Building a Web Server

Linux Processes

Connor Nelson Arizona State University

read

```
int read(
    int fd,
    void *buf,
    size_t count
)
```

read() attempts to read up to count bytes from file descriptor fd into the buffer starting at buf.

write

```
int write(
    int fd,
    void *buf,
    size_t count
)
```

write() writes up to count bytes from the buffer starting at buf to the file referred to by the file descriptor fd.

open

```
int open(
    char *pathname,
    int flags,
    mode_t mode
)
```

The open() system call opens the file specified by pathname. If the specified file does not exist, it may optionally (if O_CREAT is specified in flags) be created by open().

oper

```
int open(
    char *pathname,
    int flags,
    mode_t mode
)
```

The return value of open() is a file descriptor, a small, nonnegative integer that is used in subsequent system calls (read(2), write(2), lseek(2), fcntl(2), etc.) to refer to the open file. The file descriptor returned by a successful call will be the lowest-numbered file descriptor not currently open for the process.

PROCESS	
PID PPID	42 1
Real User ID Effective User ID Saved User ID	1000 1000 1000
FD 0 FD 1 FD 2 FD 3 FD 4 	/dev/pts/1 /dev/pts/1 /dev/pts/1
555555554000-55555555000 r- 555555555000-55555556000 r-	· ·
7ffff7da6000-7ffff7dc8000 r-7ffff7dc8000-7ffff7f40000 r-	
7ffffffde000-7ffffffff000 rw	-p [stack]

```
PROCESS
PID
                             42
PPID
Real
         User TD
                             1000
Effective User ID
                             1000
Saved
         User ID
                             1000
                             /dev/pts/1
FD 0
FD 1
                             /dev/pts/1
FD 2
                             /dev/pts/1
FD 3
FD 4
FD 1024
55555554000-555555555000 r--p /bin/program
55555555000-55555556000 r-xp /bin/program
7ffff7da6000-7ffff7dc8000 r--p /lib/.../libc.so.6
7ffff7dc8000-7ffff7f40000 r-xp /lib/.../libc.so.6
7ffffffde000-7ffffffff000 rw-p [stack]
```

MEMORY	
0000555555554000 0000555555554008	00 00 00 00 00 00 00 00
0000555555554010	00 00 00 00 00 00 00
000055555555000 0000555555555008	00 00 00 00 00 00 00 00
0000555555555010 00005555555555018	00 00 00 00 00 00 00 00
 00007fffffffe000	00 00 00 00 00 00 00 00
00007fffffffe008 00007fffffffe010	00 00 00 00 00 00 00 00
•••	

```
PROCESS
PID
                             42
PPID
Real
         User TD
                             1000
Effective User ID
                             1000
Saved
         User ID
                             1000
                             /dev/pts/1
FD 0
FD 1
                             /dev/pts/1
FD 2
                             /dev/pts/1
FD 3
FD 4
FD 1024
55555554000-555555555000 r--p /bin/program
55555555000-55555556000 r-xp /bin/program
7ffff7da6000-7ffff7dc8000 r--p /lib/.../libc.so.6
7ffff7dc8000-7ffff7f40000 r-xp /lib/.../libc.so.6
7ffffffde000-7ffffffff000 rw-p [stack]
```

MEMORY									
0000555555554000	00 6	00 00	00	00	00	00	00	ī	
0000555555554008	00 0	00 00	00	00	00	00	00	ĺ	
0000555555554010	00 0	00 00	00	00	00	00	00	İ	
								•	
0000555555555000	00 6	00 00	00	00	00	00	00	1	
0000555555555008	00 6	00 00	00	00	00	00	00	İ	
0000555555555010	00 6	00 00	00	00	00	00	00	İ	
0000555555555018	00 0	00 00	00	00	00	00	00	İ	
								•	
00007fffffffe000	00 0	00 00	00	00	00	00	00	Ι	
00007fffffffe008	00 0	00 00	00	00	00	00	00	İ	
00007fffffffe010	00 0	00 00	00	00	00	00	00	İ	
								•	
• • •									
ffff800000000000	00 6	00 00	00	00	00	00	00	1	• • • • • • •
• • •								•	
fffffffffffff8	00 6	00 00	00	00	00	00	00	1	

```
PROCESS
PID
                             42
PPID
Real
         User TD
                             1000
Effective User ID
                             1000
Saved
         User ID
                             1000
FD 0
                             /dev/pts/1
FD 1
                             /dev/pts/1
FD 2
                             /dev/pts/1
FD 3
FD 4
FD 1024
55555554000-555555555000 r--p /bin/program
55555555000-55555556000 r-xp /bin/program
7ffff7da6000-7ffff7dc8000 r--p /lib/.../libc.so.6
7ffff7dc8000-7ffff7f40000 r-xp /lib/.../libc.so.6
7ffffffde000-7ffffffff000 rw-p [stack]
```

MEMORY	
0000555555554000	00 00 00 00 00 00 00 00
0000555555554008	00 00 00 00 00 00 00 00
0000555555554010	00 00 00 00 00 00 00 00
•••	·
0000555555555000	00 00 00 00 00 00 00 00
000055555555008	00 00 00 00 00 00 00 00
0000555555555010	00 00 00 00 00 00 00 00
0000555555555018	00 00 00 00 00 00 00 00
00007fffffffe000	00 00 00 00 00 00 00 00
00007fffffffe008	00 00 00 00 00 00 00 00
00007fffffffe010	00 00 00 00 00 00 00 00
• • •	
• • •	
• • •	
ffff800000000000	00 00 00 00 00 00 00 00
• • •	
fffffffffffff8	00 00 00 00 00 00 00

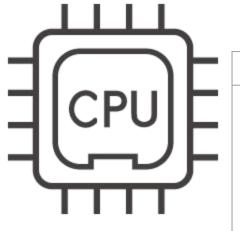
```
PROCESS
PID
                             42
PPI
         User ID
 eal
                             1000
Effective User ID
                             1000
Saved
         User ID
                             1000
FD 0
                             /dev/pts/1
FD 1
                             /dev/pts/1
FD 2
                             /dev/pts/1
FD 3
FD 4
FD 1024
55555554000-555555555000 r--p /bin/program
 5555555000-55555556000 r-xp /bin/program
rfl {7da6000-7ffff7dc8000 r--p /lib/.../libc.so.6
7ffff \c8000-7ffff7f40000 r-xp /lib/.../libc.so.
7ffffffde0 7ffffffff000 rw-p [stack]
```

open

```
int open(
    char *pathname,
    int flags,
    mode_t mode
)
```

The open() system call opens the file specified by pathname. If the specified file does not exist, it may optionally (if O_CREAT is specified in flags) be created by open().

```
mov rdi, 0x55555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

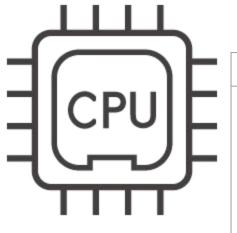


RAX	0x00000000000000000
RBX	0×0000000000000000
RCX	0×0000000000000000
RDX	0×0000000000000000
RDI	0×0000000000000000
RSI	0×0000000000000000
RSP	0x00007fffffffe010
RBP	0×0000000000000000
RIP	0x000055555555000

55555554008 00 00 00 00 00 00 00 00 00 55555554010 00 00 00 00 00 00 00 00 55555555000 48 bf 00 40 55 55 55 55 H@UUUU 5555555008 00 00 48 b8 2f 66 6c 61 H./fla 5555555010 67 00 00 00 48 89 07 48 gHH 5555555018 c7 c6 00 00 00 00 48 c7 H. 5555555020 c2 00 00 00 00 48 c7 c0 H. 5555555028 02 00 00 00 0f 05 00 00 5ffffffe000 00 00 00 00 00 00 00 00 fffffffe008 00 00 00 00 00 00 00 00										
5555554010 00 00 00 00 00 00 00 00 00 55555555000 48 bf 00 40 55 55 55 55 H@UUUU 55555555008 00 00 48 b8 2f 66 6c 61 H./fla 5555555010 67 00 00 00 48 89 07 48 gHH 5555555018 c7 c6 00 00 00 00 48 c7 H. 5555555020 c2 00 00 00 00 48 c7 c0 H. 55555555028 02 00 00 00 0f 05 00 00 6ffffffe000 00 00 00 00 00 00 00 00 fffffffe008 00 00 00 00 00 00 00 00	555555554000	00	00	00	00	00	00	00	00	
	55555554008	00	00	00	00	00	00	00	00	
5555555008 00 00 48 b8 2f 66 6c 61 H./fla 55555555010 67 00 00 00 48 89 07 48 gHH 55555555018 c7 c6 00 00 00 00 48 c7 H. 55555555020 c2 00 00 00 00 48 c7 c0 H. 55555555028 02 00 00 00 0f 05 00 00 6ffffffe000 00 00 00 00 00 00 00 00 6ffffffe008 00 00 00 00 00 00 00 00	55555554010	00	00	00	00	00	00	00	00	
5555555008 00 00 48 b8 2f 66 6c 61 H./fla 55555555010 67 00 00 00 48 89 07 48 gHH 55555555018 c7 c6 00 00 00 00 48 c7 H. 55555555020 c2 00 00 00 00 48 c7 c0 H. 55555555028 02 00 00 00 0f 05 00 00 6ffffffe000 00 00 00 00 00 00 00 00 6ffffffe008 00 00 00 00 00 00 00 00	• • •		•							
55555555010 67 00 00 00 48 89 07 48 gHH 55555555018 c7 c6 00 00 00 00 48 c7 H. 55555555020 c2 00 00 00 00 48 c7 c0 H. 55555555028 02 00 00 00 0f 05 00 00 fffffffe000 00 00 00 00 00 00 00 00 fffffffe008 00 00 00 00 00 00 00 00	55555555000	48	bf					55	55	
5555555018 c7 c6 00 00 00 00 48 c7 H. 55555555020 c2 00 00 00 00 48 c7 c0 H. 55555555028 02 00 00 00 0f 05 00 00 6fffffe000 00 00 00 00 00 00 00 00 6ffffffe008 00 00 00 00 00 00 00 00	55555555008	00	00	48	b8	2f	66	6c	61	H./fla
55555555020 c2 00 00 00 00 48 c7 c0 H 55555555028 02 00 00 00 0f 05 00 00 fffffffe000 00 00 00 00 00 00 00 00 fffffffe008 00 00 00 00 00 00 00 00	55555555010	67	00	00	00	48	89	07	48	gHH
5555555028	55555555018	c7	с6	00	00	00	00	48	с7	H.
	55555555020	c2	00	00	00	00	48	с7	c0	H
ffffffe000 00 00 00 00 00 00 00 00 ffffffe008 00 00 00 00 00 00 00 00	55555555028	02	00	00	00	0f	05	00	00	
ffffffe008 00 00 00 00 00 00 00	••		•							
	7fffffffe000	00	00	00	00	00	00	00	00	
ffffffe010 00 00 00 00 00 00 00 00	7fffffffe008	00	00	00	00	00	00	00	00	
	fffffffe010	00	00	00	00	00	00	00	00	

mov rdi, 0x55555554000

mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall



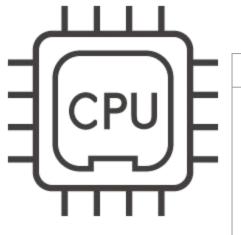
REGISTERS

RAX 0x00000000000000000 RBX 0x00000000000000000 **RCX** $0 \times 00000000000000000$ RDX 0x00000000000000000 RDI $0 \times 00000000000000000$ RSI 0x00000000000000000 **RSP** 0x00007fffffffe010 **RBP** 0x00000000000000000 RIP 0x000055555555000

MEMORY 555555554000 00 00 00 00 00 00 00 00 555555554008 00 00 00 00 00 00 00 00 555555554010 00 00 00 00 00 00 00 00 55555555000 48 bf 00 40 55 55 55 55 | H.. @UUUU 00 00 48 b8 2f 66 6c 61 l 55555555008 ..H./fla 55555555010 67 00 00 00 48 89 07 48 g...H..H 55555555018 c7 c6 00 00 00 00 48 c7H. c2 00 00 00 00 48 c7 c0H.. 55555555020 55555555028 02 00 00 00 0f 05 00 00 7fffffffe000 00 00 00 00 00 00 00 00 7fffffffe008 00 00 00 00 00 00 00 00 7fffffffe010 00 00 00 00 00 00 00 00

mov rdi, 0x55555554000

mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall

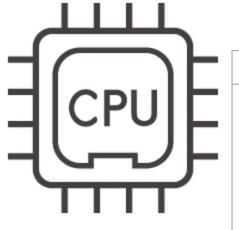


REGISTERS

RAX 0x00000000000000000 RBX 0x00000000000000000 **RCX** $0 \times 00000000000000000$ RDX 0x00000000000000000 RDI 0x0000555555554000 RSI 0x00000000000000000 **RSP** 0x00007fffffffe010 **RBP** 0x00000000000000000 RIP 0x000055555555500a

MEMORY 555555554000 00 00 00 00 00 00 00 00 555555554008 00 00 00 00 00 00 00 00 555555554010 00 00 00 00 00 00 00 00 55555555000 48 bf 00 40 55 55 55 55 | H.. @UUUU 00 00 48 b8 2f 66 6c 61 l 55555555008 ..H./fla 55555555010 67 00 00 00 48 89 07 48 g...H..H 55555555018 c7 c6 00 00 00 00 48 c7H. c2 00 00 00 00 48 c7 c0H.. 55555555020 55555555028 02 00 00 00 0f 05 00 00 7fffffffe000 00 00 00 00 00 00 00 00 7fffffffe008 00 00 00 00 00 00 00 00 7fffffffe010 00 00 00 00 00 00 00 00

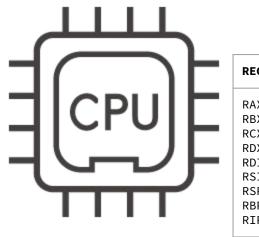
```
mov rdi, 0x55555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```



RAX	0×0000000000000000
RBX	0×0000000000000000
RCX	0×0000000000000000
RDX	0×0000000000000000
RDI	0x0000555555554000
RSI	0×0000000000000000
RSP	0x00007fffffffe010
RBP	0×0000000000000000
RIP	0x000055555555500a

```
MEMORY
555555554000
                00 00 00 00 00 00 00 00
555555554008
                00 00 00 00 00 00 00 00
555555554010
                00 00 00 00 00 00 00 00
55555555000
                48 bf 00 40 55 55 55 55 |
                                          H..@UUUU
                00 00 48 b8 2f 66 6c 61 | ..H./fla
55555555008
55555555010
                67 00 00 00 48 89 07 48 |
                                          g...H..H
55555555018
                c7 c6 00 00 00 00 48 c7 |
                                          ......H.
55555555020
                c2 00 00 00 00 48 c7 c0
                                          .....H..
55555555028
                02 00 00 00 0f 05 00 00
                                          . . . . . . . .
7fffffffe000
                00 00 00 00 00 00 00 00
7fffffffe008
                00 00 00 00 00 00 00 00
7fffffffe010
                00 00 00 00 00 00 00 00
```

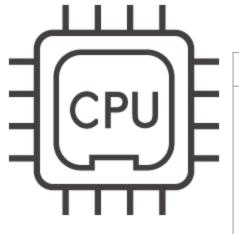
```
mov rdi, 0x55555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```



X	0x00000067616c662f
X	0×0000000000000000
X	0×00000000000000000
Χ	0×0000000000000000
I	0x0000555555554000
I	0×0000000000000000
Р	0x00007fffffffe010
P	0×0000000000000000
Р	0x0000555555555014

```
MEMORY
555555554000
               00 00 00 00 00 00 00 00
555555554008
               00 00 00 00 00 00 00 00
555555554010
               00 00 00 00 00 00 00 00
55555555000
               48 bf 00 40 55 55 55 55 |
                                         H..@UUUU
                                         ..H./fla
55555555008
               00 00 48 b8 2f 66 6c 61
55555555010
               67 00 00 00 48 89 07 48 |
                                         g...H..H
55555555018
               c7 c6 00 00 00 00 48 c7 |
                                         ......H.
55555555020
               c2 00 00 00 00 48 c7 c0
                                         ....H..
55555555028
               02 00 00 00 0f 05 00 00
7fffffffe000
               00 00 00 00 00 00 00 00
7fffffffe008
               00 00 00 00 00 00 00 00
7fffffffe010
               00 00 00 00 00 00 00
```

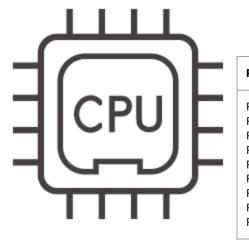
```
mov rdi, 0x55555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```



RAX	0x00000067616c662f
RBX	0×00000000000000000
RCX	0×00000000000000000
RDX	0×00000000000000000
RDI	0x0000555555554000
RSI	0×0000000000000000
RSP	0x00007fffffffe010
RBP	0×00000000000000000
RIP	0x0000555555555014

```
MEMORY
555555554000
               00 00 00 00 00 00 00 00
555555554008
               00 00 00 00 00 00 00 00
555555554010
               00 00 00 00 00 00 00 00
55555555000
               48 bf 00 40 55 55 55 55 |
                                         H..@UUUU
               00 00 48 b8 2f 66 6c 61 l
                                         ..H./fla
55555555008
55555555010
               67 00 00 00 48 89 07 48 |
                                         g...H..H
55555555018
               c7 c6 00 00 00 00 48 c7 |
                                         ......H.
55555555020
               c2 00 00 00 00 48 c7 c0
                                         ....H..
55555555028
               02 00 00 00 0f 05 00 00
7fffffffe000
               00 00 00 00 00 00 00 00
7fffffffe008
               00 00 00 00 00 00 00 00
7fffffffe010
               00 00 00 00 00 00 00 00
```

```
mov rdi, 0x55555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

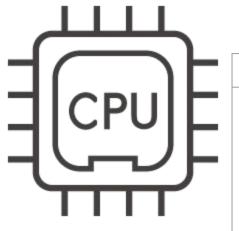


REGISTERS

RAX 0x00000067616c662f RBX 0x00000000000000000 **RCX** $0 \times 00000000000000000$ RDX 0x00000000000000000 RDI 0x0000555555554000 RSI 0x00000000000000000 **RSP** 0x00007fffffffe010 **RBP** 0x00000000000000000 RIP 0x0000555555555017

```
MEMORY
                2f 66 6c 61 67 00 00 00
                                           /flag...
555555554000
555555554008
                00 00 00 00 00 00 00 00
555555554010
                00 00 00 00 00 00 00 00
                                           . . . . . . . .
55555555000
                48 bf 00 40 55 55 55 55 |
                                           H..@UUUU
55555555008
                00 00 48 b8 2f 66 6c 61 l
                                           ..H./fla
55555555010
                67 00 00 00 48 89 07 48
                                           g...H..H
55555555018
                c7 c6 00 00 00 00 48 c7
                                           ......H.
55555555020
                c2 00 00 00 00 48 c7 c0
                                           ....H..
55555555028
                02 00 00 00 0f 05 00 00
                                           . . . . . . . .
7fffffffe000
                00 00 00 00 00 00 00 00
7fffffffe008
                00 00 00 00 00 00 00 00
7fffffffe010
                00 00 00 00 00 00 00 00
```

```
mov rdi, 0x55555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

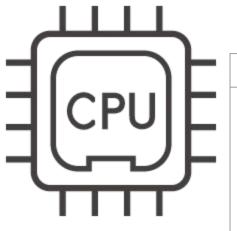


REGISTERS

RAX	0x00000067616c662f
RBX	0×00000000000000000
RCX	0×00000000000000000
RDX	0×00000000000000000
RDI	0x0000555555554000
RSI	0×00000000000000000
RSP	0x00007fffffffe010
RBP	0×00000000000000000
RIP	0x0000555555555017

MEMORY 555555554000 2f 66 6c 61 67 00 00 00 /flag... 555555554008 00 00 00 00 00 00 00 00 555555554010 00 00 00 00 00 00 00 00 55555555000 48 bf 00 40 55 55 55 55 | H..@UUUU 00 00 48 b8 2f 66 6c 61 | ..H./fla 55555555008 55555555010 67 00 00 00 48 89 07 48 g...H..H 55555555018 c7 c6 00 00 00 00 48 c7 | H . 55555555020 c2 00 00 00 00 48 c7 c0H.. 55555555028 02 00 00 00 0f 05 00 00 7fffffffe000 00 00 00 00 00 00 00 00 7fffffffe008 00 00 00 00 00 00 00 00 7fffffffe010 00 00 00 00 00 00 00 00

```
mov rdi, 0x55555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

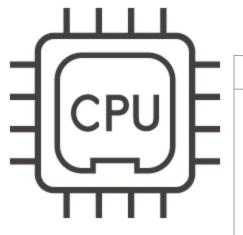


REGISTERS

RAX 0x00000067616c662f RBX 0x00000000000000000 **RCX** $0 \times 00000000000000000$ RDX 0x00000000000000000 RDI 0x0000555555554000 RSI 0x0000000000000000 **RSP** $0 \times 00007 fffffffe010$ **RBP** 0x00000000000000000 RIP 0x000055555555501e

MEMORY 2f 66 6c 61 67 00 00 00 /flag... 555555554000 555555554008 00 00 00 00 00 00 00 00 555555554010 00 00 00 00 00 00 00 00 55555555000 48 bf 00 40 55 55 55 55 | H..@UUUU 00 00 48 b8 2f 66 6c 61 l 55555555008 ..H./fla 55555555010 67 00 00 00 48 89 07 48 g...H..H 55555555018 **c7 c6 00 00 00 00** 48 c7 ••••H. 55555555020 c2 00 00 00 00 48 c7 c0H.. 55555555028 02 00 00 00 0f 05 00 00 7fffffffe000 00 00 00 00 00 00 00 00 7fffffffe008 00 00 00 00 00 00 00 00 7fffffffe010 00 00 00 00 00 00 00 00

```
mov rdi, 0x55555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

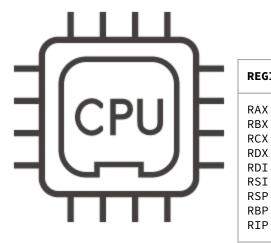


REGISTERS

RAX 0x00000067616c662f RBX 0x00000000000000000 **RCX** $0 \times 00000000000000000$ RDX 0x00000000000000000 RDI 0x0000555555554000 RSI 0x00000000000000000 **RSP** 0x00007fffffffe010 **RBP** 0x00000000000000000 RIP 0x000055555555501e

```
MEMORY
                2f 66 6c 61 67 00 00 00
                                            /flag...
555555554000
555555554008
                00 00 00 00 00 00 00 00
555555554010
                00 00 00 00 00 00 00 00
                                            . . . . . . . .
55555555000
                48 bf 00 40 55 55 55 55 |
                                            H..@UUUU
                00 00 48 b8 2f 66 6c 61 l
55555555008
                                            ..H./fla
55555555010
                67 00 00 00 48 89 07 48
                                           g...H..H
55555555018
                c7 c6 00 00 00 00 48 c7
                                            . . . . . . H.
55555555020
                c2 00 00 00 00 48 c7 c0
                                            .....H..
55555555028
                02 00 00 00 0f 05 00 00
                                            . . . . . . . .
7fffffffe000
                00 00 00 00 00 00 00 00
7fffffffe008
                00 00 00 00 00 00 00 00
7fffffffe010
                00 00 00 00 00 00 00 00
```

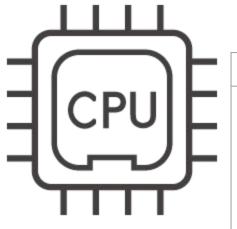
```
mov rdi, 0x55555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```



REGISTERS

MEMORY 2f 66 6c 61 67 00 00 00 555555554000 /flag... 555555554008 00 00 00 00 00 00 00 00 555555554010 00 00 00 00 00 00 00 00 55555555000 48 bf 00 40 55 55 55 55 | H..@UUUU 00 00 48 b8 2f 66 6c 61 | 55555555008 ..H./fla 55555555010 67 00 00 00 48 89 07 48 g...H..H 55555555018 c7 c6 00 00 00 00 **48 c7** H. 55555555020 **c2 00 00 00 00** 48 c7 c0H.. 55555555028 02 00 00 00 0f 05 00 00 7fffffffe000 00 00 00 00 00 00 00 00 7fffffffe008 00 00 00 00 00 00 00 00 7fffffffe010 00 00 00 00 00 00 00 00

```
mov rdi, 0x55555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```

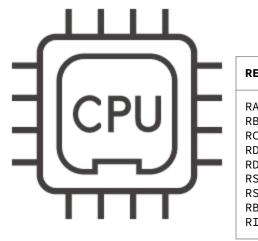


REGISTERS

RAX	0x00000067616c662f
RBX	0×0000000000000000
RCX	0×00000000000000000
RDX	0×00000000000000000
RDI	0x0000555555554000
RSI	0×00000000000000000
RSP	0x00007fffffffe010
RBP	0×00000000000000000
RIP	0x0000555555555025

MEMORY 555555554000 2f 66 6c 61 67 00 00 00 /flag... 555555554008 00 00 00 00 00 00 00 00 555555554010 00 00 00 00 00 00 00 00 55555555000 48 bf 00 40 55 55 55 55 | H..@UUUU 00 00 48 b8 2f 66 6c 61 l ..H./fla 55555555008 55555555010 67 00 00 00 48 89 07 48 1 g...H..H 55555555018 c7 c6 00 00 00 00 48 c7H. 55555555020 c2 00 00 00 00 **48 c7 c0** H . . **02 00 00 00** 0f 05 00 00 55555555028 7fffffffe000 00 00 00 00 00 00 00 00 7fffffffe008 00 00 00 00 00 00 00 00 7fffffffe010 00 00 00 00 00 00 00 00

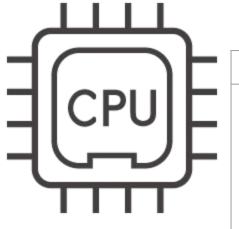
```
mov rdi, 0x55555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```



٩X	0x00000000000000002
ВХ	0×0000000000000000
CX	0×0000000000000000
DX	0×0000000000000000
DI	0x0000555555554000
SI	0×0000000000000000
SP	0x00007fffffffe010
BP	0×0000000000000000
ΙP	0x000055555555502c

```
MEMORY
555555554000
                2f 66 6c 61 67 00 00 00
                                          /flag...
555555554008
                00 00 00 00 00 00 00 00
555555554010
                00 00 00 00 00 00 00 00
55555555000
                48 bf 00 40 55 55 55 55 |
                                          H..@UUUU
                00 00 48 b8 2f 66 6c 61 |
                                          ..H./fla
55555555008
55555555010
                67 00 00 00 48 89 07 48 I
                                          g...H..H
55555555018
                c7 c6 00 00 00 00 48 c7
                                          ......H.
55555555020
                c2 00 00 00 00 48 c7 c0
                                          . . . . . H . .
                02 00 00 00 0f 05 00 00
55555555028
7fffffffe000
                00 00 00 00 00 00 00 00
7fffffffe008
                00 00 00 00 00 00 00 00
7fffffffe010
                00 00 00 00 00 00 00 00
```

```
mov rdi, 0x55555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```



RAX	0x00000000000000002
RBX	0×0000000000000000
RCX	0×0000000000000000
RDX	0×0000000000000000
RDI	0x0000555555554000
RSI	0×0000000000000000
RSP	0x00007fffffffe010
RBP	0×0000000000000000
RIP	0x000055555555502c

```
MEMORY
555555554000
               2f 66 6c 61 67 00 00 00
                                          /flag...
555555554008
               00 00 00 00 00 00 00 00
555555554010
               00 00 00 00 00 00 00 00
55555555000
               48 bf 00 40 55 55 55 55 |
                                         H..@UUUU
               00 00 48 b8 2f 66 6c 61 l
                                         ..H./fla
55555555008
55555555010
               67 00 00 00 48 89 07 48 1
                                         g...H..H
55555555018
               c7 c6 00 00 00 00 48 c7 |
                                          ......H.
55555555020
               c2 00 00 00 00 48 c7 c0
                                          ....H..
55555555028
               02 00 00 00 0f 05 00 00
7fffffffe000
               00 00 00 00 00 00 00 00
7fffffffe008
               00 00 00 00 00 00 00 00
7fffffffe010
               00 00 00 00 00 00 00 00
```

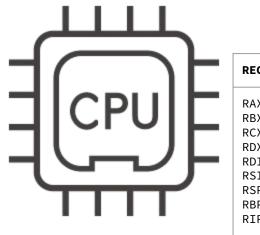
```
MEMORY
                  2f 66 6c 61 67 00 00 00 | /flag...
0000555555554000
0000555555554008
                  00 00 00 00 00 00 00 00 | ......
0000555555554010
                  00 00 00 00 00 00 00 00 | ......
                  48 bf 00 40 55 55 55 55 | H..@UUUU
0000555555555000
                  00 00 48 b8 2f 66 6c 61 | ..H./fla
0000555555555008
                  67 00 00 00 48 89 07 48 | g...H..H
0000555555555010
                  c7 c6 00 00 00 00 48 c7 | .....H.
0000555555555018
                  c2 00 00 00 00 48 c7 c0 | .....H...
0000555555555020
0000555555555028
                  02 00 00 00 0f 05 00 00 | ......
00007fffffffe000
                  00 00 00 00 00 00 00 00 | ......
                  00 00 00 00 00 00 00 00 | ......
00007fffffffe008
00007fffffffe010
                  00 00 00 00 00 00 00 00 1 ......
. . .
. . .
ffff800000000000
                   00 00 00 00 00 00 00 00 | ......
. . .
ffff????????????
                   ?? ?? ?? ?? ?? ?? ?? ! ......
. . .
fffffffffffff8
                  00 00 00 00 00 00 00 00 1 ......
```

PROCESS					
PID PPID	42 1				
Real User ID Effective User ID Saved User ID	1000 1000 1000				
FD 0 FD 1 FD 2 FD 3 FD 4 FD 1024	/dev/pts/1 /dev/pts/1 /dev/pts/1				
555555554000-55555555000 rp /bin/program 5555555555000-55555556000 r-xp /bin/program 7ffff7da6000-7ffff7dc8000 rp /lib//libc.so.6 7ffff7dc8000-7ffff7f40000 r-xp /lib//libc.so.6					
7ffffffde000-7ffffffff000 rw	-p [stack]				

```
MEMORY
                   2f 66 6c 61 67 00 00 00 | /flag...
0000555555554000
0000555555554008
                   00 00 00 00 00 00 00 00 | ......
0000555555554010
                   00 00 00 00 00 00 00 00 | ......
                   48 bf 00 40 55 55 55 55 | H..@UUUU
0000555555555000
0000555555555008
                   00 00 48 b8 2f 66 6c 61 | ..H./fla
                   67 00 00 00 48 89 07 48 | g...H..H
0000555555555010
                   c7 c6 00 00 00 00 48 c7 | .....H.
0000555555555018
                   c2 00 00 00 00 48 c7 c0 | .....H...
0000555555555020
0000555555555028
                   02 00 00 00 0f 05 00 00 | ......
00007fffffffe000
                   00 00 00 00 00 00 00 00 1 ......
00007fffffffe008
                   00 00 00 00 00 00 00 00 | ......
00007fffffffe010
                   00 00 00 00 00 00 00 00 | ......
. . .
. . .
ffff800000000000
                   00 00 00 00 00 00 00 0 | ......
. . .
ffff????????????
                   ?? ?? ?? ?? ?? ?? ?? ! ......
. . .
ffffffffffff8
                   00 00 00 00 00 00 00 00 | ......
```

```
PROCESS
PID
                             42
PPTD
                             1
Real
         User TD
                             1000
Fffective User ID
                             1000
Saved
         User TD
                             1000
FD 0
                             /dev/pts/1
FD 1
                             /dev/pts/1
FD 2
                             /dev/pts/1
FD 3
                             /flag
FD 4
FD 1024
55555554000-555555555000 r--p /bin/program
55555555000-55555556000 r-xp /bin/program
7ffff7da6000-7ffff7dc8000 r--p /lib/.../libc.so.6
7ffff7dc8000-7ffff7f40000 r-xp /lib/.../libc.so.6
7ffffffde000-7ffffffff000 rw-p [stack]
```

```
mov rdi, 0x55555554000
mov rax, 0x0067616c662f
mov qword ptr [rdi], rax
mov rsi, 0
mov rdx, 0
mov rax, 2
syscall
```



Χ	0x0000000000000003
Χ	0x0000000000000000
Χ	0x0000000000000000
Χ	0x0000000000000000
I	0x0000555555554000
I	0x0000000000000000
Р	0x00007fffffffe010
Р	0x0000000000000000
P	0x000055555555502e

```
MEMORY
555555554000
               2f 66 6c 61 67 00 00 00
                                          /flag...
555555554008
                00 00 00 00 00 00 00 00
555555554010
                00 00 00 00 00 00 00 00
55555555000
                48 bf 00 40 55 55 55 55 |
                                         H..@UUUU
                00 00 48 b8 2f 66 6c 61 |
                                         ..H./fla
55555555008
55555555010
                67 00 00 00 48 89 07 48 I
                                         g...H..H
55555555018
                c7 c6 00 00 00 00 48 c7
                                          ......H.
55555555020
                c2 00 00 00 00 48 c7 c0
                                          ....H..
55555555028
                02 00 00 00 0f 05 00 00
7fffffffe000
                00 00 00 00 00 00 00 00
7fffffffe008
                00 00 00 00 00 00 00 00
7fffffffe010
                00 00 00 00 00 00 00 00
```

* System Calls

SYSCALL	RAX	ARG0	ARG1	ARG2	ARG3	ARG4	ARG5
NAME		(rdi)	(rsi)	(rdx)	(r10)	(r8)	(r9)
read	0	int fd	char *buf	size_t count	-	-	-
write	1	int fd	char *buf	size_t count	-	-	-
open	2	char *filename	int flags	umode_t mode	-	-	-
close	3	int fd	-	-	-	-	-
mmap	9	long addr	size_t len	long prot	int flags	int fd	off_t offset
mprotect	А	long addr	size_t len	long prot	-	-	-
munmap	В	long addr	size_t len	-	-	-	-
getpid	27	-	-	-	-	-	-
fork	39	-	-	-	-	-	-
execve	3B	char *filename	char **argv	char **envp	-	-	-
exit	3C	int error_code	-	-	-	-	-
getcwd	4F	char *buf	size_t size	-	-	-	-
chdir	50	char *filename	-	-	-	-	-
chmod	5A	char *filename	umode_t mode	-	-	-	-
gettimeofday	60	struct timeval *tv s	truct timezone *tz	-	-	-	-
getuid	66	-	-	-	-	-	-
geteuid	6B	-	-	-	-	-	-
getppid	6E	-	-	-	-	-	_

For more system calls, see https://x64.syscall.sh/