

# 实验二：代码纠错

将代码复制到app-helloworld/workdir/unikraft/lib/ukallocbbuddy/bbuddy.c的对应位置中

## 实验过程

```
cd ~/os-2026/app-helloworld  
make clean  
make -j8
```

- 启动 QEMU 并开启 gdb 远程调试端口：

```
qemu-system-aarch64 -kernel workdir/build/helloworld_qemu-arm64 -nographic -  
machine virt -cpu cortex-a57 -s -S
```

- 另开一个终端，使用 gdb-multiarch 连接 QEMU：

```
gdb-multiarch workdir/build/helloworld_qemu-arm64.dbg --eval-command="target  
remote :1234"
```

- 在bbuddy\_pfree函数上打断点：

```
(gdb) b bbuddy_pfree  
Breakpoint 1 at 0x4011c978: file /home/qomolangma/os-2026/app-  
helloworld/workdir/unikraft/lib/ukallocbbuddy/bbuddy.c, line 502.  
(gdb) c
```

```
0x0000000040000000 in ?? ()  
(gdb) b bbuddy_pfree  
Breakpoint 1 at 0x4011c8e0: file /home/qomolangma/os-2026/app-helloworld/workdir/unikraft/lib/ukallocbbuddy/bbuddy.c, line 502.  
(gdb)
```

- 当断下后，记录局部变量进入循环前的初值：

```
(gdb) info locals  
(gdb) p/x obj  
(gdb) p/x freed_ct  
(gdb) p num_pages
```

发现错误：

```
574  
575     nr_page_left--;  
576     obj = (char *) freed_ct + 1;|  
577 }  
578 #endif
```

导致页面计算错误，

更新为：

```
obj = (char *)obj + (1UL << __PAGE_SHIFT);
```

```
576     obj = (char *)obj + (1UL << __PAGE_SHIFT);  
577 }  
578 #endif
```

实验记录：

```
(gdb) p freed_ct  
$4 = (chunk_tail_t *) 0x44104ffc  
(gdb) p obj  
$5 = (void *) 0x44104ffd
```

错误：

```
556     freed_ct->level = order,  
557  
558     freed_ch->next->pprev = &freed_ch->next;  
559     b->free_head[order] = freed_ch;  
560 #else
```

b->free\_head[0]可能是NULL，造成空指针解引用。需要添加：

```
if (b->free_head[0])  
    b->free_head[0]->pnext = &freed_ch->next;
```