

# 4st Homework

≡ 주제	Decompile <code>hello</code> binary and change the string value to print your STUDENT ID
📅 날짜	@2024년 10월 11일
≡ 유형	과제
↗ 2학기 학교 공부	<u>Computer System</u>

```
CS22102009@nshcdell:~/hw04$ strings hello | grep "Hello"
Hello, World!
CS22102009@nshcdell:~/hw04$ objdump -s -j .rodata hello
hello:      file format elf64-x86-64

Contents of section .rodata:
 2000 01000200 48656c6c 6f2c2057 6f726c64  ....Hello, World
 2010 2100                                !.
CS22102009@nshcdell:~/hw04$ xxd hello > hello.hex
CS22102009@nshcdell:~/hw04$ vim hello.hex

[4]+  Stopped                  vim hello.hex
CS22102009@nshcdell:~/hw04$ vim hello.hex
1044L, 70984C written
CS22102009@nshcdell:~/hw04$ xxd -r hello.hex hello
CS22102009@nshcdell:~/hw04$ ./hello
-bash: ./hello: Permission denied
CS22102009@nshcdell:~/hw04$ chmod +x hello
CS22102009@nshcdell:~/hw04$ ./hello
22102009
```

## 1. Find the string in the binary file

First, we need to search for readable string(in this case Hello, World!) in the binary file.

```
strings hello | grep "Hello"
```

⬆ This code helps locate the string that needs to be modified

```
CS22102009@nshcdell:~/hw04$ strings hello | grep "Hello"
Hello, World!
```

In this case, it revealed the **Hello, World!** string in the binary file.

## 2. Inspecting the `.rodata` segment

```
objdump -s -j .rodata hello
```

I used the `objdump` command to examine the `.rodata` section of the binary. The `.rodata` segment stores read-only data, which includes the string we want to modify. (In this case Hello, World!)

```
CS22102009@nshcdell:~/hw04$ objdump -s -j .rodata hello
hello:      file format elf64-x86-64

Contents of section .rodata:
 2000 01000200 48656c6c 6f2c2057 6f726c64  ....Hello, World
 2010 2100                                !.
```

I should find section starts with 2000 1000200.

## 3. Dumping the binary to Hexadecimal

```
xxd hello > hello.hex
```

## 4. Edit the file

I used vim editor to edit file.

```
vim hello.hex
```

⬇ When we just open the file we can find Hello, World! code in this section.

```
00001ff0: 0000 0000 0000 0000 0000 0000 0000 0000  ....
00002000: 0100 0200 4865 6c6c 6f2c 2057 6f72 6c64  ....Hello, World
00002010: 2100 0000 011b 033b 4000 0000 0700 0000  !.....;@.....
```

⬇ Change code like this to print my studentID: 22102009

```
00001ff0: 0000 0000 0000 0000 0000 0000 0000 0000  ....
00002000: 0100 0200 3232 3130 3230 3039 0000 0000  ....22102009...|.
00002010: 2100 0000 011b 033b 4000 0000 0700 0000  !.....;@.....
```

save and close the file.

## 5. Convert back to binary file

```
xxd -r hello.hex hello
```

## 6. Add Execution Permission

In my computer, it said it has no permission to execute file. So, I add execution permission.

## 7. ./hello and execute file

```
CS22102009@nshcdell:~/hw04$ ./hello  
22102009
```

↑It prints out my student ID.