

# Raport z laboratorium 3 - 03.04.2024

---

Sebastian Abramowski, 325142

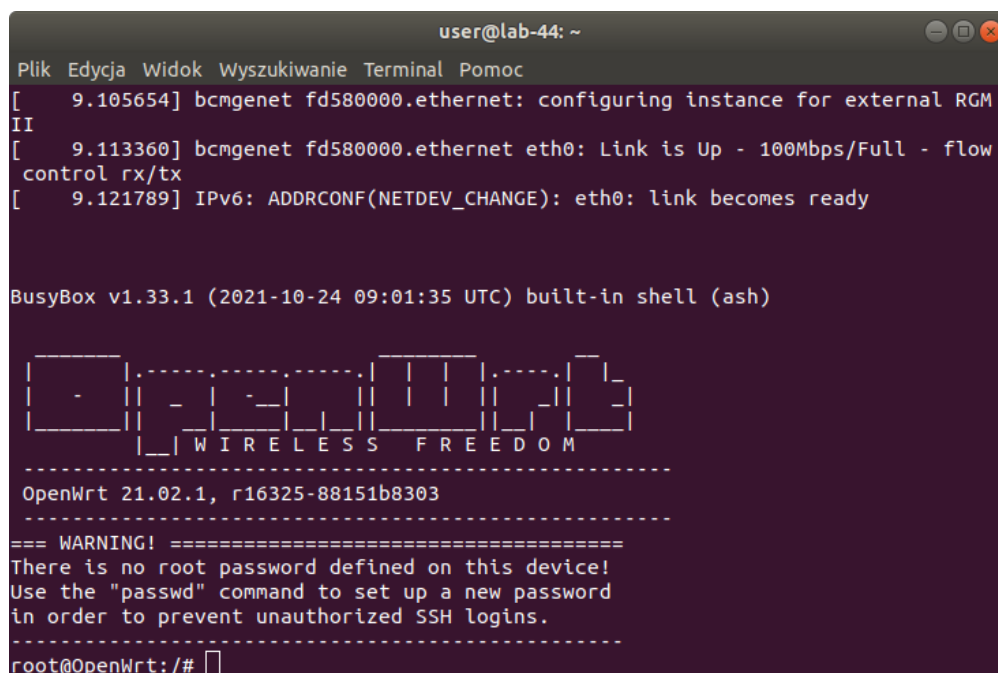
Bogumił Stoma, 325233

---

Raport wygenerowany automatycznie z pliku raport.md

## OpenWRT

Sprawdziliśmy czy system OpenWRT z poprzednich labów się odpala



```
user@lab-44: ~
Plik Edycja Widok Wyszukiwanie Terminal Pomoc
[ 9.105654] bcmgenet fd580000.ethernet: configuring instance for external RGM
II
[ 9.113360] bcmgenet fd580000.ethernet eth0: Link is Up - 100Mbps/Full - flow
control rx/tx
[ 9.121789] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready

BusyBox v1.33.1 (2021-10-24 09:01:35 UTC) built-in shell (ash)

  _   _   _   _   _   _   _   _   _   _   _   _   _   _   _   _   _   _
 | |   | |   | |   | |   | |   | |   | |   | |   | |   | |   | |   | | | | | | | | | | |
 | |_|  | |_|  | |_|  | |_|  | |_|  | |_|  | |_|  | |_|  | |_|  | |_|  | |_|
 |  _  |  _  |  _  |  _  |  _  |  _  |  _  |  _  |  _  |  _  |  _  |
 | |_|  | |_|  | |_|  | |_|  | |_|  | |_|  | |_|  | |_|  | |_|  | |_|  | |_|
 |_|   |_|   |_|   |_|   |_|   |_|   |_|   |_|   |_|   |_|   |_|   |_|   |_|
  |_|   |_|   |_|   |_|   |_|   |_|   |_|   |_|   |_|   |_|   |_|   |_|

OpenWrt 21.02.1, r16325-88151b8303
=====
=== WARNING! =====
There is no root password defined on this device!
Use the "passwd" command to set up a new password
in order to prevent unauthorized SSH logins.
=====
root@OpenWrt:/#
```

## Pierwszy pakiet

Pobraliśmy odpowiednią wersję SDK z

<https://downloads.openwrt.org/releases/21.02.1/targets/bcm27xx/bcm2711/>

---

Dodaliśmy do pliku feeds.conf.default ścieżkę do katalogu zawierającego katalogi z naszymi pakietami:

```
nano feeds.conf.default
```

Dodaliśmy ścieżkę do tego pliku:

```
src-link skps /home/user/Pulpit/openwrt.../demo1_owrt_pkg
```

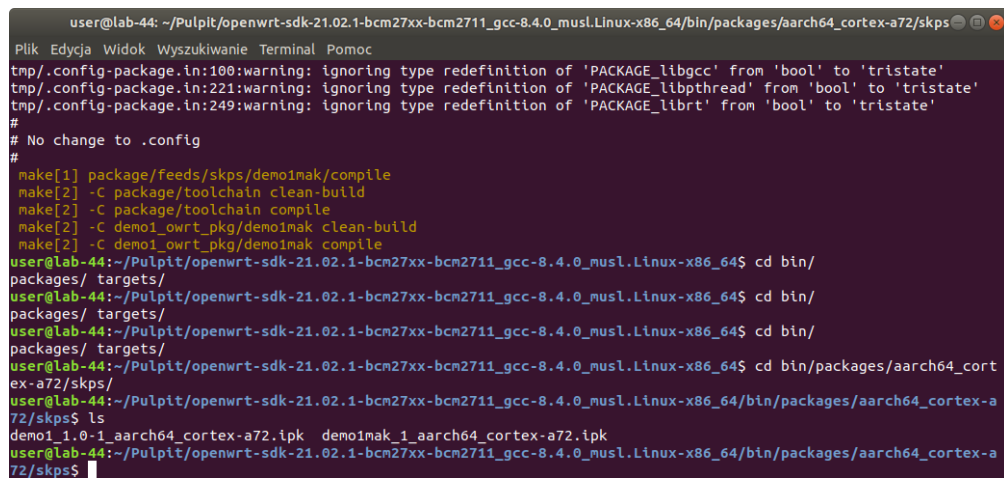
Zaktualizowaliśmy listy pakietów

```
export LANG=C
./scripts/feeds update -a
./scripts/feeds install -p skps -a
```

## Kompilacja paczek

```
make package/feeds/skps/demo1/compile
make package/feeds/skps/demo1mak/compile
```

## Skompilowane pakiety:



```
user@lab-44: ~/Pulpit/openwrt-sdk-21.02.1-bcm27xx-bcm2711_gcc-8.4.0_musl.Linux-x86_64/bin/packages/aarch64_cortex-a72/skps
Plik Edycja Widok Wyszukiwanie Terminal Pomoc
tmp/.config-package.in:100:warning: ignoring type redefinition of 'PACKAGE_libgcc' from 'bool' to 'tristate'
tmp/.config-package.in:221:warning: ignoring type redefinition of 'PACKAGE_libpthread' from 'bool' to 'tristate'
tmp/.config-package.in:249:warning: ignoring type redefinition of 'PACKAGE_librt' from 'bool' to 'tristate'
#
# No change to .config
#
make[1] package/feeds/skps/demo1mak/compile
make[2] -C package/toolchain clean-build
make[2] -C package/toolchain compile
make[2] -C demo1_owrt_pkg/demo1mak clean-build
make[2] -C demo1_owrt_pkg/demo1mak compile
user@lab-44: ~/Pulpit/openwrt-sdk-21.02.1-bcm27xx-bcm2711_gcc-8.4.0_musl.Linux-x86_64$ cd bin/
packages/ targets/
user@lab-44: ~/Pulpit/openwrt-sdk-21.02.1-bcm27xx-bcm2711_gcc-8.4.0_musl.Linux-x86_64$ cd bin/
packages/ targets/
user@lab-44: ~/Pulpit/openwrt-sdk-21.02.1-bcm27xx-bcm2711_gcc-8.4.0_musl.Linux-x86_64$ cd bin/
packages/ targets/
user@lab-44: ~/Pulpit/openwrt-sdk-21.02.1-bcm27xx-bcm2711_gcc-8.4.0_musl.Linux-x86_64$ cd bin/packages/aarch64_cort
ex-a72/skps/
user@lab-44: ~/Pulpit/openwrt-sdk-21.02.1-bcm27xx-bcm2711_gcc-8.4.0_musl.Linux-x86_64/bin/packages/aarch64_cortex-a
72/skps$ ls
demo1_1.0-1_aarch64_cortex-a72.ipk  demo1mak_1_aarch64_cortex-a72.ipk
user@lab-44: ~/Pulpit/openwrt-sdk-21.02.1-bcm27xx-bcm2711_gcc-8.4.0_musl.Linux-x86_64/bin/packages/aarch64_cortex-a
72/skps$
```

## Skorzystaliśmy z serwera http do przeniesiania plików



Przenieśliśmy paczkę demo1 w postaci pliku .ipk na RPi i ją zainstalowaliśmy i odpaliliśmy

```
user@lab-44: ~  
Plik Edycja Widok Wyszukiwanie Terminal Pomoc  
in order to prevent unauthorized SSH logins.  
-----  
root@OpenWrt:/#  
root@OpenWrt:/# wget http://10.42.0.1:8000/demo1_1.0-1_aarch64_cortex-a72.ipk  
Downloading 'http://10.42.0.1:8000/demo1_1.0-1_aarch64_cortex-a72.ipk'  
Connecting to 10.42.0.1:8000  
Writing to 'demo1_1.0-1_aarch64_cortex-a72.ipk'  
demo1_1.0-1_aarch64_ 100% |*****| 2018 0:00:00 ETA  
Download completed (2018 bytes)  
root@OpenWrt:/# opkg install demo1_1.0-1_aarch64_cortex-a72.ipk  
Installing demo1 (1.0-1) to root...  
Configuring demo1.  
root@OpenWrt:/# demo1  
dzien dobry  
Komunikat z wątku A  
Komunikat z wątku B  
Komunikat z wątku B  
Komunikat z wątku A  
Komunikat z wątku B  
Komunikat z wątku B  
Komunikat z wątku A  
^C  
root@OpenWrt:/#
```

## Pakiety worms i buggy

Pobraliśmy katalogi z programami worms i buggy i umieściliśmy je w tym samym miejscu co poprzednio demo1 i demo1mak

W katalogach **buggy** i **worms** umieściliśmy pliki Makefile, zrobiliśmy je wzorując się na Makefile z **demo1**

Aktualizacja i kompilacja paczek

```
export LANG=C  
./scripts/feeds update -a  
./scripts/feeds install -p skps -a  
make package/feeds/skps/worms/compile  
make package/feeds/skps/buggy/compile
```

Instalacja pakietów po ich przeniesieniu (zrobiliśmy to tym samym sposobem co poprzednio)

```
opkg install worms_1.0-1_aarch64_cortex-a72.ipk  
opkg install buggy_1.0-1_aarch64_cortex-a72.ipk
```

Działanie programów:

Odpalenie wormsów:

```
user@lab-44: ~  
Plik Edycja Widok Wyszukiwanie Terminal Pomoc  
X  
  
00  
00  
0000  
  
You ran into yourself!  
Your score is 16  
root@OpenWrt:/#
```

Odpalenie plików z bugami:

```
user@lab-44: ~  
Plik Edycja Widok Wyszukiwanie Terminal Pomoc  
etc/ worms_1.0-1_aarch64_cortex-a72.ipk  
lib/ www/  
lib64/ zad1.py  
lost+found/ zad2.py  
mnt/ zad22.py  
overlay/ zad3.py  
proc/ zad4.py  
rom/ zad5.py  
root/  
root@OpenWrt:/# opkg install worms_1.0-1_aarch64_cortex-a72.ipk  
Installing worms (1.0-1) to root...  
Configuring worms.  
root@OpenWrt:/# opkg install buggy_1.0-1_aarch64_cortex-a72.ipk  
Installing buggy (1.0-1) to root...  
Configuring buggy.  
root@OpenWrt:/# bug1  
Segmentation fault  
root@OpenWrt:/# bug2  
Segmentation fault  
root@OpenWrt:/# bug3  
s1=@ABCDEFGHJKLMNOPQRSTUVWXYZ  
s2=JKLMNOPQRSTUVWXYZ  
root@OpenWrt:/#
```

## Debugowanie zdalne

Sprawdziliśmy nasze IP:

```
ip_hosta: 10.42.0.1  
ip_RPi: 10.42.0.63
```

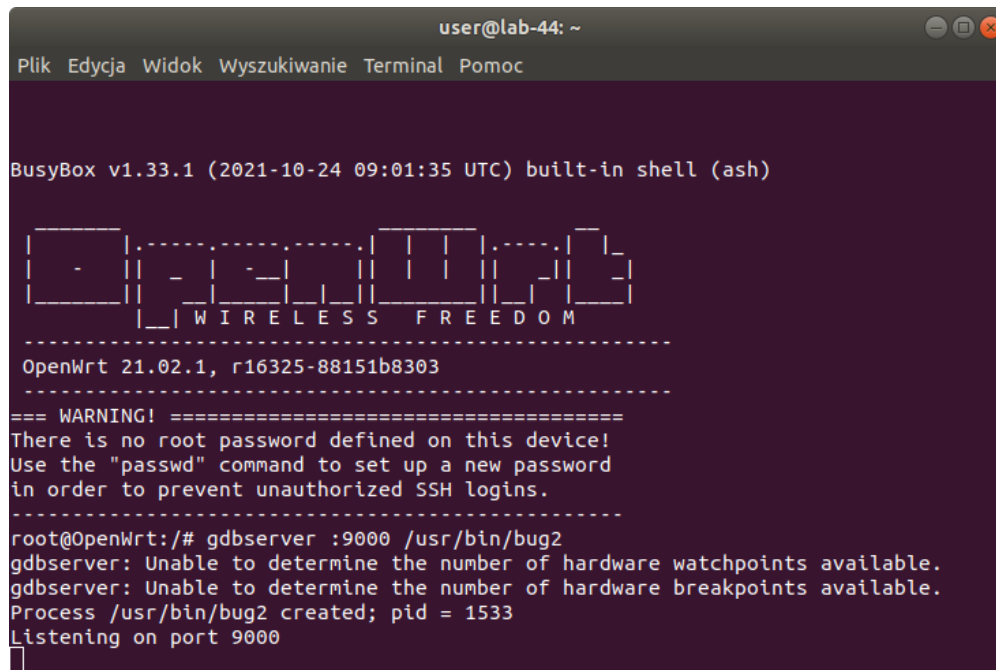
Pobraliśmy na RPi potrzebne pakiety

```
opkg update  
opkg install gdb  
opkg install gdbserver
```

Odpaliliśmy serwer gdb na RPi (przykład dla pliku bug2)

```
gdbserver :9000 /usr/bin/bug2
```

Przykładowe odpalenie serwera dla pliku wykonywalnego bug2



```
user@lab-44: ~  
Plik Edycja Widok Wyszukiwanie Terminal Pomoc  
BusyBox v1.33.1 (2021-10-24 09:01:35 UTC) built-in shell (ash)  
-  
|_| W I R E L E S S F R E E D O M  
-----  
OpenWrt 21.02.1, r16325-88151b8303  
==== WARNING! =====  
There is no root password defined on this device!  
Use the "passwd" command to set up a new password  
in order to prevent unauthorized SSH logins.  
-----  
root@OpenWrt:/# gdbserver :9000 /usr/bin/bug2  
gdbserver: Unable to determine the number of hardware watchpoints available.  
gdbserver: Unable to determine the number of hardware breakpoints available.  
Process /usr/bin/bug2 created; pid = 1533  
Listening on port 9000
```

Połączenie do serwera gdb z komputera hosta (analogicznie dla innych programów) - 10.42.0.63 to ip RPi

```
./scripts/remote-gdb 10.42.0.63:9000 ./build_dir/target-aarch64_cortex-  
a72_musl/buggy-1.0/bug2
```

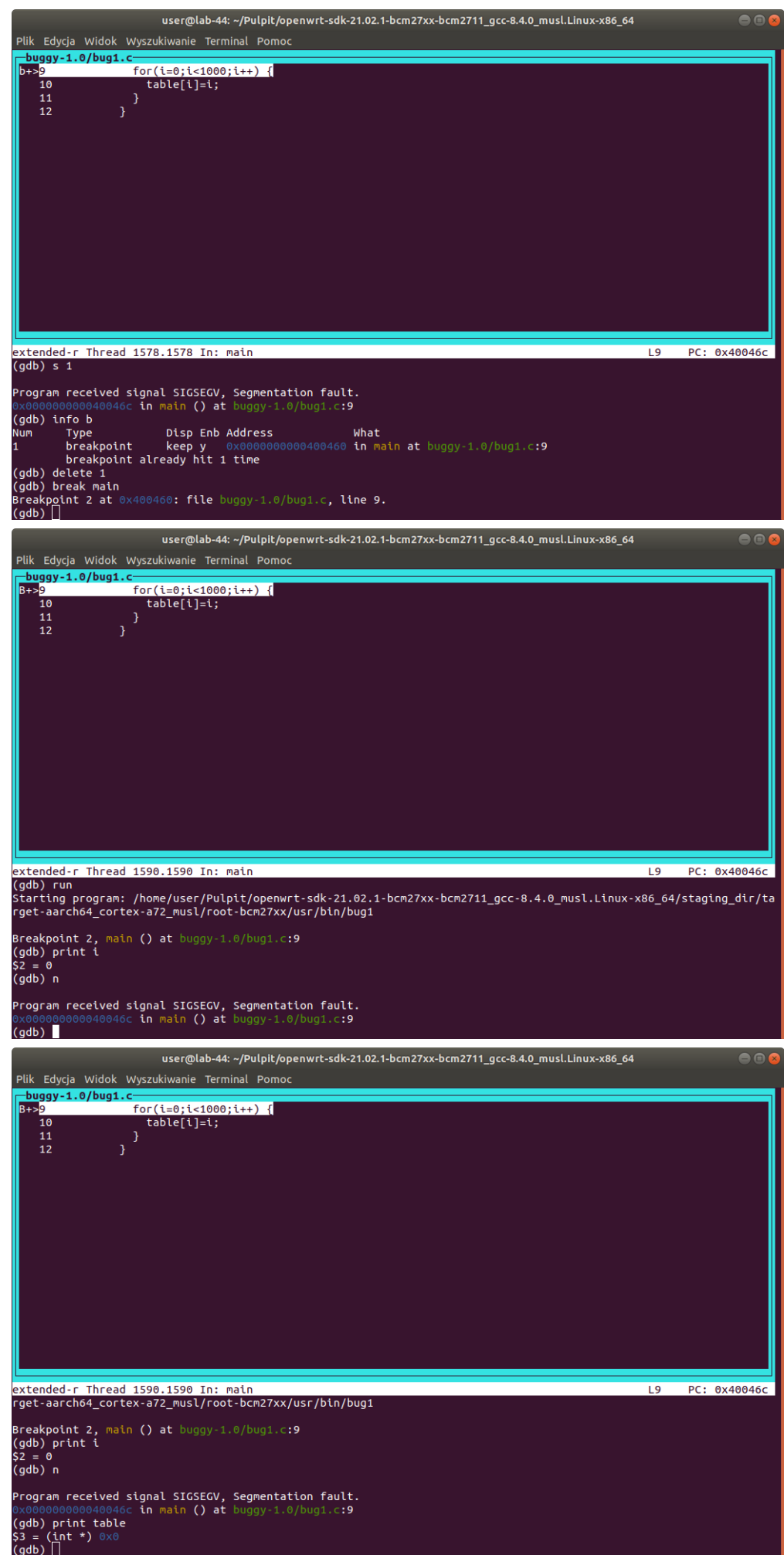
Po połączeniu z komputera hosta ustawiliśmy katalog dla gdb, w którym ma szukać kodu:

```
directory /home/user/Puplit/openwrt.../demo1_owrt_pkg/buggy/src
```

## Program bug1

Na czym polegał bug1 - (Segmentation fault) zapis do niezaalokowanej tablicy

Przedstawienie debugowania:



## Program bug2

Na czym polegał bug2 - (Segmentation fault) wyjście poza zakres tablicy

Przedstawienie debugowania:

```

user@lab-44: ~/Pulpit/openwrt-sdk-21.02.1-bcm27xx-bcm2711_gcc-8.4.0_musl.Linux-x86_64
Plik Edycja Widok Wyszukiwanie Terminal Pomoc
No symbol table is loaded. Use the "file" command.
Make breakpoint pending on future shared library load? (y or [n]) n
(gdb) break main
No symbol table is loaded. Use the "file" command.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 1 (main) pending.
(gdb) run
Starting program:
Reading symbols from /home/user/Pulpit/openwrt-sdk-21.02.1-bcm27xx-bcm2711_gcc-8.4.0_musl.Linux-x86_64/scripts/../
staging_dir/target-aarch64_cortex-a72_musl/root-bcm27xx/usr/bin/bug2...

Breakpoint 1, main () at buggy-1.0/bug2.c:7
7       for(i=0;i<1000000;i++) {
(gdb) watch i==999
Watchpoint 2: i==999
(gdb) display i
1: i = 0
(gdb) continue
Continuing.

Watchpoint 2: i==999

Old value = 0
New value = 1
main () at buggy-1.0/bug2.c:7
7       for(i=0;i<1000000;i++) {
1: i = 999
(gdb)
Continuing.

Watchpoint 2: i==999

Old value = 1
New value = 0
main () at buggy-1.0/bug2.c:7
7       for(i=0;i<1000000;i++) {
1: i = 1000
(gdb) print table[999]
$1 = 999
(gdb) print table[1000]
$2 = 0
(gdb) n
8           table[i]=i;
1: i = 1000
(gdb) n
7       for(i=0;i<1000000;i++) {
1: i = 1001
(gdb) print table[1000]
$3 = 1000
(gdb)

```

```

user@lab-44: ~/Pulpit/openwrt-sdk-21.02.1-bcm27xx-bcm2711_gcc-8.4.0_musl.Linux-x86_64
Plik Edycja Widok Wyszukiwanie Terminal Pomoc
main () at buggy-1.0/bug2.c:7
7       for(i=0;i<1000000;i++) {
1: i = 999
(gdb)
Continuing.

Watchpoint 2: i==999

Old value = 1
New value = 0
main () at buggy-1.0/bug2.c:7
7       for(i=0;i<1000000;i++) {
1: i = 1000
(gdb) print table[999]
$1 = 999
(gdb) print table[1000]
$2 = 0
(gdb) n
8           table[i]=i;
1: i = 1000
(gdb) n
7       for(i=0;i<1000000;i++) {
1: i = 1001
(gdb) print table[1000]
$3 = 1000
(gdb) n
8           table[i]=i;
1: i = 1001
(gdb) n
7       for(i=0;i<1000000;i++) {
1: i = 1002
(gdb) n
8           table[i]=i;
1: i = 1002
(gdb) n
7       for(i=0;i<1000000;i++) {
1: i = 1003
(gdb) n
8           table[i]=i;
1: i = 1003
(gdb) n
7       for(i=0;i<1000000;i++) {
1: i = 1004
(gdb) continue
Continuing.

Program received signal SIGSEGV, Segmentation fault.
main () at buggy-1.0/bug2.c:8
8           table[i]=i;
1: i = 1008
(gdb)

```

## Program bug3



Na czym polegał bug3 - wyjście poza zakres tablicy, brak Segmentation faulta w tym przypadku (nie trafiliśmy na obszar, do którego nie mamy dostępu), od razu po przepełnieniu s1, zaczęliśmy zapisywać do tablicy s2, co wydawało nam się trochę dziwne, że s1 i s2 znajdują się bezpośrednio obok w pamięci

Przedstawienie debugowania:

```
user@lab-44: ~/Pulpit/openwrt-sdk-21.02.1-bcm27xx-bcm2711_gcc-8.4.0_musl.Linux-x86_64
Plik Edycja Widok Wyszukiwanie Terminal Pomoc
Start it from the beginning? (y or n) y
Starting program: /home/user/Pulpit/openwrt-sdk-21.02.1-bcm27xx-bcm2711_gcc-8.4.0_musl.Linux-x86_64/staging_dir/target-aarch64_cortex-a72_musl/root-bcm27xx/usr/bin/bug3

^C
Program received signal SIGINT, Interrupt.
0x0000007fff7fd2a2c in _dlstart_c (sp=0x7ffffffdb0, dynv=<optimized out>) at ldso/dlstart.c:141
141   ldso/dlstart.c: No such file or directory.
(gdb) info b
Num      Type           Disp Enb Address            What
1        breakpoint      keep y   0x00000000004004b0 in main at buggy-1.0/bug3.c:12
3        watchpoint      keep y   s1[10]
(gdb) del 3
(gdb) run
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/user/Pulpit/openwrt-sdk-21.02.1-bcm27xx-bcm2711_gcc-8.4.0_musl.Linux-x86_64/staging_dir/target-aarch64_cortex-a72_musl/root-bcm27xx/usr/bin/bug3

Breakpoint 1, main () at buggy-1.0/bug3.c:12
12   for(i=0;i<24;i++) {
(gdb) watch s1[10]
Watchpoint 4: s1[10]
(gdb) watch s1[11]
Watchpoint 5: s1[11]
(gdb) c
Continuing.

Watchpoint 4: s1[10]

Old value = 97 'a'
New value = 74 'j'
main () at buggy-1.0/bug3.c:12
12   for(i=0;i<24;i++) {
(gdb) c
Continuing.

Watchpoint 5: s1[11]

Old value = 98 'b'
New value = 75 'K'
main () at buggy-1.0/bug3.c:12
12   for(i=0;i<24;i++) {
(gdb) n
13       s1[i]=i+64;
(gdb) n
12   for(i=0;i<24;i++) {
(gdb) backtrace
#0  main () at buggy-1.0/bug3.c:12
(gdb)
```