Full System Report

Flawfinder Analysis Report

```
Flawfinder version 2.0.19, (C) 2001-2019 David A. Wheeler.Đ
Number of rules (primarily dangerous function names) in C/C++ ruleset: 222Đ
*** No input filesĐ
```

Flawfinder Analysis Report

```
Flawfinder version 2.0.19, (C) 2001-2019 David A. Wheeler.Ð
Number of rules (primarily dangerous function names) in C/C++ ruleset: 222Ð
Examining ./uploads/anything.cÐ
Ð
FINAL RESULTS:Ð
Ð
./uploads/anything.c:11:  [4] (buffer) strcpy:Ð
  Does not check for buffer overflows when copying to destination [MS-banned]Ð
  (CWE-120). Consider using snprintf, strcpy_s, or strlcpy (warning: strncpyÐ
  easily misused).Ð
./uploads/anything.c:9:  [2] (buffer) char:Ð
  Statically-sized arrays can be improperly restricted, leading to potentialÐ
  overflows or other issues (CWE-119!/CWE-120). Perform bounds checking, useÐ
  functions that limit length, or ensure that the size is larger than theÐ
  maximum possible length.Ð
Ð
ANALYSIS SUMMARY:Ð
Ð
Hits = 2Ð
Lines analyzed = 13 in approximately 0.01 seconds (1852 lines/second)Ð
Physical Source Lines of Code (SLOC) = 10Ð
Hits@level = [0]   1 [1]   0 [2]   1 [3]   0 [4]   1 [5]   0Ð
Hits@level+ = [0+]   3 [1+]   2 [2+]   2 [3+]   1 [4+]   1 [5+]   0Ð
Hits/KSLOC@level+ = [0+] 300 [1+] 200 [2+] 200 [3+] 100 [4+] 100 [5+]   0Ð
Minimum risk level = 1Ð
Ð
Not every hit is necessarily a security vulnerability.Ð
You can inhibit a report by adding a comment in this form:Ð
// flawfinder: ignoreÐ
Make *sure* it's a false positive!Ð
You can use the option --neverignore to show these.Ð
Ð
There may be other security vulnerabilities; review your code!Ð
See 'Secure Programming HOWTO'Ð
(https://dwheeler.com/secure-programs) for more information.Ð
```