


Clang Static Analyzer

 Unknown macro: 'html'

Excuse the ads! We need some help to keep our site up.

 Unknown macro: 'html'

List

- [Clang Static Analyzer](#)
 - [Important Points to Consider](#)
 - [Slower than Compilation](#)
 - [False Positives](#)
 - [More Checks](#)
 - [Download](#)
 - [Install](#)
- [Example](#)
- [Related site](#)

Clang Static Analyzer

- [Clang C, C++ Objective-C](#)
- [Clang](#)
- [Clang Xcode](#)
-
- [Clang Clang Open source code](#)
 - [C++](#)
- [Clang Clang LLVM](#)

Important Points to Consider

Slower than Compilation

-
-

False Positives

-
-

More Checks

-

Download

- Mac OS X: <https://clang-analyzer.llvm.org/downloads/>
- Other Platforms: <https://clang-analyzer.llvm.org/installation#OtherPlatforms>

Install

- [Clang Scan-build](#)

Example

-

Sample.c

```
#include <stdio.h>
#include <stdlib.h>

int main(void)
{
    char *p = malloc(1);
    *p = 'a';

    char c = *p;

    printf("\n [%c]\n",c);

    free(p);
    c = *p;
    return 0;
}
```



Reading/writing memory after it has been freed

- <http://www.thegeekstuff.com/2011/11/valgrind-memcheck/>

- **scan-build** .
o .

Scan scan-build-3.7

```
lazenca0x0@ubuntu:/tmp/test$ scan-build-3.7 gcc test.c
scan-build: Using '/usr/lib/llvm-3.7/bin/clang' for static analysis
test.c:14:5: warning: Value stored to 'c' is never read
    c = *p;
    ^  ~~
test.c:14:9: warning: Use of memory after it is freed
    c = *p;
    ^~
2 warnings generated.
scan-build: 2 bugs found.
scan-build: Run 'scan-view /tmp/scan-build-2017-11-29-061740-71620-1' to examine bug reports.
lazenca0x0@ubuntu:/tmp/test$
```

- **scan-view** .

Run scan-view-3.7

```
lazenca0x0@ubuntu:/tmp/test$ scan-view-3.7 /tmp/scan-build-2017-11-29-061740-71620-1
Starting scan-view at: http://127.0.0.1:8181
Use Ctrl-C to exit.
```

- .

Report

Scan-build results

test - scan-build results

test - scan-build results

Users: isercas@ubuntu
Working Directory: /tmp/test
Command Line: gcc test.c
Clang Version: Ubuntu clang version 3.7.1-2ubuntu2 (tags/RELEASE_371final) (based on LLVM 3.7.1)
Date: Wed Nov 29 06:17:40 2017

Bug Summary

Bug Type	Quantity	Display?
All Bugs	2	<input checked="" type="checkbox"/>
Dead store		
Dead assignment	1	<input checked="" type="checkbox"/>
Memory Error		
Use after free	1	<input checked="" type="checkbox"/>

Reports

Bug Group	Bug Type *	File	Function/Method	Line	Path Length	
Dead store	Dead assignment	test.c	main	14	1	View Report Report Bug Open File
Memory Error	Use after free	test.c	main	14	3	View Report Report Bug Open File 사진

Report 1

test.c

Summary > Report ad9f48

Bug Summary

File: test.c
Location: [line 14, column 5](#)
Description: Use of memory after it is freed

Annotated Source Code

```
1 #include <stdio.h>
2 #include <stdlib.h>
3
4 int main(void)
5 {
6     char *p = malloc(10);
7     *p = 'a';
8     char c = *p;
9     printf("a: %c\n", c);
10    free(p);
11    c = *p;
12    return 0;
13 }
```

Memory is allocated =>
Memory is released =>
Use of memory after this freed

VMware Fusion

Report 2

test.c

Summary > Report file35a

Bug Summary

File: test.c
Location: [line 14, column 5](#)
Description: Value stored to 'c' is never read

Annotated Source Code

```
1 #include <stdio.h>
2 #include <stdlib.h>
3
4 int main(void)
5 {
6     char *p = malloc(10);
7     *p = 'a';
8     char c = *p;
9     printf("a: %c\n", c);
10    free(p);
11    c = *p;
12    return 0;
13 }
```

Value stored to 'c' is never read

Related site

- <https://clang-analyzer.lvm.org/>
- <https://clang-analyzer.lvm.org/scan-build.html>



Unknown macro: 'html'