



WebSVF



Static Analysis Leveraging SVF and CodeGPT

UNSW | Software Engineering | T2 2025 | Christian Tolentino and Joshua Wills

Supervisor: Yulei Sui
Assessor: Yuekang Li

Overview

1. Project Summary
 - a. Problem Statement
 - b. General Context
 - c. Revised Timeline
2. Joshua's Improvements
 - a. Import/Export Functionality
 - b. Software Clean Up
 - c. Multi File Support
3. Christian's Improvements
 - a. SVF Python Backend Conversion
 - b. General UI Improvements
4. Future Work

Problem Statement

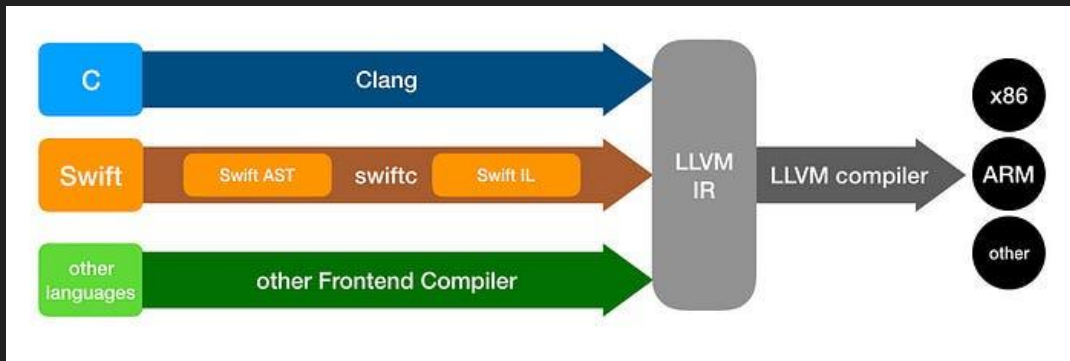
There is a significant problem in modern software development relating to the identification of bugs and security risks in large, complicated applications. As the complexity of such applications grows, the difficulty of identifying such issues worsens. The goal of WebSVF, including CodeGPT, is to provide a simple interface for users to easily identify such bugs and security risks. This is achieved by leveraging SVF, the Static Value-Flow Analysis Framework, and modern LLMs to assist in the detection of vulnerabilities, generate graphs of code structure and explain blocks of software.

General Context | Static Analysis

- Compiling and abstractly executing a program without running it
- Gain understand of software project's internal structure
- Identify common programming errors
 - Memory leaks
 - Buffer overflows
 - Null pointer dereference
 - etc.

General Context | LLVM

- Short for 'Low Level Virtual Machine'
- A compiler framework, establishing a low-level, platform-generic IR
- IR written in Single Static Assignment (SSA) form.
- SVF operates on LLVM bitcode, enabling multi language support.



General Context | SVF

- Static Value-Flow Analysis Framework
- “Source code analysis tool that enables interprocedural dependence analysis for LLVM-based languages.”



General Context | WebSVF

The screenshot displays the WebSVF web interface, which is used for analyzing code with WebSlices. The interface is divided into two main sections: a code editor on the left and a visualization area on the right.

Code Editor (Left):

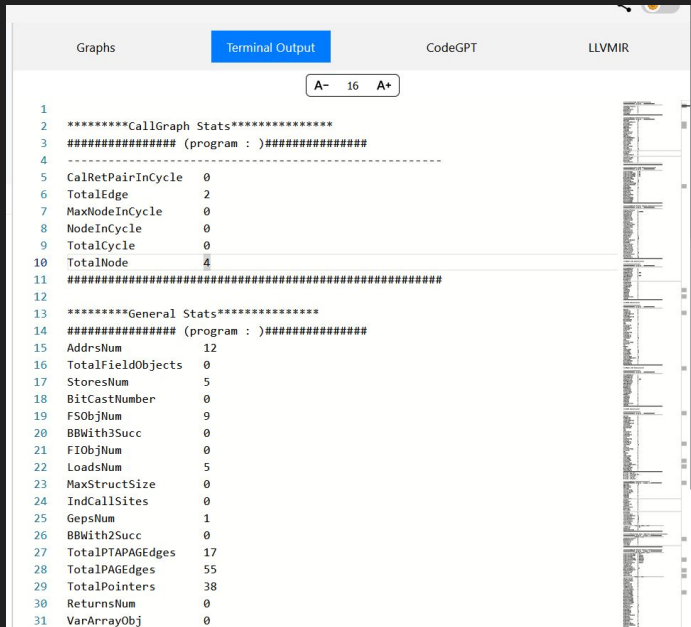
- Compile Options:** A text input field containing `-g -c -S -fno-discard-value-names -emit-llvm`. Buttons for `RESET` and `RUN` are present.
- Select executable options:** A dropdown menu currently showing `Select...`.
- Code Snippet:**

```
1 #include <stdio.h>
2
3 void assign(int *a, int *b) {
4     *a = *b;
5 }
6
7 int main(void) {
8     int a = 2, b = 3;
9
10    assign(&a, &b);
11    printf("a = %d, b = %d\n", a, b);
12 }
```

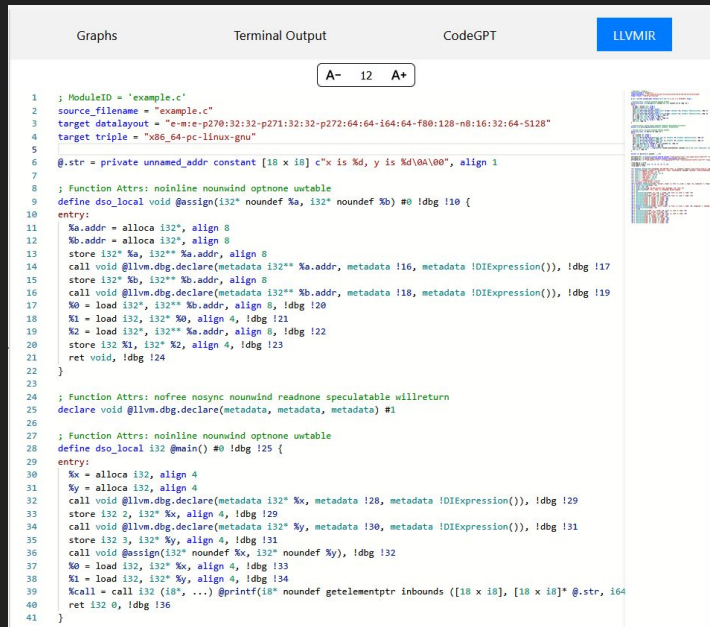
Visualization Area (Right):

- Navigation Tabs:** `Graphs` (selected), `Terminal Output`, `CodeGPT`, and `LLVMIR`.
- Call Graph:** A diagram showing the relationships between function calls. The root node is `{CallGraphNode ID: 2 {fun: main}; {<s0>1|<s1>2}}`. It has two children: `CallGraphNode ID: 3 {fun: printf}` and `{CallGraphNode ID: 0 {fun: assign}}`. A separate node `CallGraphNode ID: 1 {fun: llvm.dbg.declare}` is also shown. The label `Call Graph` is centered below the nodes.

Context | WebSVF

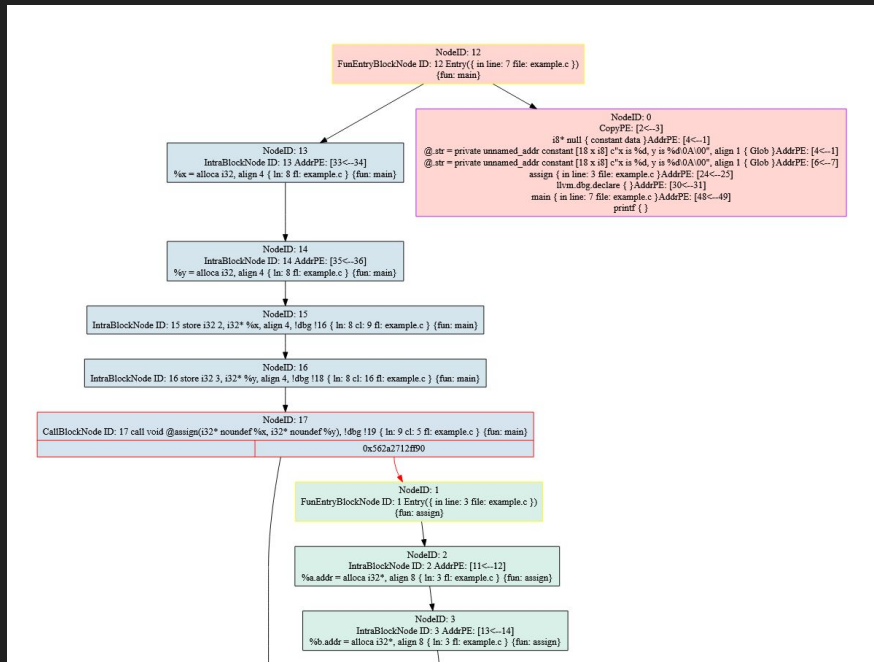


Example of the terminal output



Example of the LLVM IR output

Context | WebSVF



Example of an Interprocedural Control Flow Graph (ICFG)

Enter your compile options:

Select executable options:

[RESET](#) [RUN](#)

```
1 #include <std
2 #include <std
3
4 int main(void
5     int *x = malloc(sizeof(int) * 100);
6     x[0] = 100;
7
8 }
```

MEMORY LEAK: [1;33m NeverFree :[1;0m memory allocation at : ({ ln: 5 cl: 14 fl: example.c }) c

MEMORY LEAK: [1;33m NeverFree :[1;0m memory allocation at : (CallICFGNode: { "ln": 5, "cl": 14, "fl": "example.c" }) c

[View Problem \(Alt+F8\)](#) [Quick Fix... \(Ctrl+.\)](#)

SABER executable identifying a memory leak

Revised Timeline | Josh

Thesis B

- Continuous cycle of development, reaffirming ideas with stakeholders
- Import/Export functionality
- Code clean up and automated linting
- Adding IDE-like support

Thesis C

- Further work on the IDE-like experience
- Adding support for Rust/C++
- Integrating more executables/graph options
- Various small UI improvements

Revised Timeline | Christian

Thesis B

- Convert WebSVF Backend to use SVF-Python
- Revamp and redesign UI, fix bugs and performance, improve dark-mode and enhance user accessibility

Thesis C

- Onboarding guide for new users
- Support keybindings for an IDE-like experience
- Provide more clarity on terminal output, LLVM through tooltips and informative modals
- Analyse effectiveness of new features on user engagement, understanding and retention

Josh's Improvements

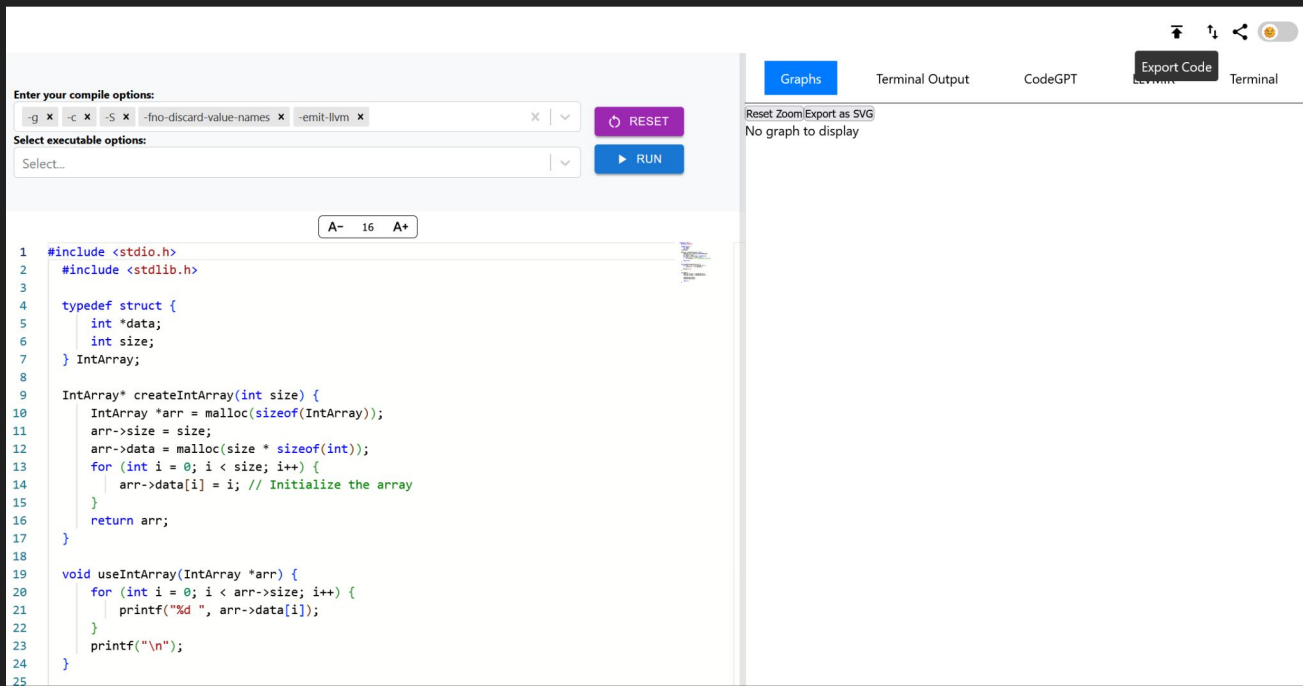
Import/Export Code

- **Why it was done:**

- Easy ability to load/store coding projects between a user's browser and their local file system
- Easy integration into a user's existing workflow
- Able to apply local file versioning/memory redundancy not possible in the browser.
- Make WebSVF more like an IDE
 - Increase user-base => greater UX and more OSS contributions

Import/Export Code

- What was done:



Import/Export buttons added to the WebSVF navbar

Import/Export Code

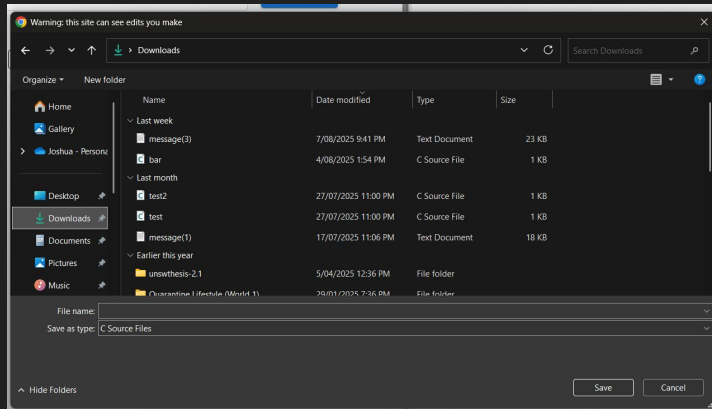
Browser compatibility

[Report problems with this compatibility data](#) • [View data on GitHub](#)

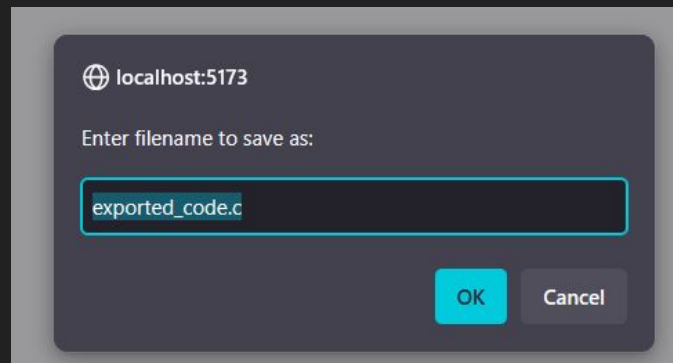
	Desktop					Mobile							Total
	Chrome	Edge	Firefox	Opera	Safari	Chrome Android	Firefox for Android	Opera Android	Safari on iOS	Samsung Internet	WebView Android	WebView on iOS	
<code>showSaveFilePicker</code> 🧪	✓ 86	✓ 86	✗ No	✓ 72	✗ No	✓ 132	✗ No	✓ 87	✗ No	✗ No	✓ 132	✗ No	✗ No

Tip: you can click/tap on a cell for more information.

✓ Full support ✗ No support 🧪 Experimental. Expect behavior to change in the future.



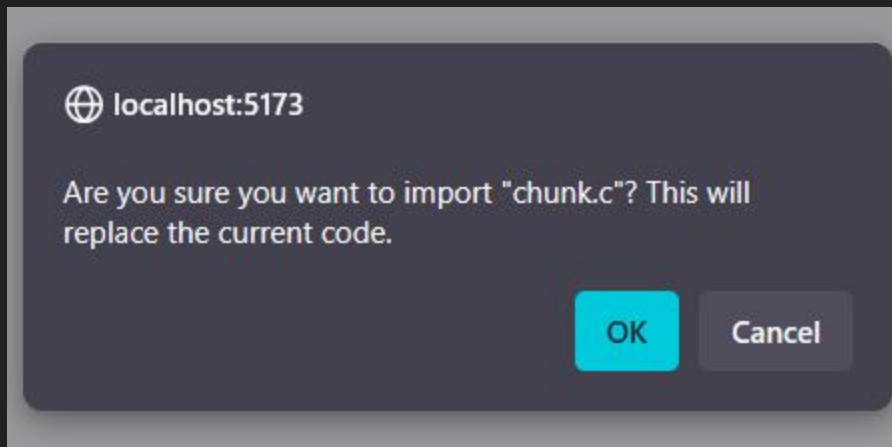
Supported browser (Chrome)



Unsupported browser (Firefox)

MDN Web Docs re. `showSaveFilePicker()` (Aug 2025)

Import/Export Code



Browser warning before import

Software Clean Up

feat: cleaning up code, automated linting #8

[Open](#) joshuawills wants to merge 6 commits into [AditiSachan:main](#) from [joshuawills:code-cleanup](#)

Conversation 1 Commits 6 Checks 0 Files changed 48 +349 -1,008

joshuawills commented last week

No description provided.

joshuawills added 6 commits 3 weeks ago

- feat: adding import/export button functionality 62b9fd4
- Merge branch 'main' into import-export-functionality fd42fa
- feat: applying prettier rules 61b364e
- feat: some eslint fixes 8cf9330
- feat: removing unnecessary things 78e3f71
- feat: automated linting/prettier ca56727

Reviewers

No reviews

Still in progress? [Convert to draft](#)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

PR adding in cleaned up code

Software Clean Up

```
Code Blame 35 lines (27 loc) · 711 Bytes

1  name: Lint and Format Check
2
3  on:
4    push:
5      branches: [ main ]
6    pull_request:
7      branches: [ main ]
8
9  jobs:
10   lint-format:
11     runs-on: ubuntu-latest
12
13     steps:
14       - name: Checkout repository
15         uses: actions/checkout@v4
16
17       - name: Set up Node.js
18         uses: actions/setup-node@v4
19         with:
20           node-version: 18
21           cache: npm
22           cache-dependency-path: frontend/package-lock.json
23
24       - name: Install dependencies
25         run: npm ci
26         working-directory: frontend
27
28       - name: Run Prettier check
29         run: npm run format:check
30         working-directory: frontend
31
32       - name: Run ESLint check
33         run: npm run lint
34         working-directory: frontend
```

Automated linting and formatting script

Multi File Support

- **Why it was done:**

- Make WebSVF more feasible for real-world projects
- Create an IDE-like environment
- Easy onboarding from/to existing projects
- Later On:
 - Support custom compilation
 - More languages supported (Rust/C++)

Christian's Improvements

Python SVF Backend Conversion

Why it was done:

- Easier open-source contributions as Python is a more commonly used language than C++/C#.
- Provides examples for users to use Python-SVF in their own projects
- Allows for more native support and extensibility since there is a Python API.
- Improves debugging, readability and dependency management

Python SVF Backend Conversion

What was done:

- Updated the main Python-SVF repository to capture stdout and stderr from tool calls
- Converted the WebSVF Backend to use Python FastAPI instead of C# .NET
 - Instead of running SVF on the command line via subprocesses, tool calls are done via `pysvf.run_svf_tool(args)`.
- Updated Dockerfile, [README.md](#) documentation and setup guides

Python SVF Backend Conversion

Add return types to run_svf_tool and svf_tool #35

Merged yuleisui merged 6 commits into `SVF-tools:main` from `istan18:add-return-types` 3 weeks ago

Conversation 0 Commits 6 Checks 1 Files changed 1



istan18 commented on Jul 18

Contributor ...

Added return types to `run_svf_tool` and `svf_tool` so its stdout can be easily captured for developer usage.



istan18 added 6 commits last month

Add return types

37b9640

Use output maps

20d308b

Updated comments

0e196ac

Added stderr

77b1c10

Omit error if empty

a8286cc

delete __pycache__

✓ a66689c

yuleisui merged commit **46f42c5** into `SVF-tools:main` 3 weeks ago

View details

Revert

1 check passed



Pull request successfully merged and closed

Delete branch

You're all set — the `add-return-types` branch can be safely deleted. If you wish, you can also delete this fork of `SVF-tools/SVF-Python` in the [settings](#).

Add return types to run_svf_tool and svf_tool #35

Merged yuleisui merged 6 commits into `SVF-tools:main` from `istan18:add-return-types` 3 weeks ago

Conversation 0 Commits 6 Checks 1 Files changed 1

Changes from all commits File filter Conversations Jump to

```

  42 42     print(f"[INFO] Running {tool_name} with args {args}")
  43 43     result = subprocess.run([tool_path] + args, check=True, text=True, capture_output=True)
  44 44     print(f"[INFO] Output:\n{result.stdout}")
  45 +     if result.stderr:
  46 +         print(f"[INFO] Errors:\n{result.stderr}")
  47 +     return result.stdout, result.stderr
  48
  49 48     except subprocess.CalledProcessError as e:
  50 49         print(f"[ERROR] Execution failed: {e}")
  51 50         print(f"[ERROR] STDERR:\n{e.stderr}")
  52
  53 @@ -55,16 +58,20 @@ def run_svf_tool(tool_name, args=None):
  54
  55 58     Args:
  56 59         tool_name (str): The name of the tool to run.
  57 60         args (list, optional): The arguments to pass to the tool. Defaults to sys.argv[1:].
  58
  59 61     Returns:
  60 62         output (str): The standard output of the tool.
  61 63         error (str): The standard error of the tool.
  62
  63 64     """
  64 65     if args is None:
  65 66         args = sys.argv[1:]
  66 67
  67 68     if tool_name in TOOL_NAMES:
  68 69         run_tool(TOOL_NAMES[tool_name], args)
  69 70         output, error = run_tool(TOOL_NAMES[tool_name], args)
  70 71     else:
  71 72         print(f"[ERROR] Unknown tool: {tool_name}", file=sys.stderr)
  72 73         print(f"[INFO] Available tools: {' '.join(TOOL_NAMES.keys())}", file=sys.stderr)
  73 74         sys.exit(1)
  74 75     return output, error
  75
  76 76 # Main entry point when module is executed directly
  77 77 def main():
  78
  79
  80
  81
  82
  83
  84
  85
  86
  87
  88
  89
  90
  91
  92
  93
  94
  95
  96
  97
  98
  99
  100
  101
  102
  103
  104
  105
  106
  107
  108
  109
  110
  111
  112
  113
  114
  115
  116
  117
  118
  119
  120
  121
  122
  123
  124
  125
  126
  127
  128
  129
  130
  131
  132
  133
  134
  135
  136
  137
  138
  139
  140
  141
  142
  143
  144
  145
  146
  147
  148
  149
  150
  151
  152
  153
  154
  155
  156
  157
  158
  159
  160
  161
  162
  163
  164
  165
  166
  167
  168
  169
  170
  171
  172
  173
  174
  175
  176
  177
  178
  179
  180
  181
  182
  183
  184
  185
  186
  187
  188
  189
  190
  191
  192
  193
  194
  195
  196
  197
  198
  199
  200
  201
  202
  203
  204
  205
  206
  207
  208
  209
  210
  211
  212
  213
  214
  215
  216
  217
  218
  219
  220
  221
  222
  223
  224
  225
  226
  227
  228
  229
  230
  231
  232
  233
  234
  235
  236
  237
  238
  239
  240
  241
  242
  243
  244
  245
  246
  247
  248
  249
  250
  251
  252
  253
  254
  255
  256
  257
  258
  259
  260
  261
  262
  263
  264
  265
  266
  267
  268
  269
  270
  271
  272
  273
  274
  275
  276
  277
  278
  279
  280
  281
  282
  283
  284
  285
  286
  287
  288
  289
  290
  291
  292
  293
  294
  295
  296
  297
  298
  299
  300
  301
  302
  303
  304
  305
  306
  307
  308
  309
  310
  311
  312
  313
  314
  315
  316
  317
  318
  319
  320
  321
  322
  323
  324
  325
  326
  327
  328
  329
  330
  331
  332
  333
  334
  335
  336
  337
  338
  339
  340
  341
  342
  343
  344
  345
  346
  347
  348
  349
  350
  351
  352
  353
  354
  355
  356
  357
  358
  359
  360
  361
  362
  363
  364
  365
  366
  367
  368
  369
  370
  371
  372
  373
  374
  375
  376
  377
  378
  379
  380
  381
  382
  383
  384
  385
  386
  387
  388
  389
  390
  391
  392
  393
  394
  395
  396
  397
  398
  399
  400
  401
  402
  403
  404
  405
  406
  407
  408
  409
  410
  411
  412
  413
  414
  415
  416
  417
  418
  419
  420
  421
  422
  423
  424
  425
  426
  427
  428
  429
  430
  431
  432
  433
  434
  435
  436
  437
  438
  439
  440
  441
  442
  443
  444
  445
  446
  447
  448
  449
  450
  451
  452
  453
  454
  455
  456
  457
  458
  459
  460
  461
  462
  463
  464
  465
  466
  467
  468
  469
  470
  471
  472
  473
  474
  475
  476
  477
  478
  479
  480
  481
  482
  483
  484
  485
  486
  487
  488
  489
  490
  491
  492
  493
  494
  495
  496
  497
  498
  499
  500
  501
  502
  503
  504
  505
  506
  507
  508
  509
  510
  511
  512
  513
  514
  515
  516
  517
  518
  519
  520
  521
  522
  523
  524
  525
  526
  527
  528
  529
  530
  531
  532
  533
  534
  535
  536
  537
  538
  539
  540
  541
  542
  543
  544
  545
  546
  547
  548
  549
  550
  551
  552
  553
  554
  555
  556
  557
  558
  559
  560
  561
  562
  563
  564
  565
  566
  567
  568
  569
  570
  571
  572
  573
  574
  575
  576
  577
  578
  579
  580
  581
  582
  583
  584
  585
  586
  587
  588
  589
  590
  591
  592
  593
  594
  595
  596
  597
  598
  599
  600
  601
  602
  603
  604
  605
  606
  607
  608
  609
  610
  611
  612
  613
  614
  615
  616
  617
  618
  619
  620
  621
  622
  623
  624
  625
  626
  627
  628
  629
  630
  631
  632
  633
  634
  635
  636
  637
  638
  639
  640
  641
  642
  643
  644
  645
  646
  647
  648
  649
  650
  651
  652
  653
  654
  655
  656
  657
  658
  659
  660
  661
  662
  663
  664
  665
  666
  667
  668
  669
  670
  671
  672
  673
  674
  675
  676
  677
  678
  679
  680
  681
  682
  683
  684
  685
  686
  687
  688
  689
  690
  691
  692
  693
  694
  695
  696
  697
  698
  699
  700
  701
  702
  703
  704
  705
  706
  707
  708
  709
  710
  711
  712
  713
  714
  715
  716
  717
  718
  719
  720
  721
  722
  723
  724
  725
  726
  727
  728
  729
  730
  731
  732
  733
  734
  735
  736
  737
  738
  739
  740
  741
  742
  743
  744
  745
  746
  747
  748
  749
  750
  751
  752
  753
  754
  755
  756
  757
  758
  759
  760
  761
  762
  763
  764
  765
  766
  767
  768
  769
  770
  771
  772
  773
  774
  775
  776
  777
  778
  779
  780
  781
  782
  783
  784
  785
  786
  787
  788
  789
  790
  791
  792
  793
  794
  795
  796
  797
  798
  799
  800
  801
  802
  803
  804
  805
  806
  807
  808
  809
  810
  811
  812
  813
  814
  815
  816
  817
  818
  819
  820
  821
  822
  823
  824
  825
  826
  827
  828
  829
  830
  831
  832
  833
  834
  835
  836
  837
  838
  839
  840
  841
  842
  843
  844
  845
  846
  847
  848
  849
  850
  851
  852
  853
  854
  855
  856
  857
  858
  859
  860
  861
  862
  863
  864
  865
  866
  867
  868
  869
  870
  871
  872
  873
  874
  875
  876
  877
  878
  879
  880
  881
  882
  883
  884
  885
  886
  887
  888
  889
  890
  891
  892
  893
  894
  895
  896
  897
  898
  899
  900
  901
  902
  903
  904
  905
  906
  907
  908
  909
  910
  911
  912
  913
  914
  915
  916
  917
  918
  919
  920
  921
  922
  923
  924
  925
  926
  927
  928
  929
  930
  931
  932
  933
  934
  935
  936
  937
  938
  939
  940
  941
  942
  943
  944
  945
  946
  947
  948
  949
  950
  951
  952
  953
  954
  955
  956
  957
  958
  959
  960
  961
  962
  963
  964
  965
  966
  967
  968
  969
  970
  971
  972
  973
  974
  975
  976
  977
  978
  979
  980
  981
  982
  983
  984
  985
  986
  987
  988
  989
  990
  991
  992
  993
  994
  995
  996
  997
  998
  999
  1000

```

UI Improvements

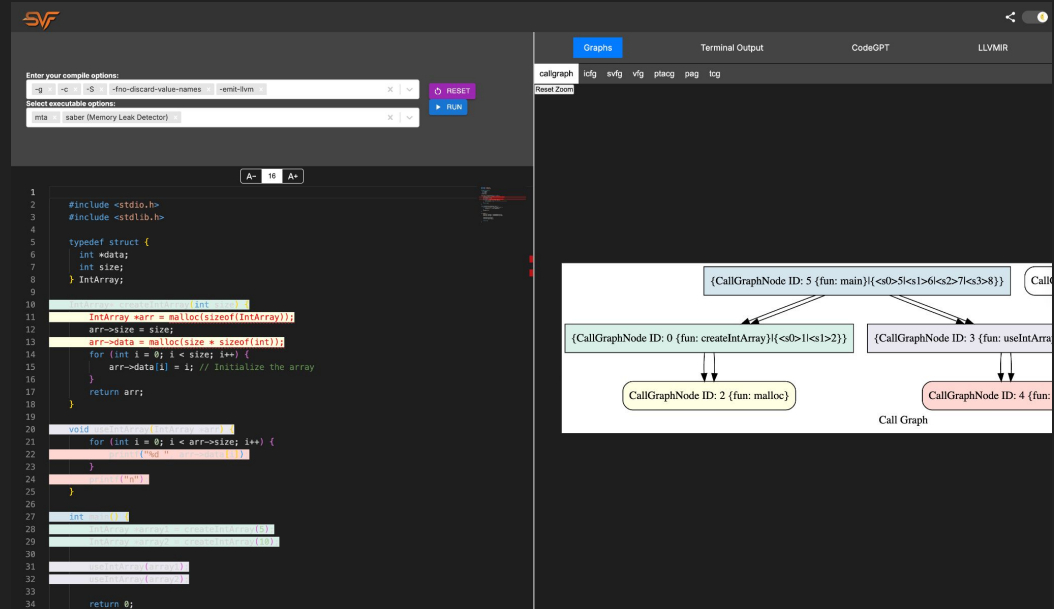
Why it was done:

- Increases user productivity and efficiency by making WebSVF easier to understand
- More responsive and interactive UI -> improves user engagement, retention and conversion
- 88% of users won't return after a bad UI/UX experience ([HubSpot](#))

UI/UX Improvements - Dark Mode

- Multiple spacing issues
- Poor colour contrast
- Inconsistent button design
- Laggy, delayed responsiveness
- Edges are too rough
- Some components not fully converted to dark mode equivalent

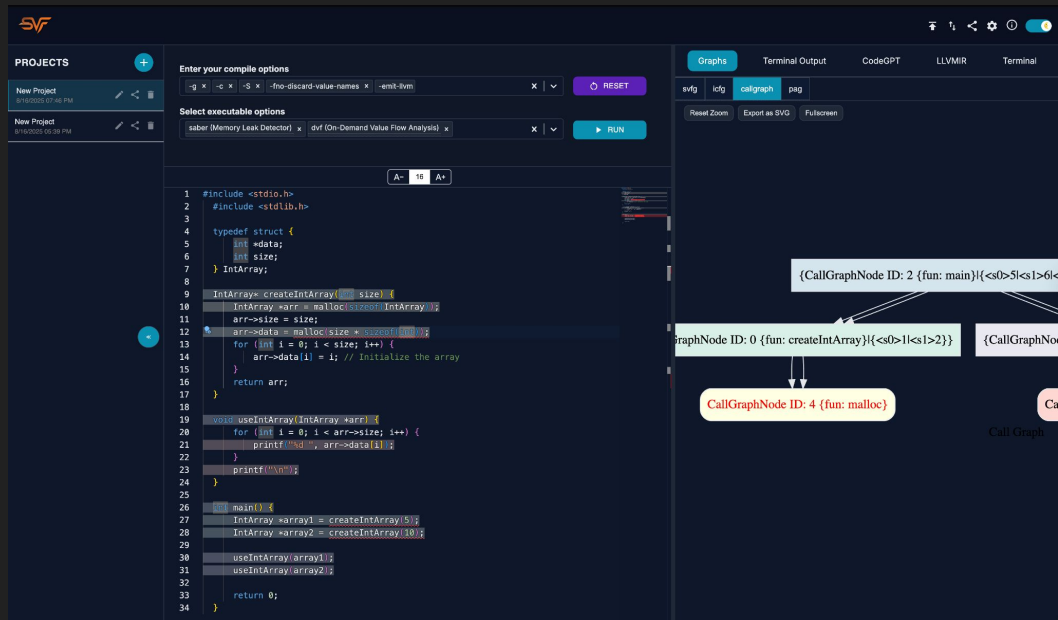
Old Version



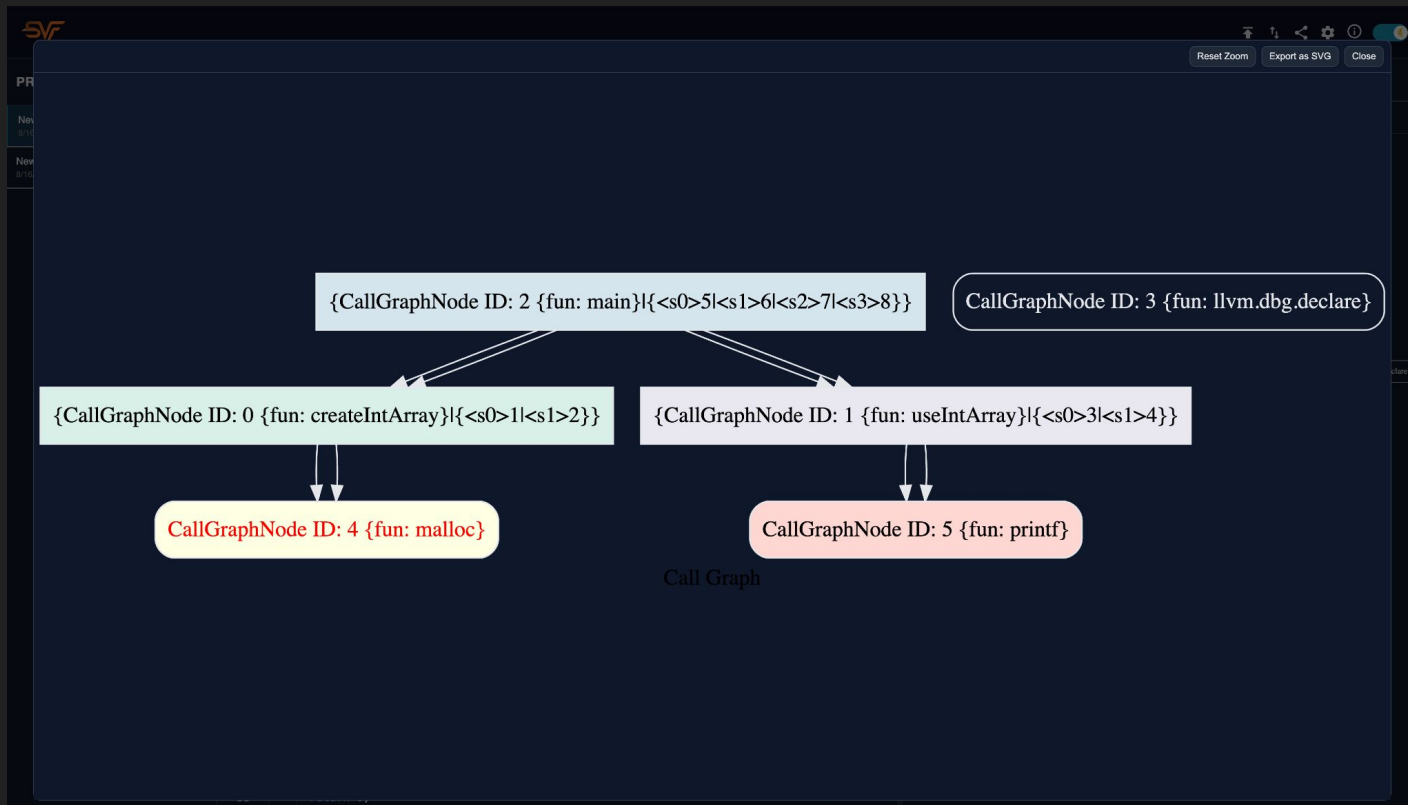
UI/UX Improvements - Dark Mode

- Consistent colour design
- Consistent spacing
- Rounded and consistent buttons
- Clear colour contrast
- Rounded corners
- Consistent with light mode design

New Version



UI/UX Improvements - Fullscreen



UI/UX Improvements - Toast



Code processed successfully!

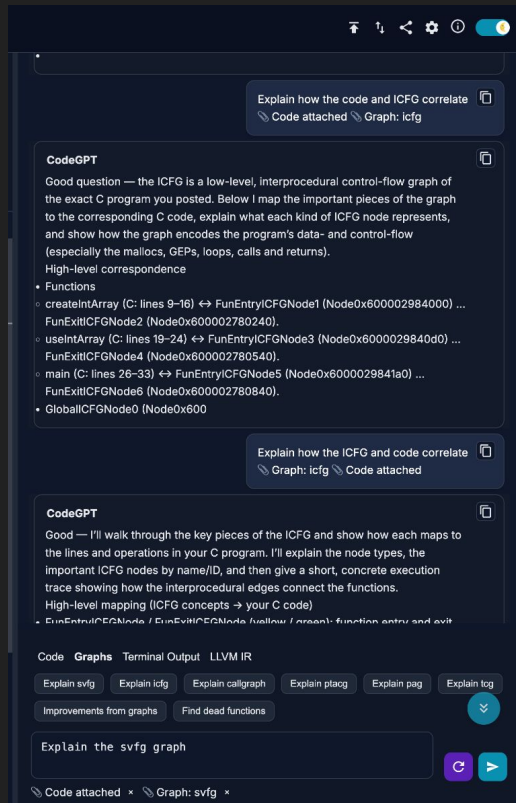


Backend Error: Failed to fetch



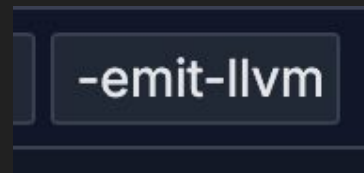
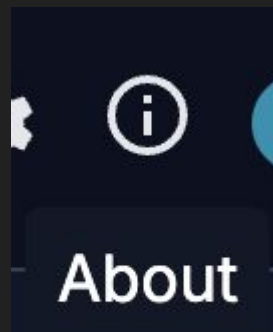
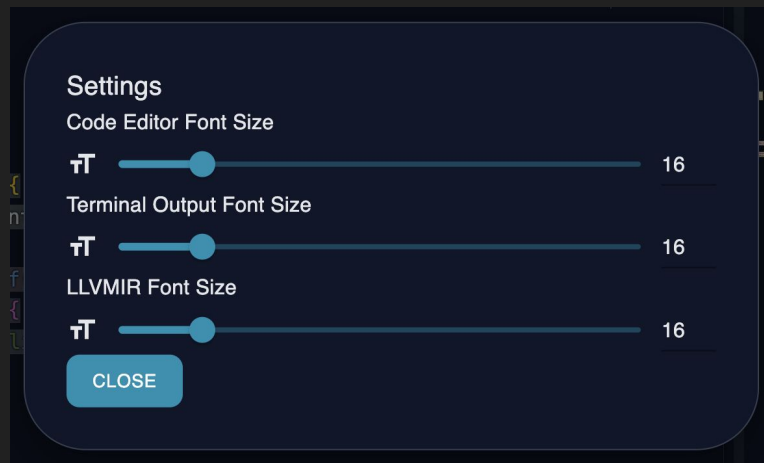
UI/UX Improvements - CodeGPT

- Updated CodeGPT to use the latest GPT-5 model with web search capabilities
- Added copy feature
- Ability to add and delete multiple attachments (code and multiple graphs)
- Reduce chatbox bloat when adding attachments
- General chat formatting and UI improvements



UI/UX Improvements - General

- Added about page -> allows users to gather context about SVF and WebSVF
- Added settings page
- Fixed bugs and error handling



Questions/Feedback