

# ENPM691 Homework 09: Exploiting Format String Vulnerability with Direct GOT Overwrite

Kalpesh Parmar  
M.Eng Cybersecurity  
University [REDACTED]e Park  
[REDACTED]  
UMD Directory ID [REDACTED]  
Course and section - ENPM691 0101

**Abstract**—In this assignment, I explored a format string vulnerability in a 32-bit compiled C program and used it to redirect program execution to a custom function with elevated privileges. I explain step-by-step the exploitation process, system configuration, compilation commands, debugging steps, and payload construction. References to relevant course materials and documentation are included [1][2][3].

## I. INTRODUCTION

I implemented a format string attack to redirect a vulnerable program's execution flow to a custom target function. This target function executes a child process with root privileges to print a message. All operations were conducted in a controlled Kali-Linux-2025.2 environment using gcc 14.3.0 with multilib support and GDB 16.3 with the pwndbg extension [1].

## II. SYSTEM CONFIGURATION

- **Operating System:** Kali-Linux-2025.2
- **Compiler:** gcc 14.3.0 (Debian 14.3.0-5) with multilib
- **Debugger:** GDB 16.3 with pwndbg extension
- **Architecture:** Compiled and executed in 32-bit mode

## III. COMPILATION

I compiled the program with the following command:

```
gcc -m32 -fno-stack-protector -no-pie -Wl,-z,norelro -g directPrintf.c -o directPrintf
```

### Explanation:

- `-m32`: Compile as 32-bit
- `-g`: Include debug symbols for GDB
- `-fno-stack-protector`: Disable stack canaries to allow exploitation
- `-no-pie`: Disable position independent executable for fixed addresses
- `-Wl,-z,norelro`: Disable RELRO (read-only relocations) to allow GOT overwrite

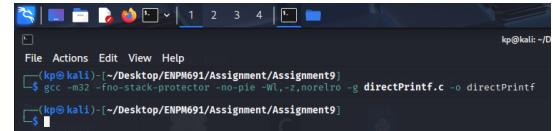


Fig. 1: Compilation output showing no errors and the program ready for exploitation.

## IV. SETTING SUID BIT

To execute the program with root privileges, I set the SUID bit:

```
sudo chown root:root directPrintf
sudo chmod u+s directPrintf
ls -ll
```

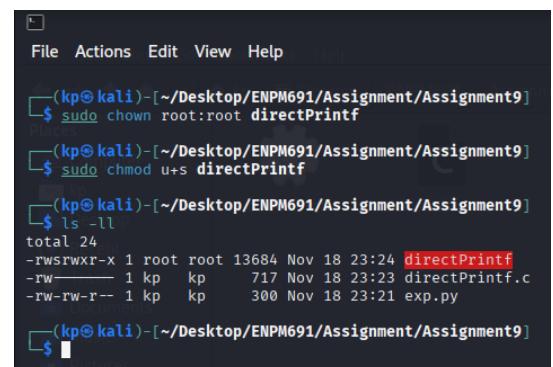


Fig. 2: SUID bit set on directPrintf for root execution.

## V. DISABLING ASLR

I disabled Address Space Layout Randomization (ASLR) to make exploitation deterministic:

```
sudo sysctl -w kernel.randomize_va_space=0
cat /proc/sys/kernel/randomize_va_space
```

```

File Actions Edit View Help
(kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment9]
$ sudo chmod root:root directPrintf
(kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment9]
$ sudo chmod u+s directPrintf
(kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment9]
$ ls -l
total 24
-rwsrwxr-x 1 root root 13684 Nov 18 23:24 directPrintf
-rw-r--r-- 1 kp kp 717 Nov 18 23:23 directPrintf.c
-rw-rw-r-- 1 kp kp 300 Nov 18 23:21 exp.py
(kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment9]
$ sudo sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
(kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment9]
$ cat /proc/sys/kernel/randomize_va_space
0

```

Fig. 3: ASLR disabled to ensure predictable memory addresses.

## VI. VULNERABILITY ANALYSIS AND TARGET ADDRESS

I analyzed the target function to determine its address for the exploit.

```

(kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment9]
$ objdump -R directPrintf | grep target
08049206 <target>:    75 4b      jne    80492b8 <target+0x85>

```

Fig. 4: Target function address obtained from objdump [1].

I also located the GOT entry for putchar:

```

(kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment9]
$ objdump -R directPrintf | grep putchar
0804b2a8 R_386_JUMP_SLOT putchar@GLIBC_2.0

```

Fig. 5: GOT entry of putchar used for redirection [2].

## VII. STACK OFFSET IDENTIFICATION

I used a test payload to determine the correct stack offset for the format string:

```

(kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment9]
$ ./directPrintf AAAA-0x4ffffd1c3-0xf7fffcfec-0x80492bc-0x41414141-0x2d70252d-0x252d7025-0x78252d78
Normal execution

```

Fig. 6: Stack inspection showing memory addresses and offsets for payload [2].

## VIII. DISASSEMBLY AND BREAKPOINTS

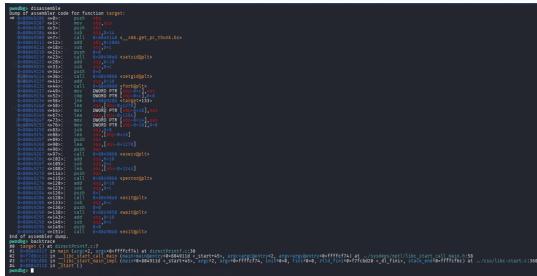
I disassembled main() and target() functions to confirm the vulnerable line and set breakpoints:

```

Disassembly of section .text:
00401000 <main>:
    0:    .text
    1:    .file   "/tmp/gdb-pwngdb-14444"
    2:    .section    ".rodata", "r"
    3:    .align   1, .LC0
    4:    .string  "%c\n"
    5:    .text
    6:    .globl   _start
    7:    .type    _start, %function
    8:    .size    _start, .-_
    9:    .text
   10:   .globl   _start_main
   11:   .type    _start_main, %function
   12:   .size    _start_main, .-_
   13:   .text
   14:   .globl   _start_main1
   15:   .type    _start_main1, %function
   16:   .size    _start_main1, .-_
   17:   .text
   18:   .globl   _start_main16
   19:   .type    _start_main16, %function
   20:   .size    _start_main16, .-_
   21:   .text
   22:   .globl   _start_main17
   23:   .type    _start_main17, %function
   24:   .size    _start_main17, .-_
   25:   .text
   26:   .globl   _start_main18
   27:   .type    _start_main18, %function
   28:   .size    _start_main18, .-_
   29:   .text
   30:   .globl   _start_main19
   31:   .type    _start_main19, %function
   32:   .size    _start_main19, .-_
   33:   .text
   34:   .globl   _start_main20
   35:   .type    _start_main20, %function
   36:   .size    _start_main20, .-_
   37:   .text
   38:   .globl   _start_main21
   39:   .type    _start_main21, %function
   40:   .size    _start_main21, .-_
   41:   .text
   42:   .globl   _start_main22
   43:   .type    _start_main22, %function
   44:   .size    _start_main22, .-_
   45:   .text
   46:   .globl   _start_main23
   47:   .type    _start_main23, %function
   48:   .size    _start_main23, .-_
   49:   .text
   50:   .globl   _start_main24
   51:   .type    _start_main24, %function
   52:   .size    _start_main24, .-_
   53:   .text
   54:   .globl   _start_main25
   55:   .type    _start_main25, %function
   56:   .size    _start_main25, .-_
   57:   .text
   58:   .globl   _start_main26
   59:   .type    _start_main26, %function
   60:   .size    _start_main26, .-_
   61:   .text
   62:   .globl   _start_main27
   63:   .type    _start_main27, %function
   64:   .size    _start_main27, .-_
   65:   .text
   66:   .globl   _start_main28
   67:   .type    _start_main28, %function
   68:   .size    _start_main28, .-_
   69:   .text
   70:   .globl   _start_main29
   71:   .type    _start_main29, %function
   72:   .size    _start_main29, .-_
   73:   .text
   74:   .globl   _start_main30
   75:   .type    _start_main30, %function
   76:   .size    _start_main30, .-_
   77:   .text
   78:   .globl   _start_main31
   79:   .type    _start_main31, %function
   80:   .size    _start_main31, .-_
   81:   .text
   82:   .globl   _start_main32
   83:   .type    _start_main32, %function
   84:   .size    _start_main32, .-_
   85:   .text
   86:   .globl   _start_main33
   87:   .type    _start_main33, %function
   88:   .size    _start_main33, .-_
   89:   .text
   90:   .globl   _start_main34
   91:   .type    _start_main34, %function
   92:   .size    _start_main34, .-_
   93:   .text
   94:   .globl   _start_main35
   95:   .type    _start_main35, %function
   96:   .size    _start_main35, .-_
   97:   .text
   98:   .globl   _start_main36
   99:   .type    _start_main36, %function
   100:  .size   _start_main36, .-_
   101:  .text
   102:  .globl   _start_main37
   103:  .type    _start_main37, %function
   104:  .size   _start_main37, .-_
   105:  .text
   106:  .globl   _start_main38
   107:  .type    _start_main38, %function
   108:  .size   _start_main38, .-_
   109:  .text
   110:  .globl   _start_main39
   111:  .type    _start_main39, %function
   112:  .size   _start_main39, .-_
   113:  .text
   114:  .globl   _start_main40
   115:  .type    _start_main40, %function
   116:  .size   _start_main40, .-_
   117:  .text
   118:  .globl   _start_main41
   119:  .type    _start_main41, %function
   120:  .size   _start_main41, .-_
   121:  .text
   122:  .globl   _start_main42
   123:  .type    _start_main42, %function
   124:  .size   _start_main42, .-_
   125:  .text
   126:  .globl   _start_main43
   127:  .type    _start_main43, %function
   128:  .size   _start_main43, .-_
   129:  .text
   130:  .globl   _start_main44
   131:  .type    _start_main44, %function
   132:  .size   _start_main44, .-_
   133:  .text
   134:  .globl   _start_main45
   135:  .type    _start_main45, %function
   136:  .size   _start_main45, .-_
   137:  .text
   138:  .globl   _start_main46
   139:  .type    _start_main46, %function
   140:  .size   _start_main46, .-_
   141:  .text
   142:  .globl   _start_main47
   143:  .type    _start_main47, %function
   144:  .size   _start_main47, .-_
   145:  .text
   146:  .globl   _start_main48
   147:  .type    _start_main48, %function
   148:  .size   _start_main48, .-_
   149:  .text
   150:  .globl   _start_main49
   151:  .type    _start_main49, %function
   152:  .size   _start_main49, .-_
   153:  .text
   154:  .globl   _start_main50
   155:  .type    _start_main50, %function
   156:  .size   _start_main50, .-_
   157:  .text
   158:  .globl   _start_main51
   159:  .type    _start_main51, %function
   160:  .size   _start_main51, .-_
   161:  .text
   162:  .globl   _start_main52
   163:  .type    _start_main52, %function
   164:  .size   _start_main52, .-_
   165:  .text
   166:  .globl   _start_main53
   167:  .type    _start_main53, %function
   168:  .size   _start_main53, .-_
   169:  .text
   170:  .globl   _start_main54
   171:  .type    _start_main54, %function
   172:  .size   _start_main54, .-_
   173:  .text
   174:  .globl   _start_main55
   175:  .type    _start_main55, %function
   176:  .size   _start_main55, .-_
   177:  .text
   178:  .globl   _start_main56
   179:  .type    _start_main56, %function
   180:  .size   _start_main56, .-_
   181:  .text
   182:  .globl   _start_main57
   183:  .type    _start_main57, %function
   184:  .size   _start_main57, .-_
   185:  .text
   186:  .globl   _start_main58
   187:  .type    _start_main58, %function
   188:  .size   _start_main58, .-_
   189:  .text
   190:  .globl   _start_main59
   191:  .type    _start_main59, %function
   192:  .size   _start_main59, .-_
   193:  .text
   194:  .globl   _start_main60
   195:  .type    _start_main60, %function
   196:  .size   _start_main60, .-_
   197:  .text
   198:  .globl   _start_main61
   199:  .type    _start_main61, %function
   200:  .size   _start_main61, .-_
   201:  .text
   202:  .globl   _start_main62
   203:  .type    _start_main62, %function
   204:  .size   _start_main62, .-_
   205:  .text
   206:  .globl   _start_main63
   207:  .type    _start_main63, %function
   208:  .size   _start_main63, .-_
   209:  .text
   210:  .globl   _start_main64
   211:  .type    _start_main64, %function
   212:  .size   _start_main64, .-_
   213:  .text
   214:  .globl   _start_main65
   215:  .type    _start_main65, %function
   216:  .size   _start_main65, .-_
   217:  .text
   218:  .globl   _start_main66
   219:  .type    _start_main66, %function
   220:  .size   _start_main66, .-_
   221:  .text
   222:  .globl   _start_main67
   223:  .type    _start_main67, %function
   224:  .size   _start_main67, .-_
   225:  .text
   226:  .globl   _start_main68
   227:  .type    _start_main68, %function
   228:  .size   _start_main68, .-_
   229:  .text
   230:  .globl   _start_main69
   231:  .type    _start_main69, %function
   232:  .size   _start_main69, .-_
   233:  .text
   234:  .globl   _start_main70
   235:  .type    _start_main70, %function
   236:  .size   _start_main70, .-_
   237:  .text
   238:  .globl   _start_main71
   239:  .type    _start_main71, %function
   240:  .size   _start_main71, .-_
   241:  .text
   242:  .globl   _start_main72
   243:  .type    _start_main72, %function
   244:  .size   _start_main72, .-_
   245:  .text
   246:  .globl   _start_main73
   247:  .type    _start_main73, %function
   248:  .size   _start_main73, .-_
   249:  .text
   250:  .globl   _start_main74
   251:  .type    _start_main74, %function
   252:  .size   _start_main74, .-_
   253:  .text
   254:  .globl   _start_main75
   255:  .type    _start_main75, %function
   256:  .size   _start_main75, .-_
   257:  .text
   258:  .globl   _start_main76
   259:  .type    _start_main76, %function
   260:  .size   _start_main76, .-_
   261:  .text
   262:  .globl   _start_main77
   263:  .type    _start_main77, %function
   264:  .size   _start_main77, .-_
   265:  .text
   266:  .globl   _start_main78
   267:  .type    _start_main78, %function
   268:  .size   _start_main78, .-_
   269:  .text
   270:  .globl   _start_main79
   271:  .type    _start_main79, %function
   272:  .size   _start_main79, .-_
   273:  .text
   274:  .globl   _start_main80
   275:  .type    _start_main80, %function
   276:  .size   _start_main80, .-_
   277:  .text
   278:  .globl   _start_main81
   279:  .type    _start_main81, %function
   280:  .size   _start_main81, .-_
   281:  .text
   282:  .globl   _start_main82
   283:  .type    _start_main82, %function
   284:  .size   _start_main82, .-_
   285:  .text
   286:  .globl   _start_main83
   287:  .type    _start_main83, %function
   288:  .size   _start_main83, .-_
   289:  .text
   290:  .globl   _start_main84
   291:  .type    _start_main84, %function
   292:  .size   _start_main84, .-_
   293:  .text
   294:  .globl   _start_main85
   295:  .type    _start_main85, %function
   296:  .size   _start_main85, .-_
   297:  .text
   298:  .globl   _start_main86
   299:  .type    _start_main86, %function
   300:  .size   _start_main86, .-_
   301:  .text
   302:  .globl   _start_main87
   303:  .type    _start_main87, %function
   304:  .size   _start_main87, .-_
   305:  .text
   306:  .globl   _start_main88
   307:  .type    _start_main88, %function
   308:  .size   _start_main88, .-_
   309:  .text
   310:  .globl   _start_main89
   311:  .type    _start_main89, %function
   312:  .size   _start_main89, .-_
   313:  .text
   314:  .globl   _start_main90
   315:  .type    _start_main90, %function
   316:  .size   _start_main90, .-_
   317:  .text
   318:  .globl   _start_main91
   319:  .type    _start_main91, %function
   320:  .size   _start_main91, .-_
   321:  .text
   322:  .globl   _start_main92
   323:  .type    _start_main92, %function
   324:  .size   _start_main92, .-_
   325:  .text
   326:  .globl   _start_main93
   327:  .type    _start_main93, %function
   328:  .size   _start_main93, .-_
   329:  .text
   330:  .globl   _start_main94
   331:  .type    _start_main94, %function
   332:  .size   _start_main94, .-_
   333:  .text
   334:  .globl   _start_main95
   335:  .type    _start_main95, %function
   336:  .size   _start_main95, .-_
   337:  .text
   338:  .globl   _start_main96
   339:  .type    _start_main96, %function
   340:  .size   _start_main96, .-_
   341:  .text
   342:  .globl   _start_main97
   343:  .type    _start_main97, %function
   344:  .size   _start_main97, .-_
   345:  .text
   346:  .globl   _start_main98
   347:  .type    _start_main98, %function
   348:  .size   _start_main98, .-_
   349:  .text
   350:  .globl   _start_main99
   351:  .type    _start_main99, %function
   352:  .size   _start_main99, .-_
   353:  .text
   354:  .globl   _start_main100
   355:  .type    _start_main100, %function
   356:  .size   _start_main100, .-_
   357:  .text
   358:  .globl   _start_main101
   359:  .type    _start_main101, %function
   360:  .size   _start_main101, .-_
   361:  .text
   362:  .globl   _start_main102
   363:  .type    _start_main102, %function
   364:  .size   _start_main102, .-_
   365:  .text
   366:  .globl   _start_main103
   367:  .type    _start_main103, %function
   368:  .size   _start_main103, .-_
   369:  .text
   370:  .globl   _start_main104
   371:  .type    _start_main104, %function
   372:  .size   _start_main104, .-_
   373:  .text
   374:  .globl   _start_main105
   375:  .type    _start_main105, %function
   376:  .size   _start_main105, .-_
   377:  .text
   378:  .globl   _start_main106
   379:  .type    _start_main106, %function
   380:  .size   _start_main106, .-_
   381:  .text
   382:  .globl   _start_main107
   383:  .type    _start_main107, %function
   384:  .size   _start_main107, .-_
   385:  .text
   386:  .globl   _start_main108
   387:  .type    _start_main108, %function
   388:  .size   _start_main108, .-_
   389:  .text
   390:  .globl   _start_main109
   391:  .type    _start_main109, %function
   392:  .size   _start_main109, .-_
   393:  .text
   394:  .globl   _start_main110
   395:  .type    _start_main110, %function
   396:  .size   _start_main110, .-_
   397:  .text
   398:  .globl   _start_main111
   399:  .type    _start_main111, %function
   400:  .size   _start_main111, .-_
   401:  .text
   402:  .globl   _start_main112
   403:  .type    _start_main112, %function
   404:  .size   _start_main112, .-_
   405:  .text
   406:  .globl   _start_main113
   407:  .type    _start_main113, %function
   408:  .size   _start_main113, .-_
   409:  .text
   410:  .globl   _start_main114
   411:  .type    _start_main114, %function
   412:  .size   _start_main114, .-_
   413:  .text
   414:  .globl   _start_main115
   415:  .type    _start_main115, %function
   416:  .size   _start_main115, .-_
   417:  .text
   418:  .globl   _start_main116
   419:  .type    _start_main116, %function
   420:  .size   _start_main116, .-_
   421:  .text
   422:  .globl   _start_main117
   423:  .type    _start_main117, %function
   424:  .size   _start_main117, .-_
   425:  .text
   426:  .globl   _start_main118
   427:  .type    _start_main118, %function
   428:  .size   _start_main118, .-_
   429:  .text
   430:  .globl   _start_main119
   431:  .type    _start_main119, %function
   432:  .size   _start_main119, .-_
   433:  .text
   434:  .globl   _start_main120
   435:  .type    _start_main120, %function
   436:  .size   _start_main120, .-_
   437:  .text
   438:  .globl   _start_main121
   439:  .type    _start_main121, %function
   440:  .size   _start_main121, .-_
   441:  .text
   442:  .globl   _start_main122
   443:  .type    _start_main122, %function
   444:  .size   _start_main122, .-_
   445:  .text
   446:  .globl   _start_main123
   447:  .type    _start_main123, %function
   448:  .size   _start_main123, .-_
   449:  .text
   450:  .globl   _start_main124
   451:  .type    _start_main124, %function
   452:  .size   _start_main124, .-_
   453:  .text
   454:  .globl   _start_main125
   455:  .type    _start_main125, %function
   456:  .size   _start_main125, .-_
   457:  .text
   458:  .globl   _start_main126
   459:  .type    _start_main126, %function
   460:  .size   _start_main126, .-_
   461:  .text
   462:  .globl   _start_main127
   463:  .type    _start_main127, %function
   464:  .size   _start_main127, .-_
   465:  .text
   466:  .globl   _start_main128
   467:  .type    _start_main128, %function
   468:  .size   _start_main128, .-_
   469:  .text
   470:  .globl   _start_main129
   471:  .type    _start_main129, %function
   472:  .size   _start_main129, .-_
   473:  .text
   474:  .globl   _start_main130
   475:  .type    _start_main130, %function
   476:  .size   _start_main130, .-_
   477:  .text
   478:  .globl   _start_main131
   479:  .type    _start_main131, %function
   480:  .size   _start_main131, .-_
   481:  .text
   482:  .globl   _start_main132
   483:  .type    _start_main132, %function
   484:  .size   _start_main132, .-_
   485:  .text
   486:  .globl   _start_main133
   487:  .type    _start_main133, %function
   488:  .size   _start_main133, .-_
   489:  .text
   490:  .globl   _start_main134
   491:  .type    _start_main134, %function
   492:  .size   _start_main134, .-_
   493:  .text
   494:  .globl   _start_main135
   495:  .type    _start_main135, %function
   496:  .size   _start_main135, .-_
   497:  .text
   498:  .globl   _start_main136
   499:  .type    _start_main136, %function
   500:  .size   _start_main136, .-_
   501:  .text
   502:  .globl   _start_main137
   503:  .type    _start_main137, %function
   504:  .size   _start_main137, .-_
   505:  .text
   506:  .globl   _start_main138
   507:  .type    _start_main138, %function
   508:  .size   _start_main138, .-_
   509:  .text
   510:  .globl   _start_main139
   511:  .type    _start_main139, %function
   512:  .size   _start_main139, .-_
   513:  .text
   514:  .globl   _start_main140
   515:  .type    _start_main140, %function
   516:  .size   _start_main140, .-_
   517:  .text
   518:  .globl   _start_main141
   519:  .type    _start_main141, %function
   520:  .size   _start_main141, .-_
   521:  .text
   522:  .globl   _start_main142
   523:  .type    _start_main142, %function
   524:  .size   _start_main142, .-_
   525:  .text
   526:  .globl   _start_main143
   527:  .type    _start_main143, %function
   528:  .size   _start_main143, .-_
   529:  .text
   530:  .globl   _start_main144
   531:  .type    _start_main144, %function
   532:  .size   _start_main144, .-_
   533:  .text
   534:  .globl   _start_main145
   535:  .type    _start_main145, %function
   536:  .size   _start_main145, .-_
   537:  .text
   538:  .globl   _start_main146
   539:  .type    _start_main146, %function
   540:  .size   _start_main146, .-_
   541:  .text
   542:  .globl   _start_main147
   543:  .type    _start_main147, %function
   544:  .size   _start_main147, .-_
   545:  .text
   546:  .globl   _start_main148
   547:  .type    _start_main148, %function
   548:  .size   _start_main148, .-_
   549:  .text
   550:  .globl   _start_main149
   551:  .type    _start_main149, %function
   552:  .size   _start_main149, .-_
   553:  .text
   554:  .globl   _start_main150
   555:  .type    _start_main150, %function
   556:  .size   _start_main150, .-_
   557:  .text
   558:  .globl   _start_main151
   559:  .type    _start_main151, %function
   560:  .size   _start_main151, .-_
   561:  .text
   562:  .globl   _start_main152
   563:  .type    _start_main152, %function
   564:  .size   _start_main152, .-_
   565:  .text
   566:  .globl   _start_main153
   567:  .type    _start_main153, %function
   568:  .size   _start_main153, .-_
   569:  .text
   570:  .globl   _start_main154
   571:  .type    _start_main154, %function
   572:  .size   _start_main154, .-_
   573:  .text
   574:  .globl   _start_main155
   575:  .type    _start_main155, %function
   576:  .size   _start_main155, .-_
   577:  .text
   578:  .globl   _start_main156
   579:  .type    _start_main156, %function
   580:  .size   _start_main156, .-_
   581:  .text
   582:  .globl   _start_main157
   583:  .type    _start_main157, %function
   584:  .size   _start_main157, .-_
   585:  .text
   586:  .globl   _start_main158
   587:  .type    _start_main158, %function
   588:  .size   _start_main158, .-_
   589:  .text
   590:  .globl   _start_main159
   591:  .type    _start_main159, %function
   592:  .size   _start_main159, .-_
   593:  .text
   594:  .globl   _start_main160
   595:  .type    _start_main160, %function
   596:  .size   _start_main160, .-_
   597:  .text
   598:  .globl   _start_main161
   599:  .type    _start_main161, %function
   600:  .size   _start_main161, .-_
   601:  .text
   602:  .globl   _start_main162
   603:  .type    _start_main162, %function
   604:  .size   _start_main162, .-_
   605:  .text
   606:  .globl   _start_main163
   607:  .type    _start_main163, %function
   608:  .size   _start_main163, .-_
   609:  .text
   610:  .globl   _start_main164
   611:  .type    _start_main164, %function
   612:  .size   _start_main164, .-_
   613:  .text
   614:  .globl   _start_main165
  
```

## XI. TARGET FUNCTION EXECUTION

After successfully overwriting the GOT entry of putchar, execution redirected to target():

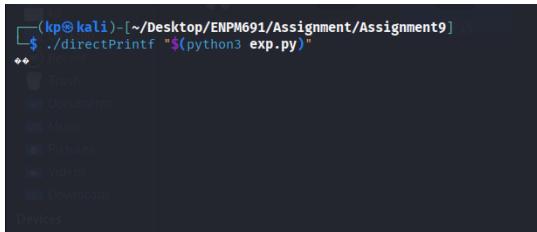


The screenshot shows the assembly code for the target function in GDB. The code includes instructions like movl \$0x40101010, %eax, movl %eax, %esi, and movl %esi, %edi. It also contains calls to \_\_libc\_start\_main and \_start. The assembly is color-coded with green for comments and blue for labels.

Fig. 13: In target function, privileges escalated and child process prepared [2].

## XII. EXPLOIT RESULTS

Finally, the payload executed the target function, printing the root-level message:



The terminal window shows the command ./directPrintt "\$(python3 exp.py)". The output is a single character, likely a carriage return or similar control character.

Fig. 14: Exploit output part 1 [2].



The terminal window shows the command ./directPrintt "\$(python3 exp.py)". The output is "Hello World from ROOT KP heheh !".

Fig. 15: Exploit output part 2 showing "Hello World from ROOT KP heheh !" [2].

## XIII. CONCLUSION

I successfully exploited a format string vulnerability to hijack program execution, redirecting it to a privileged function. Through this exercise, I reinforced my understanding of memory corruption vulnerabilities, GOT manipulation, format string payload construction, and controlled privilege escalation. This practical work demonstrated the importance of compiler protections, stack layout awareness, and precise memory inspection in real-world exploitation scenarios.

Additionally, I observed firsthand how compiler flags like -fno-stack-protector, -no-pie, and disabling ASLR contribute to exploit feasibility, and how these conditions can affect program security. This reinforces the critical

need for proper defensive programming and runtime protections in secure software development.

## XIV. WHAT I LEARNED

From this experiment, I learned:

- How format string vulnerabilities can be used to overwrite GOT entries and hijack program execution.
- The importance of stack analysis and offset determination for constructing reliable exploits.
- How system protections like SUID, ASLR, and RELRO interact with memory corruption vulnerabilities.
- Practical skills in using GDB and pwndbg to debug and validate exploit payloads.
- The real-world implications of these vulnerabilities and the importance of designing software with security in mind.

## XV. REFERENCES

- 1) ENPM691 Lecture 08 – Return Oriented Programming (ROP) Part 2.
- 2) pwndbg Documentation, <https://pwndbg.com/>.
- 3) Linux man pages for gcc, chmod, chown, printf, and sysctl.