

```
/* victim.c */
```

```
int main()
```

```
{
```

```
    char name[64];
```

```
    puts("What's your name?");
```

```
    gets(name);
```

```
    printf("Hello, %s!\n", name);
```

```
    return 0;
```

```
}
```

Return address (8-byte)

EBP Register (8-byte)

char name[64] (64-byte)

stack of ./victim

overwrite

overwrite

overwrite

string "/bin/sh"

addr of system() in libc.so

addr of "/bin/sh"

addr of **pop rdi; ret**

0x0

0x0



input of
gets(name);