<http://cwe.mitre.org/top25/index.html>

<https://dwheeler.com/flawfinder/#speed>

<file:///F:/First%20Semester/Software%20Testing_8%20Credit/Assignment/FULLTEXT01.pdf>

file:///F:/First%20Semester/Software%20Testing\_8%20Credit/Assignment/Secure-Programs-HOWTO.pdf

<https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/>

### <https://in.mathworks.com/help/matlab/ref/strtrim.html> Remove Leading and Trailing Whitespace from Cell Array

Search: flawfinder tutorial

https://dwheeler.com/flawfinder/

<http://linux-tutorial.info/modules.php?name=Howto#LinuxOS>

<https://www.tipsandtricks-hq.com/unix-vi-commands-take-advantage-of-the-unix-vi-editor-374>

For test.c Docs:

<https://www.debian.org/security/audit/examples/flawfinder>

<https://www.debian.org/security/audit/examples/test.c.html>

<https://hackernoon.com/lexical-analysis-861b8bfe4cb0> [15.12.2018]

<https://www.youtube.com/watch?v=WccZQSERfCM>

<https://www.youtube.com/watch?v=VGgIZl5WjH0> - - - Good Explanation

https://www.youtube.com/watch?v=C7NykE7PS9A

[Online]: Daniel Persson, Dejan Baca, Software Security Analysis - Managing source code audit, <https://www.diva-portal.org/smash/get/diva2:830925/FULLTEXT01.pdf> [19.12.2018]

<https://www.tutorialspoint.com/compiler_design/compiler_design_lexical_analysis.htm> [21.12.2018]

https://github.com/engineer-man/youtube/tree/master/016 [21.12.2018]

https://www.youtube.com/watch?v=CQ6pGrXY1Us

<https://github.com/engineer-man/youtube/tree/master/017> [22.12.2018]

https://www.youtube.com/watch?v=ytGATjX3nqc

<https://www.hahwul.com/2015/12/system-hacking-flawfinder-cc-source.html> [22.12.2018]

<https://flylib.com/books/en/3.85.1.66/1/> [23.12.2018]

<https://www.youtube.com/watch?v=JpxHaQ9qlnE> --- Program 5b: Hard LInks and Soft Links | Unix

<http://cwe.mitre.org/top25/archive/2011/2011_training.html> [07.01.2019]

10. Flawfinder (2004), URL http://www.dwheeler.com/flawfinder/ [07.01.2019]

11. ITS4 (2004), URL https://www.openfoundry.org/en/resourcecatalog/Security/Source-Code-Audit/its4 [07.01.2019]

12. Rough Auditing Tool for Security (2004), URL [http://www.securesw.com/rats[07.01.2019](http://www.securesw.com/rats%5b07.01.2019)]

Installing flawfinder URL: https://dwheeler.com/flawfinder/INSTALL.txt

for tutorial of –allowlink : Follow symbolic links.

<https://www.gnu.org/software/libc/manual/html_node/Symbolic-Links.html> [23.12.2018]

<https://www.youtube.com/watch?v=l_1Q3DG3uoE> Symbolic Links in Linux

<https://www.youtube.com/watch?v=E4xZnIPNTN4> C Programming in Linux Tutorial #064 - mkdir()

C-Based Application Exploits and Countermeasures - Yves Younan

<https://www.youtube.com/watch?v=tVG8e_Dneag&t=1828s>

# Low-Level Software Security: Attacks and Countermeasures - Frank Piessens

https://www.youtube.com/watch?v=ZLZkf8FVcsU

<https://www.youtube.com/watch?v=Mtbb_R8X--4>

# WHAT IS UNICODE UTF 8 AND HOW IT IS ENCODED EXAMPLE

rmdir() symlink() unlink() Functions

**Flawfinder** Flawfinder was written by the author of “Secure Programming for Linux and Unix HOWTO”, David Wheeler. Flawfinder scans C/C++ code and has a database of 128 C/C++ vulnerabilities. Flawfinder has 6 levels of reporting warnings, level 0 to 5, where level 5 only shows the most dangerous warnings. Standard level in Flawfinder is level 1. Flawfinder version 1.24 was used [10]. 3.2.3 ITS4 Cigital developed **ITS4**, “**I**t's **T**he **S**oftware **S**tupid! **S**ecurity **S**canner”. ITS4 scans C/C++ code and its database has 144 vulnerabilities. ITS4 has 6 levels of reporting warnings, level 0 to 5 where level 5 only showed the most dangerous warnings. Standard level in ITS4 is level 2. Version 1.1.1 of ITS4 was used [11]. 3.2.4 RATS **RATS**, “**R**ough **A**utomatic **T**ool for **S**ecurity”. Secure Software, Inc developed RATS and some of the programmers of RATS have also worked with ITS4. RATS scans C/C++, Python, PHP and Perl source code. Rats has 3 levels of reporting warnings, Low, Medium and High where High shows the most dangerous warnings. The standard level is Medium. Version 2.1 was used and it has a database with 334 C/C++ vulnerabilities [12].

**Brief Tutorials:**

Linux Based Environments:

Testing of /exploits/overflow.c or vuln.c

------------------------------------------------- -----------------------------------------------------------------

root@kali:~/softwareTesting# gcc -w vuln.c -o vuln

-------------------------------------- ----------------------------------- ----------------------------------------

root@kali:~/exploits# flawfinder overflow.c|less

For Exit from text editor: ctrl+z

/\*Flawfinder:ignore\*/

-------------------------------------------------------------------------------------------------------------

$flawfinder --minlevel=4 vuln.c

root@kali:~/softwareTesting# flawfinder --minlevel=4 vuln.c|less

[43]+ Stopped flawfinder --minlevel=4 vuln.c | less

root@kali:~/softwareTesting# flawfinder --minlevel=5 vuln.c|less

[44]+ Stopped flawfinder --minlevel=5 vuln.c | less

root@kali:~/softwareTesting# flawfinder -m 4 vuln.c|less

[45]+ Stopped flawfinder -m 4 vuln.c | less

root@kali:~/softwareTesting# flawfinder -m 5 vuln.c|less

[46]+ Stopped flawfinder -m 5 vuln.c | less

root@kali:~/softwareTesting# flawfinder vuln.c|less

[6]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder -F vuln.c|less

[7]+ Stopped flawfinder -F vuln.c | less

root@kali:~/softwareTesting# flawfinder -F -n vuln.c|less

[8]+ Stopped flawfinder -F -n vuln.c | less

root@kali:~/softwareTesting# flawfinder -F -n vuln.c|less

[9]+ Stopped flawfinder -F -n vuln.c | less

root@kali:~/softwareTesting#

-------------------------------------------------------------------------------------------------------

$root@kali:~/softwareTesting# flawfinder vuln.c|less

[2]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder -n vuln.c|less

[3]+ Stopped flawfinder -n vuln.c | less

----------------------------------- **Selecting Hits to Display** ------------------------------------

root@kali:~/softwareTesting# gcc -w vuln.c -o vuln^C

root@kali:~/softwareTesting# flawfinder vuln.c|less

[11]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder -F vuln.c|less

[12]+ Stopped flawfinder -F vuln.c | less

root@kali:~/softwareTesting# flawfinder -I vuln.c|less

[13]+ Stopped flawfinder -I vuln.c | less

root@kali:~/softwareTesting# flawfinder -I -n vuln.c|less

[21]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder --input vuln.c|less

[22]+ Stopped flawfinder --input vuln.c | less

[14]+ Stopped flawfinder -I -n vuln.c | less

root@kali:~/softwareTesting# flawfinder -I -F -n vuln.c|less

[15]+ Stopped flawfinder -I -F -n vuln.c | less

root@kali:~/softwareTesting# flawfinder -F -n vuln.c|less

[16]+ Stopped flawfinder -F -n vuln.c | less

root@kali:~/softwareTesting# flawfinder -n vuln.c|less

[17]+ Stopped flawfinder -n vuln.c | less

root@kali:~/softwareTesting#

root@kali:~/softwareTesting# flawfinder -e CWE-20 vuln.c|less

[19]+ Stopped flawfinder -e CWE-20 vuln.c | less

root@kali:~/softwareTesting# flawfinder --regex "CWE-119|CWE-120" vuln.c | less

[58]+ Stopped flawfinder --regex "CWE-119|CWE-120" vuln.c | less

root@kali:~/softwareTesting# flawfinder --regex "CWE-119|CWE-20" vuln.c | less

[59]+ Stopped flawfinder --regex "CWE-119|CWE-20" vuln.c | less

-------------------------------------------------------------------------------------------------------------

$flawfinder --minlevel=4 vuln.c

root@kali:~/softwareTesting# flawfinder --minlevel=4 vuln.c|less

[43]+ Stopped flawfinder --minlevel=4 vuln.c | less

root@kali:~/softwareTesting# flawfinder --minlevel=5 vuln.c|less

[44]+ Stopped flawfinder --minlevel=5 vuln.c | less

root@kali:~/softwareTesting# flawfinder -m 4 vuln.c|less

[45]+ Stopped flawfinder -m 4 vuln.c | less

root@kali:~/softwareTesting# flawfinder -m 5 vuln.c|less

[46]+ Stopped flawfinder -m 5 vuln.c | less

-------------------------------- ---------------**Selecting Output Format ----------------------------------------------**

root@kali:~/softwareTesting# flawfinder vuln.c|less

[47]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder -C vuln.c|less

[48]+ Stopped flawfinder -C vuln.c | less

root@kali:~/softwareTesting# flawfinder vuln.c|less

[49]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder -C vuln.c|less

[50]+ Stopped flawfinder -C vuln.c | less

root@kali:~/softwareTesting# flawfinder --columns vuln.c|less

[51]+ Stopped flawfinder --columns vuln.c | less

root@kali:~/softwareTesting# flawfinder vuln.c|less

[52]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder -c vuln.c|less

[53]+ Stopped flawfinder -c vuln.c | less

root@kali:~/softwareTesting# flawfinder vuln.c|less

[54]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder -c vuln.c|less

[55]+ Stopped flawfinder -c vuln.c | less

root@kali:~/softwareTesting# flawfinder --context vuln.c|less

[56]+ Stopped flawfinder --context vuln.c | less

root@kali:~/softwareTesting# flawfinder --csv vuln.c

File,Line,Column,Level,Category,Name,Warning,Suggestion,Note,CWEs,Context,Fingerprint

vuln.c,8,1,5,buffer,gets,"Does not check for buffer overflows (CWE-120, CWE-20)",Use fgets() instead,,"CWE-120, CWE-20",gets(buffer);,8574681bcf016b459efe0a123d75643927688f096b753ca762978b7c7aa81c29

vuln.c,18,2,4,buffer,strcpy,Does not check for buffer overflows when copying to destination [MS-banned] (CWE-120),"Consider using snprintf, strcpy\_s, or strlcpy (warning: strncpy easily misused)",,CWE-120," strcpy(buf, argv[1]);",ec15926452585fb0f64c4b89b2303693a78314070b7ae452808885cc6cfbe3dd

vuln.c,6,2,2,buffer,char,"Statically-sized arrays can be improperly restricted, leading to potential overflows or other issues (CWE-119!/CWE-120)","Perform bounds checking, use functions that limit length, or ensure that the size is larger than the maximum possible length",,CWE-119!/CWE-120, char buffer[8];,f420a5f42499098507ccdc6f3b4d180b3edc68742667aff39ca3b5c7d299a22d

vuln.c,17,2,2,buffer,char,"Statically-sized arrays can be improperly restricted, leading to potential overflows or other issues (CWE-119!/CWE-120)","Perform bounds checking, use functions that limit length, or ensure that the size is larger than the maximum possible length",,CWE-119!/CWE-120, char buf[500];,4a58776addf47a448f194916e4e2342f7c7ebfcf8bb53f488de91272a5509d4e

root@kali:~/softwareTesting# flawfinder --csv vuln.c|less

[57]+ Stopped flawfinder --csv vuln.c | less

root@kali:~/softwareTesting# flawfinder --csv vuln.c >>csv.txt

root@kali:~/softwareTesting# flawfinder --dataonly vuln.c|less

[60]+ Stopped flawfinder --dataonly vuln.c | less

root@kali:~/softwareTesting# flawfinder -D vuln.c|less

[61]+ Stopped flawfinder -D vuln.c | less

root@kali:~/softwareTesting# flawfinder --html vuln.c|less

[62]+ Stopped flawfinder --html vuln.c | less

root@kali:~/softwareTesting# flawfinder -H vuln.c|less

[63]+ Stopped flawfinder -H vuln.c | less

root@kali:~/softwareTesting# flawfinder -H vuln.c|less >>vuln.html

root@kali:~/softwareTesting# flawfinder -H -c vuln.c|less >>vuln.html

root@kali:~/softwareTesting# flawfinder -c -H vuln.c|less >>vuln.html

root@kali:~/softwareTesting# flawfinder -cH vuln.c|less >>vuln.html

root@kali:~/softwareTesting#

root@kali:~/softwareTesting# flawfinder -cH vuln.c|less >>vuln.html

root@kali:~/softwareTesting# flawfinder -i vuln.c|less

[64]+ Stopped flawfinder -i vuln.c | less

root@kali:~/softwareTesting# flawfinder --immediate vuln.c|less

[65]+ Stopped flawfinder --immediate vuln.c | less

root@kali:~/softwareTesting# flawfinder vuln.c|less

[3]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder -S vuln.c|less

[4]+ Stopped flawfinder -S vuln.c | less

root@kali:~/softwareTesting# flawfinder vuln.c|less

[5]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder --singleline vuln.c|less

[7]+ Stopped flawfinder --singleline vuln.c | less

root@kali:~/softwareTesting# flawfinder vuln.c|less

[8]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder --omittime vuln.c|less

[9]+ Stopped flawfinder --omittime vuln.c | less

root@kali:~/softwareTesting# flawfinder vuln.c|less

[10]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder -Q vuln.c|less

[11]+ Stopped flawfinder -Q vuln.c | less

root@kali:~/softwareTesting# flawfinder vuln.c|less

[12]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder -Q vuln.c|less

[13]+ Stopped flawfinder -Q vuln.c | less

root@kali:~/softwareTesting# flawfinder vuln.c|less

[14]+ Stopped flawfinder vuln.c | less

root@kali:~/softwareTesting# flawfinder --quiet vuln.c|less

[15]+ Stopped flawfinder --quiet vuln.c | less

**Hit list Management**

-------------------------------------------------------- --------------------------------- --------------------------------------------

root@kali:~/softwareTesting# flawfinder -Q --loadhitlist hitlist.txt|less

[19]+ Stopped flawfinder -Q --loadhitlist hitlist.txt | less

root@kali:~/softwareTesting# ^C

root@kali:~/softwareTesting# flawfinder -Q --savehitlist hitlist.txt vuln.c|less

[20]+ Stopped flawfinder -Q --savehitlist hitlist.txt vuln.c | less

root@kali:~/softwareTesting# flawfinder -Q --loadhitlist hitlist.txt|less

[21]+ Stopped flawfinder -Q --loadhitlist hitlist.txt | less

root@kali:~/softwareTesting# flawfinder -m 4 --savehitlist minhitlist.txt vuln.c

root@kali:~/softwareTesting# flawfinder -m 4 --savehitlist minhitlist.txt vuln.c|less

[22]+ Stopped flawfinder -m 4 --savehitlist minhitlist.txt vuln.c | less

root@kali:~/softwareTesting# flawfinder -m 4 --loadhitlist minhitlist.txt|less

[23]+ Stopped flawfinder -m 4 --loadhitlist minhitlist.txt | less

root@kali:~/softwareTesting# flawfinder -m 5 --loadhitlist minhitlist.txt|less

[24]+ Stopped flawfinder -m 5 --loadhitlist minhitlist.txt | less

root@kali:~/softwareTesting#

------------------------------------------- Can’t Tested ----------------------------------------------------------------

root@kali:~/softwareTesting# flawfinder --savehitlist minhitlist.txt overflow.c|less

[31]+ Stopped flawfinder --savehitlist minhitlist.txt overflow.c | less

root@kali:~/softwareTesting# flawfinder --loadhitlist minhitlist.txt|less

[32]+ Stopped flawfinder --loadhitlist minhitlist.txt | less

root@kali:~/softwareTesting# flawfinder --diffhitlist hitlist.txt minhitlist.txt|less

[33]+ Stopped flawfinder --**diffhitlist** hitlist.txt minhitlist.txt | less

root@kali:~/softwareTesting# flawfinder --loadhitlist --diffhitlist hitlist.txt minhitlist.txt|less

[34]+ Stopped flawfinder --loadhitlist --diffhitlist hitlist.txt minhitlist.txt | less

root@kali:~/softwareTesting# flawfinder --savehitlist savehit.txt vuln.c|less

[42]+ Stopped flawfinder --savehitlist savehit.txt vuln.c | less

root@kali:~/softwareTesting# flawfinder --loadhitlist savehit.txt|less

[43]+ Stopped flawfinder --loadhitlist savehit.txt | less

root@kali:~/softwareTesting# flawfinder --diffhitlist savehit.txt vuln.c|less

[44]+ Stopped flawfinder --diffhitlist savehit.txt vuln.c | less

root@kali:~/softwareTesting# flawfinder --loadhitlist savehit.txt|less

[45]+ Stopped flawfinder --loadhitlist savehit.txt | less

root@kali:~/softwareTesting# flawfinder --diffhitlist savehit.txt vuln.c|less

[47]+ Stopped flawfinder --diffhitlist savehit.txt vuln.c | less

--------------------------------- ------------------------- ---------------------------- ------------------------------------

Can’t test with the command line with different combination

**root@kali:~/softwareTesting# flawfinder -e CWE-119 vuln.c|less**

**[28]+ Stopped flawfinder -e CWE-119 vuln.c | less**

**root@kali:~/softwareTesting# flawfinder --regexp=CWE-119 vuln.c|less**

**[29]+ Stopped flawfinder --regexp=CWE-119 vuln.c | less**

**root@kali:~/softwareTesting# flawfinder --regexp='CWE-119' vuln.c|less**

**[30]+ Stopped flawfinder --regexp='CWE-119' vuln.c | less**

**root@kali:~/softwareTesting# flawfinder --regexp="CWE-119" vuln.c|less**

**[31]+ Stopped flawfinder --regexp="CWE-119" vuln.c | less**

**root@kali:~/softwareTesting# flawfinder --regexp "CWE-119" vuln.c|less**

**[32]+ Stopped flawfinder --regexp "CWE-119" vuln.c | less**

**root@kali:~/softwareTesting# flawfinder --regexp CWE-119 vuln.c|less**

**[33]+ Stopped flawfinder --regexp CWE-119 vuln.c | less**

**root@kali:~/softwareTesting# flawfinder --regexp 'CWE-119' vuln.c|less**

**[34]+ Stopped flawfinder --regexp 'CWE-119' vuln.c | less**

------------------------------ ------------------------- ----------------------- ---------------------- ----------------------------

root@kali:~/softwareTesting# ls -i

2760868 hello.c 2752810 vulnargv.c  **2760093** vulnlink.c

2760869 overflow.c **2755603** vuln.c

root@kali:~/softwareTesting# flawfinder --allowlink vuln.c vulnlink.c

--------------------------------------------------------- Example----------------------------------------------------------------

root@kali:~/softwareTesting# flawfinder -QDSC vuln.c|less

[35]+ Stopped flawfinder -QDSC vuln.c | less

root@kali:~/softwareTesting# flawfinder -quiet --html --context vuln.c>result.html

root@kali:~/softwareTesting# flawfinder -QHc vuln.c>result.html

root@kali:~/softwareTesting# flawfinder vuln.c>result.html

root@kali:~/softwareTesting# flawfinder -H vuln.c>result.html

root@kali:~/softwareTesting# flawfinder -H -Q vuln.c>result.html

root@kali:~/softwareTesting# flawfinder -H vuln.c>result.html

root@kali:~/softwareTesting# flawfinder -H -Q vuln.c>result\_Q.html

root@kali:~/softwareTesting# flawfinder -H -Q -c vuln.c>result\_HQc.html