Off_by_one writeup

Recon

file ./off-by-one
checksec ./off-by-one
r2 -e bin.relocs.apply=true -A ./off-by-one
objdump -d ./off-by-one -M intel --start-address=0x401000 --stop-address=0x401200

Extract bytes

xxd -s 0x1069 -l 8 -g 1 ./off-by-one

Compute passphrase

python3 - <<'PY'
with open('./off-by-one','rb') as f:
f.seek(0x401069 - 0x400000)
data = f.read(8)
print('passphrase:', ''.join(chr((b % 64) + 48) for b in data))
PY

Verify

printf "DXUPWYfU
" | ./off-by-one