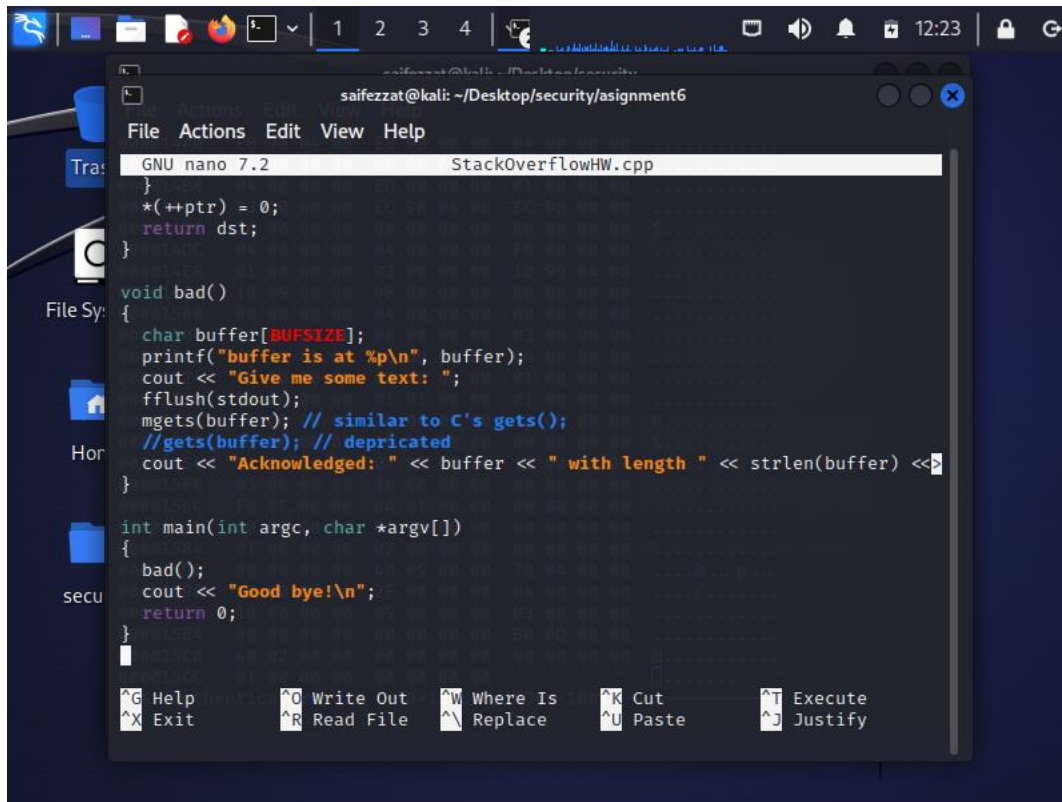


StackOverflow.
Saif Ezzat.



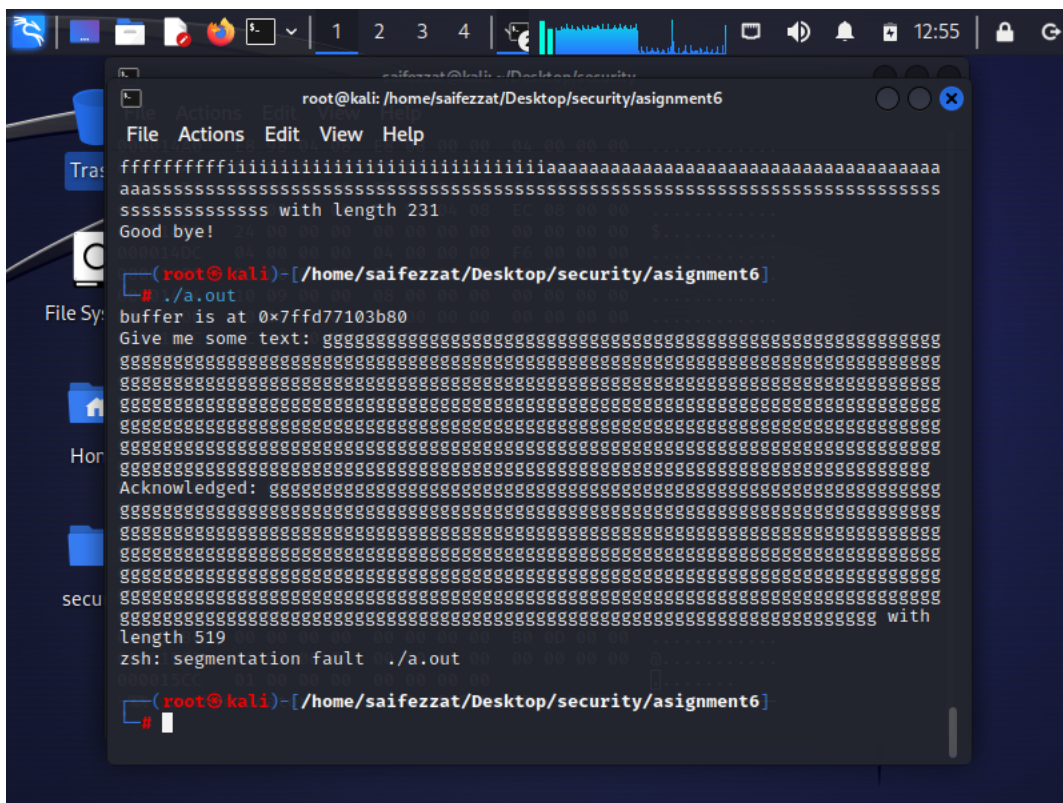
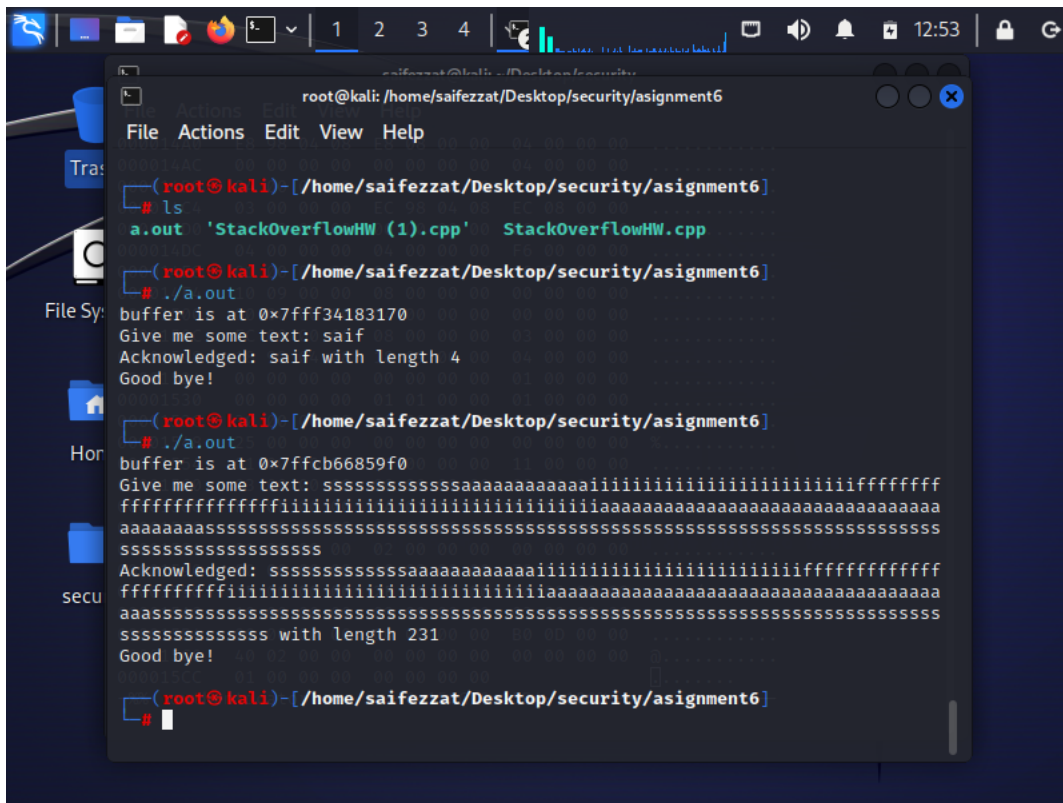
```
saifezzat@kali: ~/Desktop/security/assignment6
GNU nano 7.2 StackOverflowHW.cpp
}
*(++ptr) = 0;
return dst;
}

void bad()
{
    char buffer[BUFSIZE];
    printf("buffer is at %p\n", buffer);
    cout << "Give me some text: ";
    fflush(stdout);
    mgets(buffer); // similar to C's gets();
    //gets(buffer); // deprecated
    cout << "Acknowledged: " << buffer << " with length " << strlen(buffer) << endl;
}

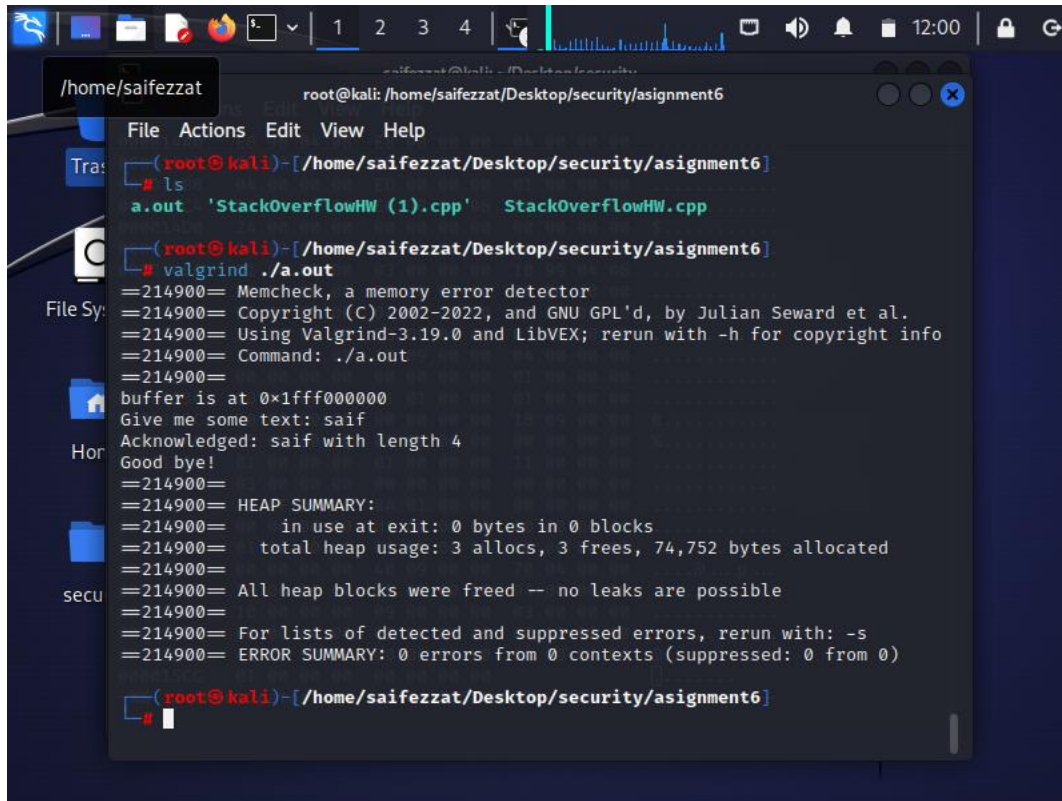
int main(int argc, char *argv[])
{
    bad();
    cout << "Good bye!\n";
    return 0;
}
```

Using nano I was able to examine the code. Clearly we can see a vulnerability in the bad() function it allows user to input any number of items without checking the size of the input which makes the stack vulnerable to overflow.

I executed the program with the security flags disabled like canary and pie. And I passed a valid input and another time an invalid input and the program crashed.



Using valgrind I checked for vulnerabilities and found spaced allocated without being freed after use.

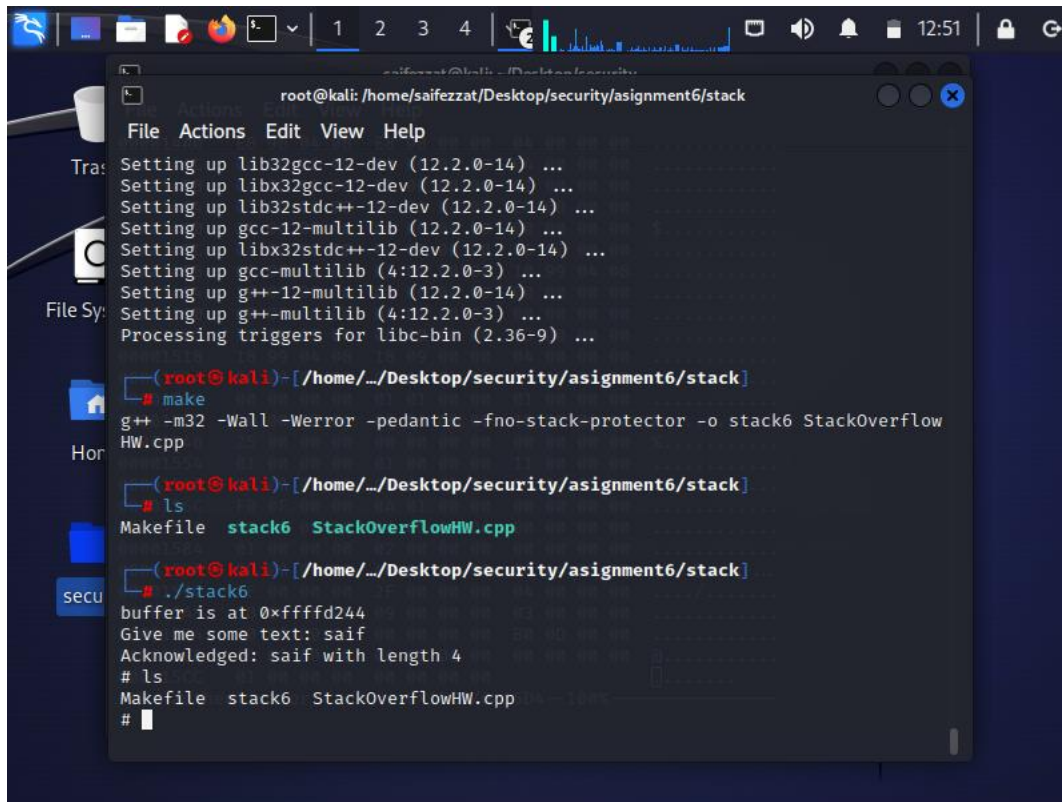


```
root@kali: /home/saifezzat/Desktop/security/assignment6
File Actions Edit View Help
ls
a.out 'StackOverflowHW (1).cpp' StackOverflowHW.cpp
valgrind ./a.out
=214900= Memcheck, a memory error detector
=214900= Copyright (C) 2002-2022, and GNU GPL'd, by Julian Seward et al.
=214900= Using Valgrind-3.19.0 and LibVEX; rerun with -h for copyright info
=214900= Command: ./a.out
=214900=
buffer is at 0x1fff000000
Give me some text: saif
Acknowledged: saif with length 4
Good bye!
=214900=
=214900= HEAP SUMMARY:
=214900=   in use at exit: 0 bytes in 0 blocks
=214900=   total heap usage: 3 allocs, 3 frees, 74,752 bytes allocated
=214900=
=214900= All heap blocks were freed -- no leaks are possible
=214900=
=214900= For lists of detected and suppressed errors, rerun with: -s
=214900= ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
root@kali: /home/saifezzat/Desktop/security/assignment6
```

```
root@kali: /home/saifezzat/Desktop/security/assignment6
File Actions Edit View Help
=====
=====
=====
===== with length 653
=215397= Jump to the invalid address stated on the next line
=215397= at 0x7373737373737373: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= Address 0x7373737373737373 is not stack'd, malloc'd or (recently)
free'd
=215397=
=215397= Process terminating with default action of signal 11 (SIGSEGV)
=215397= Bad permissions for mapped region at address 0x7373737373737373
=215397= at 0x7373737373737373: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
```

```
root@kali: /home/saifezzat/Desktop/security/assignment6
File Actions Edit View Help
=215397= Process terminating with default action of signal 11 (SIGSEGV)
=215397= Bad permissions for mapped region at address 0x7373737373737373
=215397= at 0x7373737373737373: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397= by 0x7373737373737372: ???
=215397=
=215397= HEAP SUMMARY:
=215397= in use at exit: 74,752 bytes in 3 blocks
=215397= total heap usage: 3 allocs, 0 frees, 74,752 bytes allocated
=215397=
=215397= LEAK SUMMARY:
=215397= definitely lost: 0 bytes in 0 blocks
=215397= indirectly lost: 0 bytes in 0 blocks
=215397= possibly lost: 0 bytes in 0 blocks
=215397= still reachable: 74,752 bytes in 3 blocks
=215397= suppressed: 0 bytes in 0 blocks
=215397= Rerun with --leak-check=full to see details of leaked memory
=215397=
```


I changed the permission on the file using `chmod` and `chown` to have the file owned by root then I passed in some padding + addr in the memory for the pointer of the eip + some `'/x90'` no operation slide then a shell code I was able to create using `shellcraft`.linux.i386



```
root@kali: /home/saifezzat/Desktop/security/assignment6/stack
File Actions Edit View Help
Setting up lib32gcc-12-dev (12.2.0-14) ...
Setting up lib32gcc-12-dev (12.2.0-14) ...
Setting up lib32stdc++-12-dev (12.2.0-14) ...
Setting up gcc-12-multilib (12.2.0-14) ...
Setting up lib32stdc++-12-dev (12.2.0-14) ...
Setting up gcc-multilib (4:12.2.0-3) ...
Setting up g++-12-multilib (12.2.0-14) ...
Setting up g++-multilib (4:12.2.0-3) ...
Processing triggers for libc-bin (2.36-9) ...

(root@kali)-[/home/.../Desktop/security/assignment6/stack]
# make
g++ -m32 -Wall -Werror -pedantic -fno-stack-protector -o stack6 StackOverflowHW.cpp

(root@kali)-[/home/.../Desktop/security/assignment6/stack]
# ls
Makefile  stack6  StackOverflowHW.cpp

(root@kali)-[/home/.../Desktop/security/assignment6/stack]
# ./stack6
buffer is at 0xffffd244
Give me some text: saif
Acknowledged: saif with length 4
# ls
Makefile  stack6  StackOverflowHW.cpp
#
```

