

---

# A Source Code - Vulnerability Automatic Analyzer.

v0.01

---



0x00. Overview.

0x01.

0x02.

0x03.

0x04. End.

INetCop Security Technologies

---

0x00. Overview.

=====

SC-VA2(RealCodeName)

C

, secure

, secure



```

char *fmts_printf;
char *fmts_sprintf; //
char *fmts_snprintf;
char *fmts_fprintf;
char *func_strcpy;
char *func_strcat;
char *envr_getenv;
char *race_tmpnam;
char *race_mktemp;
};
--

```

2. 3가

```

—
struct statm /* */
{
    char *statm_if;
    char *statm_for;
    char *statm_while;
};
--

```

3. 4가

```

—
int string_f_num[LINESIZE]={0}; // ,
// (Buffer Overflow)
int format_f_num[LINESIZE]={0}; // (Format String)
int getstr_f_num[LINESIZE]={0}; // (Buffer Overflow)
int racecn_f_num[LINESIZE]={0}; // (Race Condition)
--

```

C code

bug 가

C source code :

---

```
[x82@SC-VA2 SC-VA2_Project]$ cat vuln.c
```

```
main() {  
    strcpy(  
    }  
}
```

```
[x82@SC-VA2 SC-VA2_Project]$ ./sc-va2 -ac vuln.c
```

OK, Waiting. make result now.

```
[-] 가 . signal: 11
```

, C

Debugging mode

```
[*] BETA Tester ?
```

, C

[1] [mailto: xpl017elz@inetcop.org](mailto:xpl017elz@inetcop.org)

[2] [mailto: xploit@hackermail.com](mailto:xploit@hackermail.com)

[3] [mailto: szoahc@hotmail.com](mailto:szoahc@hotmail.com)

---

```
[x82@SC-VA2 SC-VA2_Project]$
```

--

signal 11(Segmentation fault)

C source code

.;-)

**0x02.**

=====

0.

**[Team INetCop Security] WIN32 MS-DOS SC-VA2 Project**

**Usage: ./sc-va2 -[option] [arguments]**

**Example: ./sc-va2 -sc test\_vuln\_src/test1.c**

**Options:**

- c [filename]** Source code filename.
- s** String copy function: `strcpy()`, `strcat()`, `sprintf()`;
- e** Environment function: `getenv()`;
- f** Fmt print function: `syslog()`, `*printf()`, `snprintf()`;
- g** Get string function: `gets()`, `scanf()`;
- r** Race condition function: `tmpnam()`, `mktemp()`;
- a** All function set rule.
- h** Display this help information.

For reference, '-e' option must use with '-s' option.

Example, it's "-sec[filename]".

Detailed information visits lower part site:

[URL:<http://project.underattack.co.kr/sc-va2.html>] (English).

[URL:<http://project.underattack.co.kr/hangul.html>] (Korean).

'-c' :  
:  
.  
  
'-s' :  
:  
.  
  
'-e' :  
:  
., '-s'  
  
'-f' :  
:  
.  
  
'-g' :  
:  
.  
  
'-r' :  
:  
.  
  
'-a' :  
:  
.  
  
'-h' :  
:  
.

1. .

**sc-va2 -sec test\_vuln\_src/test2.c**

test\_vuln\_src/test2.c

**sc-va2 -fgr test\_vuln\_src/test1.c**

test\_vuln\_src/test1.c

sc-va2 -a test\_vuln\_src/test1.c

test\_vuln\_src/test1.c

**0x03.**

=====

sc-va2

log

DB

[--- -----]

OK, Waiting. make result now.

test\_vuln\_src/test2.c:25: dangerous: the `fprintf()' function found:

test\_vuln\_src/test2.c:25:               'format string'

test\_vuln\_src/test2.c:25: fprintf()

test\_vuln\_src/test2.c:25: input validation error

test\_vuln\_src/test2.c:37: dangerous: the `gets()' function found:

test\_vuln\_src/test2.c:37:           fgets()

test\_vuln\_src/test2.c:37: boundary condition error

test\_vuln\_src/test2.c:38: dangerous: the `snprintf()' function found:

test\_vuln\_src/test2.c:38:               'format string'

test\_vuln\_src/test2.c:38: snprintf()

test\_vuln\_src/test2.c:38: input validation error

test\_vuln\_src/test2.c:43: dangerous: the `strcpy()' function found:

test\_vuln\_src/test2.c:43:           strcpy()

test\_vuln\_src/test2.c:43: boundary condition error

test\_vuln\_src/test2.c:50: dangerous: the `scanf()' function found:

test\_vuln\_src/test2.c:50:           'format string'

test\_vuln\_src/test2.c:50: boundary condition error



가

input validation error                      format string

format string

, test\_vuln\_src/test2.c    25

```
bash# cat -n test_vuln_src/test2.c | grep 25
```

```
    25            fprintf(stderr,argv[0]);
```

```
bash#
```

fprintf()    가 format string

```
bash# ln -s test2 %x%x%x
```

```
bash# ./%x%x%x
```

```
usages: ./58585445585858580 -option arguments
```

```
-A,-a,-b,-B
```

```
bash#
```

format string

```
test_vuln_src/test2.c:25: input validation error
```

```
test_vuln_src/test2.c:38: input validation error
```

```
test_vuln_src/test2.c:57: input validation error
```

```
test_vuln_src/test2.c:61: input validation error
```

```
test_vuln_src/test2.c:63: input validation error
```

boundary condition error

boundary

, buffer overflow

, test\_vuln\_src/test2.c    37

```
bash# cat -n test_vuln_src/test2.c | grep 37
```

```
37          gets(x0x);
```

```
bash#
```

```
          x0x          gets()
```

```
bash# ./test2 -A
```

```
input: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA ...
```

```
tst: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
Segmentation fault
```

```
bash#
```

```
test_vuln_src/test2.c:37: boundary condition error
```

```
test_vuln_src/test2.c:43: boundary condition error
```

```
test_vuln_src/test2.c:50: boundary condition error
```

```
, race condition error
```

```
test_vuln_src/test2.c:60: race condition error
```

```
test_vuln_src/test2.c:62: race condition error
```

securityfocus

: .

:

1. 가 .
2. .
3. 가 .  
buffer overflow .

: .

:

1. .
2. module .
3. module .
4. 가 .

:

1. exploit .

:

1. 가 .
2. machine, .
3. 가 가 .

**0x04. End.**

=====

szoahc(at)hotmail(dot)com

C source code

--

By "dong-houn yoU" (Xpl017Elz), in INetCop(c) Security.

MSN & E-mail: [szoahc\(at\)hotmail\(dot\)com](mailto:szoahc(at)hotmail(dot)com),  
[xploit\(at\)hackermail\(dot\)com](mailto:xploit(at)hackermail(dot)com)

INetCop Security Home: <http://www.inetcop.org/> (Korean hacking game)

My World: <http://x82.inetcop.org/>

GPG public key: <http://wizard.underattack.co.kr/~x82/h0me/pr0file/x82.k3y>

--