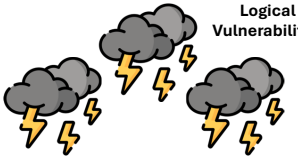




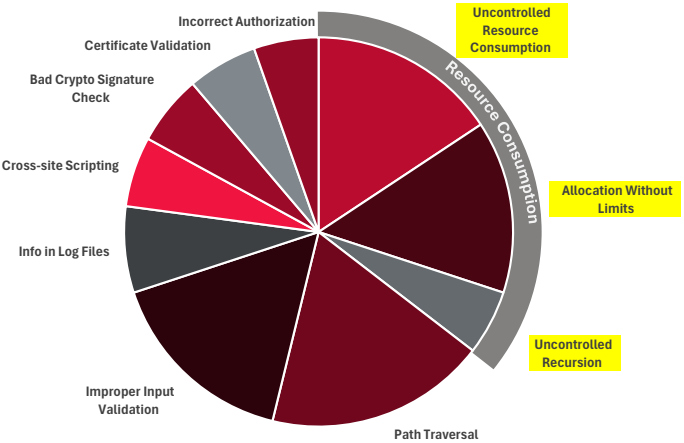



Top 10 CWE Category for Go

# Memory Safety ≠ Secure

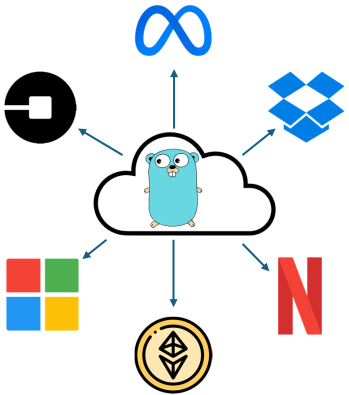




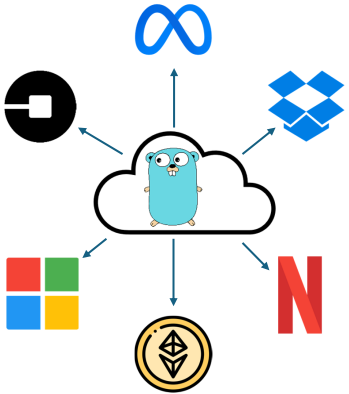



Top 10 CWE Category for Go

# Go: Backbone of Cloud Services



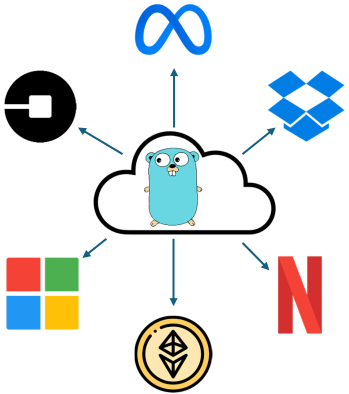
# Go: Backbone of Cloud Services



**OWASP API Security Top Vulnerabilities 2023**

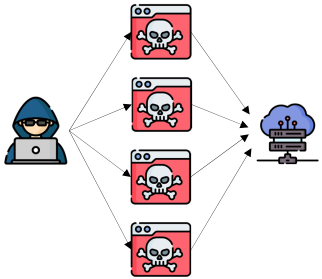
| # | Description | Exploitability | Prevalence | Impacts |
|---|---|---|---|---|
| API1 | Broken Object Level Authorization | Easy | Widespread | Moderate |
| API2 | Broken Authentication | Easy | Common | Severe |
| API3 | Broken Object Property Level Authorization | Easy | Common | Moderate |
| **API4** | **Unrestricted Resource Consumption** | **Average** | **Widespread** | **Severe** |
| API5 | Broken Function Level Authorization | Easy | Common | Severe |

# Go: Backbone of Cloud Services



**OWASP API Security Top Vulnerabilities 2023**

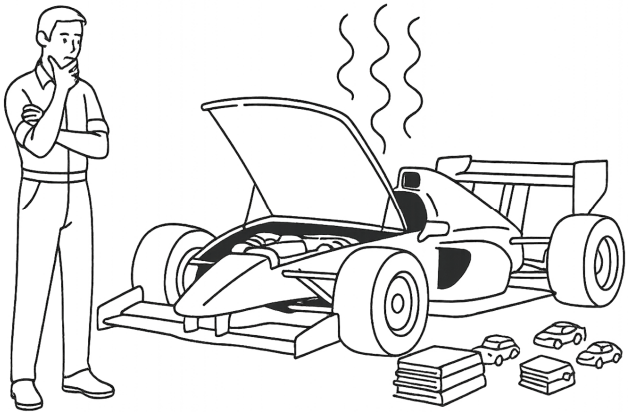
| # | Description | Exploitability | Prevalence | Impacts |
|---|---|---|---|---|
| API1 | Broken Object Level Authorization | Easy | Widespread | Moderate |
| API2 | Broken Authentication | Easy | Common | Severe |
| API3 | Broken Object Property Level Authorization | Easy | Common | Moderate |
| **API4** | **Unrestricted Resource Consumption** | **Average** | **Widespread** | **Severe** |
| API5 | Broken Function Level Authorization | Easy | Common | Severe |



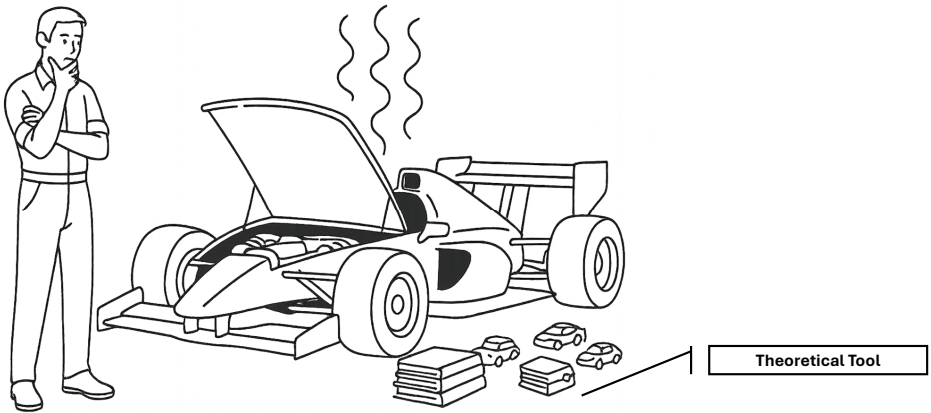
Traditional DDoS

DDoS Using Logical Vulnerabilities

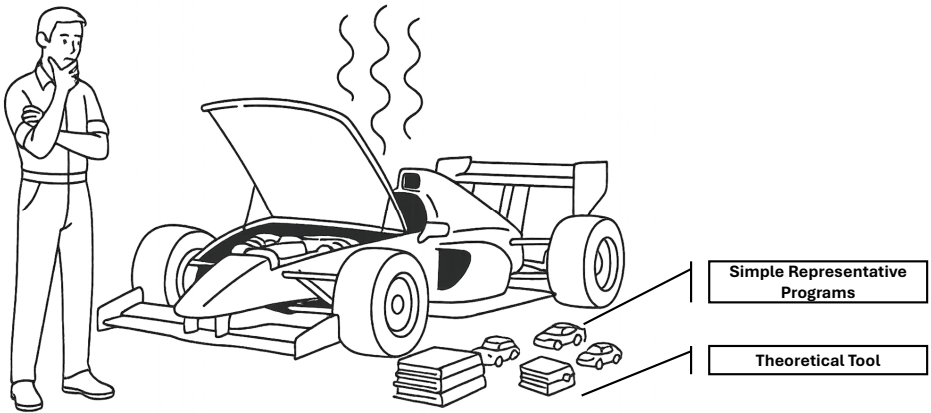
# We Solved Nontermination... Right?



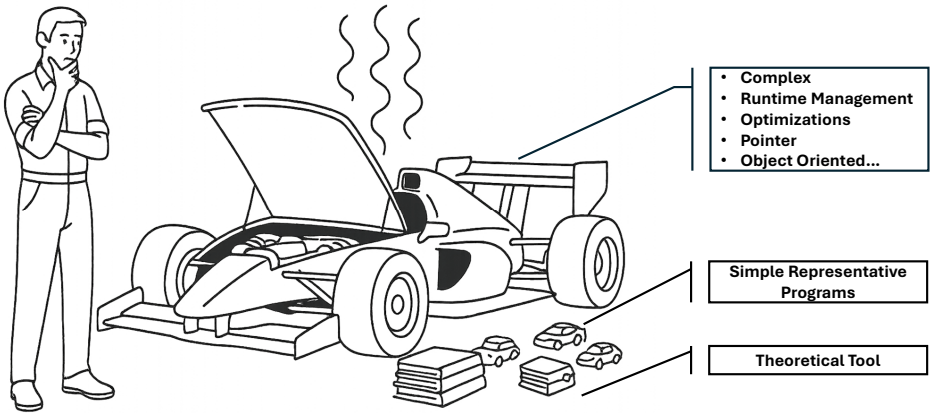
# We Solved Nontermination... Right?



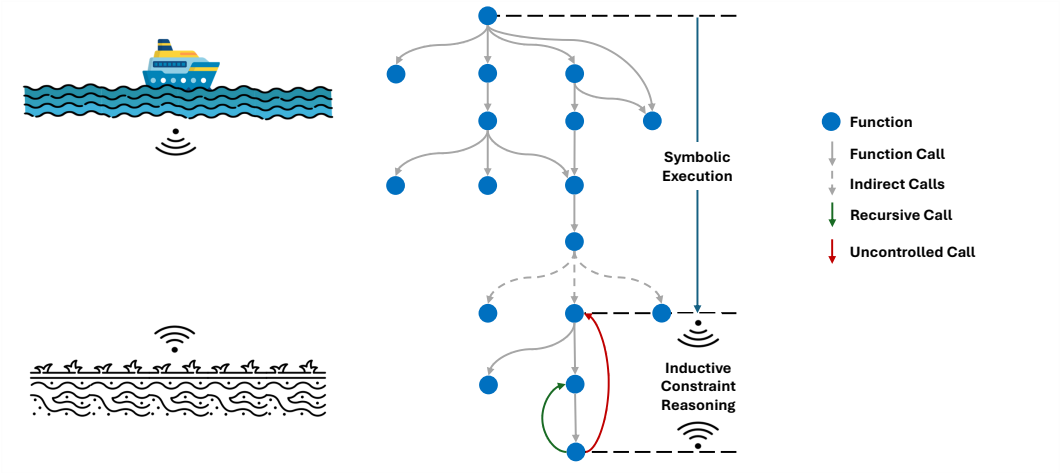
# We Solved Nontermination... Right?



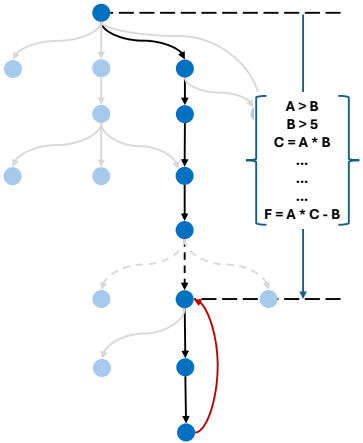
# We Solved Nontermination... Right?



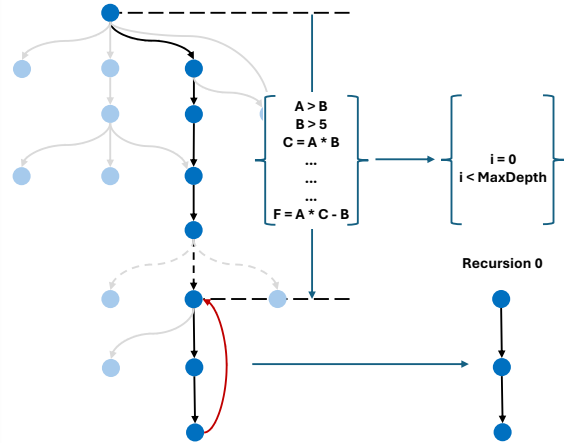
# GoSonar: Sonar for Recursion!



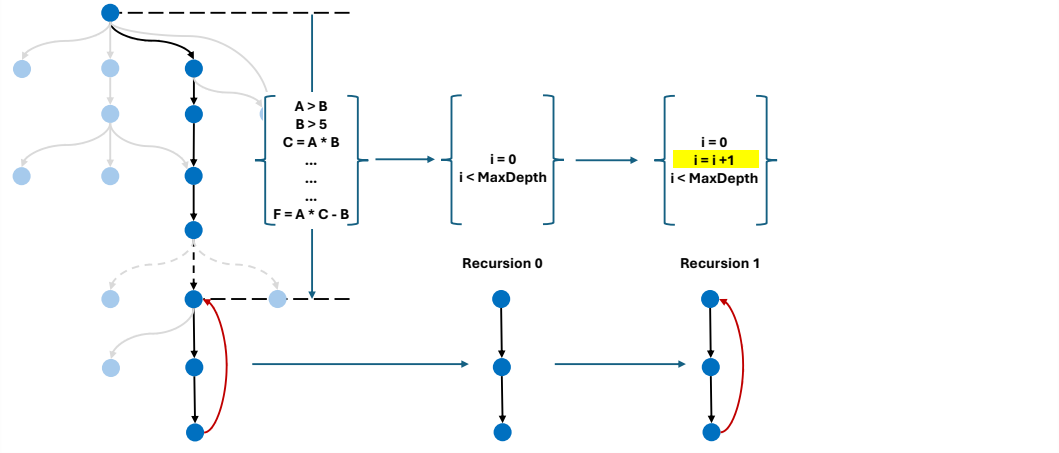
# Inductive Constraint Reasoning



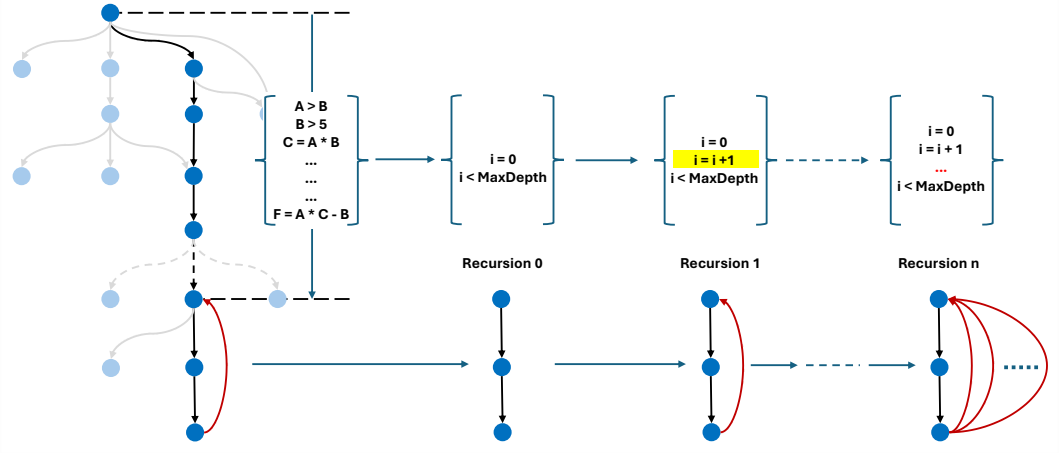
# Inductive Constraint Reasoning



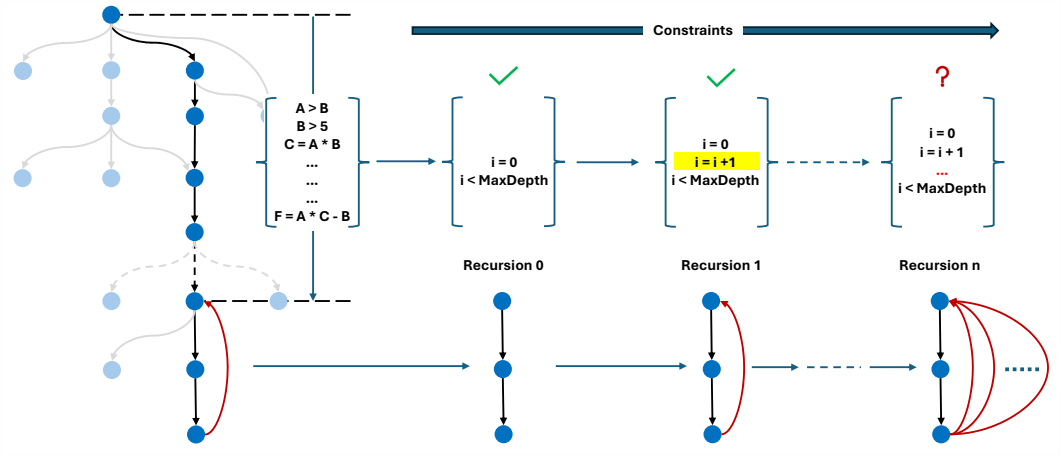
# Inductive Constraint Reasoning



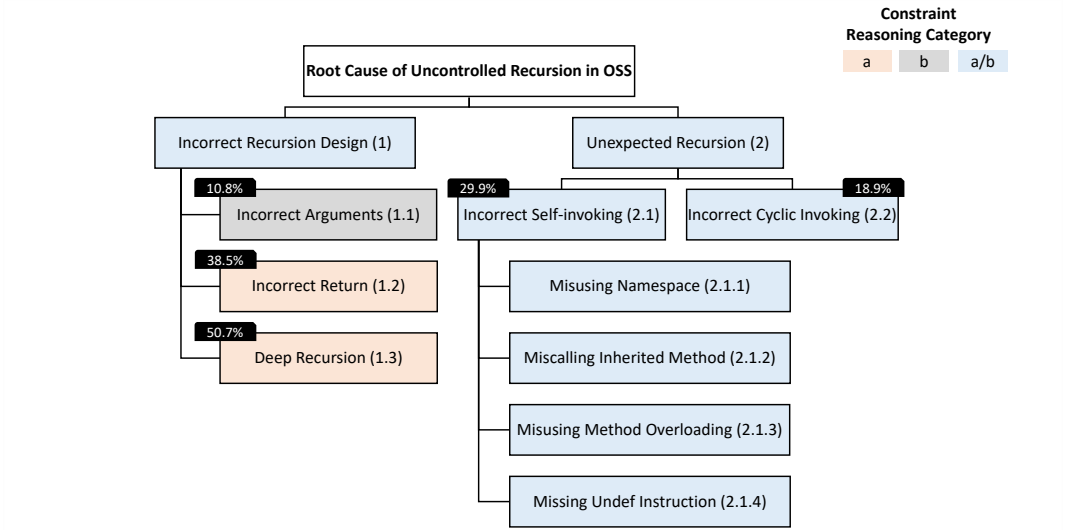
# Inductive Constraint Reasoning



# Inductive Constraint Reasoning



# Taxonomy of Uncontrolled Recursion in OSS



# Outperforming State-of-the-Art Tools

| | |
|---|---|
| **V** | **Vulnerable** |
| **P** | **Patched** |
| **✓** | **Correct Detection** |
| **UN** | **Unknonwn** |
| **E** | **Errored** |
| **?** | **Maybe** |

| Related Work | Reason |
|---|---|
| **UAutomizer** | SV-COMP (2017-2021) Winner |
| **CPAchecker** | SV-COMP (2020) 2nd Place |
| **2LS** | SV-COMP (2021) 3rd Place |
| **AProVE** | SV-COMP (2017-2019) Top 3 |
| **T2** | >> Julia, TNT |

| Root Cause | Type | UAutomizer | AProVE | CPAchecker | 2LS | T2 | GoSonar |
|---|---|---|---|---|---|---|---|
| **Incorrect Arguments (1.1)** | V | ✓ | ? | UN | E | E | ✓ |
| | P | ✓ | ? | ✓ | E | E | ✓ |
| **Incorrect Return (1.2)** | V | E | ? | UN | UN | E | ✓ |
| | P | E | ? | UN | ✓ | E | ✓ |
| **Miscalling Inherited Method (2.1.2)** | V | - | - | - | - | - | ✓ |
| | P | - | - | - | - | - | ✓ |
| **Misusing Method Overloading (2.1.3)** | V-1 | - | - | - | - | - | ✓ |
| | P-1 | - | - | - | - | - | ✓ |
| | V-2 | - | - | - | - | - | ✓ |
| | P-2 | - | - | - | - | - | ✓ |
| | V-3 | - | - | - | - | - | ✓ |
| | P-3 | - | - | - | - | - | ✓ |
| | V-4 | - | - | - | - | - | ✓ |
| | P-4 | - | - | - | - | - | ✓ |
| **Missing Undef Instruction (2.1.4)** | V | ✓ | ✓ | UN | UN | E | ✓ |
| | P | UN | ✓ | ✓ | ✓ | E | ✓ |
| **Incorrect Cyclic Invoking (2.2)** | V-1 | ✓ | ? | UN | E | E | ✓ |
| | P-1 | ✓ | ✓ | ✓ | ✓ | E | ✓ |
| | V-2 | UN | ? | UN | UN | E | ✓ |
| | P-2 | UN | ? | UN | UN | E | ✓ |

# Outperforming State-of-the-Art Tools

| | |
|---|---|
| V | Vulnerable |
| P | Patched |
| ✓ | Correct Detection |
| UN | Unknonwn |
| E | Errored |
| ? | Maybe |

| Related Work | Reason |
|---|---|
| UAutomizer | SV-COMP (2017-2021) Winner |
| CPAchecker | SV-COMP (2020) 2nd Place |
| 2LS | SV-COMP (2021) 3rd Place |
| AProVE | SV-COMP (2017-2019) Top 3 |
| T2 | >> Julia, TNT |

| Root Cause | Type | UAutomizer | AProVE | CPAchecker | 2LS | T2 | GoSonar |
|---|---|---|---|---|---|---|---|
| Incorrect Arguments (1.1) | V | ✓ | ? | UN | E | E | ✓ |
| | P | ✓ | ? | ✓ | E | E | ✓ |
| Incorrect Return (1.2) | V | E | ? | UN | UN | E | ✓ |
| | P | E | ? | UN | ✓ | E | ✓ |
| Miscalling Inherited Method (2.1.2) | V | - | - | - | - | - | ✓ |
| | P | - | - | - | - | - | ✓ |
| Misusing Method Overloading (2.1.3) | V-1 | - | - | - | - | - | ✓ |
| | P-1 | - | - | - | - | - | ✓ |
| | V-2 | - | - | - | - | - | ✓ |
| | P-2 | - | - | - | - | - | ✓ |
| | V-3 | - | - | - | - | - | ✓ |
| | P-3 | - | - | - | - | - | ✓ |
| | V-4 | - | - | - | - | - | ✓ |
| | P-4 | - | - | - | - | - | ✓ |
| Missing Undef Instruction (2.1.4) | V | ✓ | ✓ | UN | UN | E | ✓ |
| | P | UN | ✓ | ✓ | ✓ | E | ✓ |
| Incorrect Cyclic Invoking (2.2) | V-1 | ✓ | ? | UN | E | E | ✓ |
| | P-1 | ✓ | ✓ | ✓ | ✓ | E | ✓ |
| | V-2 | UN | ? | UN | UN | E | ✓ |
| | P-2 | UN | ? | UN | UN | E | ✓ |

# Outperforming State-of-the-Art Tools

| | |
|---|---|
| V | Vulnerable |
| P | Patched |
| ✓ | Correct Detection |
| UN | Unknonwn |
| E | Errored |
| ? | Maybe |

| Related Work | Reason |
|---|---|
| UAutomizer | SV-COMP (2017-2021) Winner |
| CPAchecker | SV-COMP (2020) 2nd Place |
| 2LS | SV-COMP (2021) 3rd Place |
| AProVE | SV-COMP (2017-2019) Top 3 |
| T2 | >> Julia, TNT |

| Root Cause | Type | UAutomizer | AProVE | CPAchecker | 2LS | T2 | GoSonar |
|---|---|---|---|---|---|---|---|
| Incorrect Arguments (1.1) | V | ✓ | ? | UN | E | E | ✓ |
| | P | ✓ | ? | ✓ | E | E | ✓ |
| Incorrect Return (1.2) | V | E | ? | UN | UN | E | ✓ |
| | P | E | ? | UN | ✓ | E | ✓ |
| Miscalling Inherited Method (2.1.2) | V | - | - | - | - | - | ✓ |
| | P | - | - | - | - | - | ✓ |
| Misusing Method Overloading (2.1.3) | V-1 | - | - | - | - | - | ✓ |
| | P-1 | - | - | - | - | - | ✓ |
| | V-2 | - | - | - | - | - | ✓ |
| | P-2 | - | - | - | - | - | ✓ |
| | V-3 | - | - | - | - | - | ✓ |
| | P-3 | - | - | - | - | - | ✓ |
| | V-4 | - | - | - | - | - | ✓ |
| | P-4 | - | - | - | - | - | ✓ |
| Missing Undef Instruction (2.1.4) | V | ✓ | ✓ | UN | UN | E | ✓ |
| | P | UN | ✓ | ✓ | ✓ | E | ✓ |
| Incorrect Cyclic Invoking (2.2) | V-1 | ✓ | ? | UN | E | E | ✓ |
| | P-1 | ✓ | ✓ | ✓ | ✓ | E | ✓ |
| | V-2 | UN | ? | UN | UN | E | ✓ |
| | P-2 | UN | ? | UN | UN | E | ✓ |

# Outperforming State-of-the-Art Tools

| | |
|---|---|
| **V** | **Vulnerable** |
| **P** | **Patched** |
| **✓** | **Correct Detection** |
| **UN** | **Unknonwn** |
| **E** | **Errored** |
| **?** | **Maybe** |

| Related Work | Reason |
|---|---|
| **UAutomizer** | SV-COMP (2017-2021) Winner |
| **CPAchecker** | SV-COMP (2020) 2nd Place |
| **2LS** | SV-COMP (2021) 3rd Place |
| **AProVE** | SV-COMP (2017-2019) Top 3 |
| **T2** | >> Julia, TNT |

| Root Cause | Type | UAutomizer | AProVE | CPAchecker | 2LS | T2 | GoSonar |
|---|---|---|---|---|---|---|---|
| **Incorrect Arguments (1.1)** | V | ✓ | ? | UN | E | E | ✓ |
| | P | ✓ | ? | ✓ | E | E | ✓ |
| **Incorrect Return (1.2)** | V | E | ? | UN | UN | E | ✓ |
| | P | E | ? | UN | ✓ | E | ✓ |
| **Miscalling Inherited Method (2.1.2)** | V | - | - | - | - | - | ✓ |
| | P | - | - | - | - | - | ✓ |
| **Misusing Method Overloading (2.1.3)** | V-1 | - | - | - | - | - | ✓ |
| | P-1 | - | - | - | - | - | ✓ |
| | V-2 | - | - | - | - | - | ✓ |
| | P-2 | - | - | - | - | - | ✓ |
| | V-3 | - | - | - | - | - | ✓ |
| | P-3 | - | - | - | - | - | ✓ |
| | V-4 | - | - | - | - | - | ✓ |
| | P-4 | - | - | - | - | - | ✓ |
| **Missing Undef Instruction (2.1.4)** | V | ✓ | ✓ | UN | UN | E | ✓ |
| | P | UN | ✓ | ✓ | ✓ | E | ✓ |
| **Incorrect Cyclic Invoking (2.2)** | V-1 | ✓ | ? | UN | E | E | ✓ |
| | P-1 | ✓ | ✓ | ✓ | ✓ | E | ✓ |
| | V-2 | UN | ? | UN | UN | E | ✓ |
| | P-2 | UN | ? | UN | UN | E | ✓ |

# Outperforming State-of-the-Art Tools

| | |
|---|---|
| **V** | **Vulnerable** |
| **P** | **Patched** |
| ✓ | **Correct Detection** |
| **UN** | **Unknonwn** |
| **E** | **Errored** |
| **?** | **Maybe** |

| Related Work | Reason |
|---|---|
| **UAutomizer** | SV-COMP (2017-2021) Winner |
| **CPAchecker** | SV-COMP (2020) 2nd Place |
| **2LS** | SV-COMP (2021) 3rd Place |
| **AProVE** | SV-COMP (2017-2019) Top 3 |
| **T2** | >> Julia, TNT |

| Root Cause | Type | UAutomizer | AProVE | CPAchecker | 2LS | T2 | GoSonar |
|---|---|---|---|---|---|---|---|
| **Incorrect Arguments (1.1)** | V | ✓ | ? | UN | E | E | ✓ |
| | P | ✓ | ? | ✓ | E | E | ✓ |
| **Incorrect Return (1.2)** | V | E | ? | UN | UN | E | ✓ |
| | P | E | ? | UN | ✓ | E | ✓ |
| **Miscalling Inherited Method (2.1.2)** | V | - | - | - | - | - | ✓ |
| | P | - | - | - | - | - | ✓ |
| **Misusing Method Overloading (2.1.3)** | V-1 | - | - | - | - | - | ✓ |
| | P-1 | - | - | - | - | - | ✓ |
| | V-2 | - | - | - | - | - | ✓ |
| | P-2 | - | - | - | - | - | ✓ |
| | V-3 | - | - | - | - | - | ✓ |
| | P-3 | - | - | - | - | - | ✓ |
| | V-4 | - | - | - | - | - | ✓ |
| | P-4 | - | - | - | - | - | ✓ |
| **Missing Undef Instruction (2.1.4)** | V | ✓ | ✓ | UN | UN | E | ✓ |
| | P | UN | ✓ | ✓ | ✓ | E | ✓ |
| **Incorrect Cyclic Invoking (2.2)** | V-1 | ✓ | ? | UN | E | E | ✓ |
| | P-1 | ✓ | ✓ | ✓ | ✓ | E | ✓ |
| | V-2 | UN | ? | UN | UN | E | ✓ |
| | P-2 | UN | ? | UN | UN | E | ✓ |

# Bugs in Go's Standard Library

| Package | Func. Name (s) | # of Func. Recur. | # of Func. Stem | Execution Time w/o Path Guidance | Execution Time w/ Path Guidance | Verified? | New? |
|---|---|---|---|---|---|---|---|
| **compress** | glob/Reader.Read | 1 | 1 | - | 1.01 | ✓ | ✗ |
| **encoding** | binary.sizeof | 1 | 3 | - | 12.18 | ✓ | ✓ |
| **go** | filterExprList | 2 | 5 | 465.35 | 357.36 | ✓ | ✓ |
| | | | 4 | 117.51 | 46.68 | ✓ | ✓ |
| | | | 4 | 17.98 | 26.38 | ✓ | ✓ |
| | | | 3 | 26.79 | 8.72 | ✓ | ✓ |
| | | | 4 | 36.79 | 18.83 | ✓ | ✓ |
| | Sign | 1 | 1 | 69.1 | 62.38 | ✗ | - |
| | appendReverse | 1 | 3 | 35.04 | 24.23 | ✓ | ✓ |
| | | | 3 | 1.62 | 1.49 | ✓ | ✓ |
| | | | 3 | 1.32 | 1.4 | ✓ | ✓ |
| **math** | mulRange | 1 | 2 | 2.18 | 1.06 | ✓ | ✓ |
| | | | 3 | 30.62 | 29.75 | ✓ | ✓ |
| **path** | Glob | 1 | 1 | 33.18 | 41.97 | ✓ | ✗ |
| **text** | IsEmptyTree | 1 | 1 | 1.45 | 1.4 | ✓ | ✓ |
| **Total** | **8** | **9** | **41** | **838.92** | **634.83** | **14** | **12** |
| **Average** | | | | **64.53** | **42.32** | | |

# Bugs in Go's Standard Library

| | | # of Func. | | Execution Time | | | |
|---|---|---|---|---|---|---|---|
| **Package** | **Func. Name (s)** | **Recur.** | **Stem** | **w/o Path Guidance** | **w/ Path Guidance** | **Verified?** | **New?** |
| **compress** | glob/Reader.Read | 1 | 1 | - | 1.01 | ✓ | ✗ |
| **encoding** | binary.sizeof | 1 | 3 | - | 12.18 | ✓ | ✓ |
| **go** | filterExprList | 2 | 5 | 465.35 | 357.36 | ✓ | ✓ |
| | | | 4 | 117.51 | 46.68 | ✓ | ✓ |
| | | | 4 | 17.98 | 26.38 | ✓ | ✓ |
| | | | 3 | 26.79 | 8.72 | ✓ | ✓ |
| | | | 4 | 36.79 | 18.83 | ✓ | ✓ |
| | Sign | 1 | 1 | 69.1 | 62.38 | ✗ | - |
| | appendReverse | 1 | 3 | 35.04 | 24.23 | ✓ | ✓ |
| | | | 3 | 1.62 | 1.49 | ✓ | ✓ |
| | | | 3 | 1.32 | 1.4 | ✓ | ✓ |
| **math** | mulRange | 1 | 2 | 2.18 | 1.06 | ✓ | ✓ |
| | | | 3 | 30.62 | 29.75 | ✓ | ✓ |
| **path** | Glob | 1 | 1 | 33.18 | 41.97 | ✓ | ✗ |
| **text** | IsEmptyTree | 1 | 1 | 1.45 | 1.4 | ✓ | ✓ |
| **Total** | **8** | **9** | **41** | **838.92** | **634.83** | **14** | **12** |
| **Average** | | | | **64.53** | **42.32** | | |

# Bugs in Go's Standard Library

| Package | Func. Name (s) | # of Func. Recur. | # of Func. Stem | Execution Time w/o Path Guidance | Execution Time w/ Path Guidance | Verified? | New? |
|---|---|---|---|---|---|---|---|
| **compress** | glob/Reader.Read | 1 | 1 | - | 1.01 | ✓ | ✗ |
| **encoding** | binary.sizeof | 1 | 3 | - | 12.18 | ✓ | ✓ |
| **go** | filterExprList | 2 | 5 | 465.35 | 357.36 | ✓ | ✓ |
| | | | 4 | 117.51 | 46.68 | ✓ | ✓ |
| | | | 4 | 17.98 | 26.38 | ✓ | ✓ |
| | | | 3 | 26.79 | 8.72 | ✓ | ✓ |
| | | | 4 | 36.79 | 18.83 | ✓ | ✓ |
| | Sign | 1 | 1 | 69.1 | 62.38 | ✗ | - |
| | appendReverse | 1 | 3 | 35.04 | 24.23 | ✓ | ✓ |
| | | | 3 | 1.62 | 1.49 | ✓ | ✓ |
| | | | 3 | 1.32 | 1.4 | ✓ | ✓ |
| **math** | mulRange | 1 | 2 | 2.18 | 1.06 | ✓ | ✓ |
| | | | 3 | 30.62 | 29.75 | ✓ | ✓ |
| **path** | Glob | 1 | 1 | 33.18 | 41.97 | ✓ | ✗ |
| **text** | IsEmptyTree | 1 | 1 | 1.45 | 1.4 | ✓ | ✓ |
| **Total** | **8** | **9** | **41** | **838.92** | **634.83** | **14** | **12** |
| **Average** | | | | **64.53** | **42.32** | | |

# Bugs in Go's Standard Library

| Package | Func. Name (s) | # of Func. Recur. | # of Func. Stem | Execution Time w/o Path Guidance | Execution Time w/ Path Guidance | Verified? | New? |
|---|---|---|---|---|---|---|---|
| **compress** | glob/Reader.Read | 1 | 1 | - | 1.01 | ✓ | ✗ |
| **encoding** | binary.sizeof | 1 | 3 | - | 12.18 | ✓ | ✓ |
| **go** | filterExprList | 2 | 5 | 465.35 | 357.36 | ✓ | ✓ |
| | | | 4 | 117.51 | 46.68 | ✓ | ✓ |
| | | | 4 | 17.98 | 26.38 | ✓ | ✓ |
| | | | 3 | 26.79 | 8.72 | ✓ | ✓ |
| | | | 4 | 36.79 | 18.83 | ✓ | ✓ |
| | Sign | 1 | 1 | 69.1 | 62.38 | ✗ | - |
| | appendReverse | 1 | 3 | 35.04 | 24.23 | ✓ | ✓ |
| | | | 3 | 1.62 | 1.49 | ✓ | ✓ |
| | | | 3 | 1.32 | 1.4 | ✓ | ✓ |
| **math** | mulRange | 1 | 2 | 2.18 | 1.06 | ✓ | ✓ |
| | | | 3 | 30.62 | 29.75 | ✓ | ✓ |
| **path** | Glob | 1 | 1 | 33.18 | 41.97 | ✓ | ✗ |
| **text** | IsEmptyTree | 1 | 1 | 1.45 | 1.4 | ✓ | ✓ |
| **Total** | **8** | **9** | **41** | **838.92** | **634.83** | **14** | **12** |
| **Average** | | | | **64.53** | **42.32** | | |

# Bugs in Go's Standard Library

| Package | Func. Name (s) | # of Func. Recur. | # of Func. Stem | Execution Time w/o Path Guidance | Execution Time w/ Path Guidance | Verified? | New? |
|---|---|---|---|---|---|---|---|
| **compress** | glob/Reader.Read | 1 | 1 | - | 1.01 | ✓ | ✗ |
| **encoding** | binary.sizeof | 1 | 3 | - | 12.18 | ✓ | ✓ |
| **go** | filterExprList | 2 | 5 | 465.35 | 357.36 | ✓ | ✓ |
| | | | 4 | 117.51 | 46.68 | ✓ | ✓ |
| | | | 4 | 17.98 | 26.38 | ✓ | ✓ |
| | | | 3 | 26.79 | 8.72 | ✓ | ✓ |
| | | | 4 | 36.79 | 18.83 | ✓ | ✓ |
| | Sign | 1 | 1 | 69.1 | 62.38 | ✗ | - |
| | appendReverse | 1 | 3 | 35.04 | 24.23 | ✓ | ✓ |
| | | | 3 | 1.62 | 1.49 | ✓ | ✓ |
| | | | 3 | 1.32 | 1.4 | ✓ | ✓ |
| **math** | mulRange | 1 | 2 | 2.18 | 1.06 | ✓ | ✓ |
| | | | 3 | 30.62 | 29.75 | ✓ | ✓ |
| **path** | Glob | 1 | 1 | 33.18 | 41.97 | ✓ | ✗ |
| **text** | IsEmptyTree | 1 | 1 | 1.45 | 1.4 | ✓ | ✓ |
| **Total** | **8** | **9** | **41** | **838.92** | **634.83** | **14** | **12** |
| **Average** | | | | **64.53** | **42.32** | | |

# Thank You – Try GoSonar!

- ONCD Press Release : https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/02/26/press-release-technical-report/
- Taxonomy of Uncontrolled Recursion in OSS : Xiuhan Shi, Xiaofei Xie, Yi Li, Yao Zhang, Sen Chen, and Xiaohong Li. 2022. Large-scale analysis of non-termination bugs in real-world OSS projects.
- Icons made by Freepik from www.flaticon.com