Exploiting

one after $\vee$ is `call` return address

care about return a[ddress]


```
                         one after is return address
       ┌──────────────┐
       │    return    │  ← rsp when we start
 0x38  │   address    │
       ├──────────────┤   ┐
       │              │   │  how much
       │              │   │   space we
       │  password    │   │   need to fill
       │              │   │   to get to
       │              │   │   start of
       ├──────────────┤  32   return address
       │     fd       │   4
       ├──────────────┤   4    ↑
       │ Pass length  │   │   0xC  Buffer
       ├──────────────┤   8    │
       │              │   ↓  ← rsp
       └──────────────┘
```