CTF - RE secret.exe

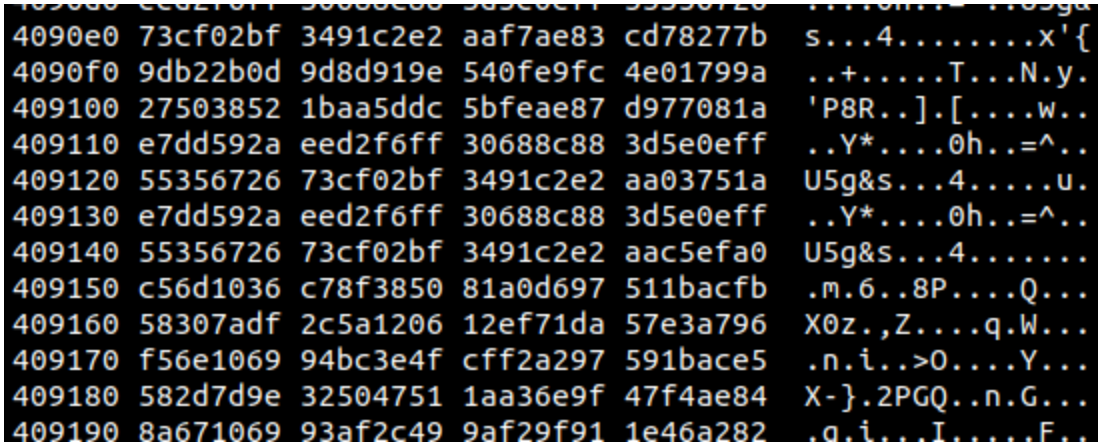
Chunk secret.exe binary into Ghidra and find main:

```
___main();
if (DAT_00409020 != '\0') {
  __Z12DecodeParamsv();
}
local_11 = '\x01';
local_28.lpSecurityDescriptor = (LPVOID)0x0;
local_28.bInheritHandle = 0;
local_28.nLength = 0xc;
BVar2 = _CreateDirectoryA@8(&DAT_00409021,(LPSECURITY_ATTRIBUTES)&local_28);
if ((BVar2 == 0) && (DVar3 = _GetLastError@0(), DVar3 == 0xb7)) {
  local_11 = '\0';
}
local_1c = (HANDLE)0xffffffff;
local_1c = _CreateFileA@28(&DAT_00409085,0xc0000000,1,(LPSECURITY_ATTRIBUTES)0x0,2,0x80,
                           (HANDLE)0x0);
if (local_1c == (HANDLE)0xffffffff) {
  DVar3 = _GetLastError@0();
}
else {
  local_2c = 0;
  BVar2 = _WriteFile@20(local_1c,&DAT_004090e9,100,&local_2c,(LPOVERLAPPED)0x0);
  if ((BVar2 == 0) || (local_2c != 100)) {
    bVar1 = true;
  }
  else {
    bVar1 = false;
  }
```

Notices WriteFile trying to write 100 bytes data at 0x004090e9.

```
  else {
    local_2c = 0;
    BVar2 = _WriteFile@20(local_1c,&DAT_004090e9,100,&local_2c,(LPOVERLAPPED)0x0);
    if ((BVar2 == 0) || (local_2c != 100)) {
      bVar1 = true;
    }
    else {
      bVar1 = false;
    }
    if (bVar1) {
```

Checkout 0x004090e9, I am guessing this is the flag



We found the encrypted flag, now here is how to decrypt

```
void __Z12DecodeParamsv(void)

{
  uint local_8;

  for (local_8 = 0; local_8 < 100; local_8 = local_8 + 1) {
    (&DAT_00409021)[local_8] = (&DAT_00409021)[local_8] ^ (&DAT_00409000)[local_8 & 0x1f];
    (&DAT_00409085)[local_8] = (&DAT_00409085)[local_8] ^ (&DAT_00409000)[local_8 & 0x1f];
    (&DAT_004090e9)[local_8] = (&DAT_004090e9)[local_8] ^ (&DAT_00409000)[local_8 & 0x1f];
    (&DAT_0040914d)[local_8] = (&DAT_0040914d)[local_8] ^ (&DAT_00409000)[local_8 & 0x1f];
    (&DAT_004091b1)[local_8] = (&DAT_004091b1)[local_8] ^ (&DAT_00409000)[local_8 & 0x1f];
  }
  DAT_00409020 = 0;
  return;
}
```

Now, a simple python script can simply decrypt this.