We have a x64 ELF relocatable file, cannot execute it huh? (maybe just because IDK)

So static analysis is required!

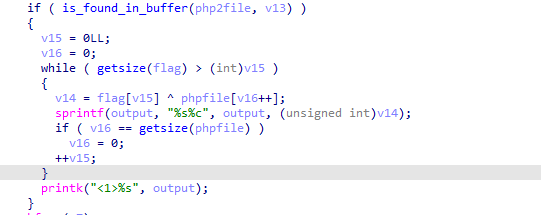
Load it into IDA, F5 to get pseudocode



At first, you can see it call some strange functions (at least, for me it’s strange, i seldom see them) like kmem\_cache\_alloc\_trace or orifinal\_read\_call, d\_path

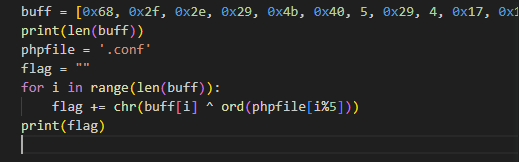
But the most important thing we should notice here is flag variable, which is was written by qmemcpy(), has length equal to 29

Bunch of code after that, i think we shouldn’t pay attentions for them because it doesn’t affect or use flag variable, So find code where them affect or use flag var, easy huh?



There we go, simple xor algorithm

i use python script to find the output which is FLAG



buff variable here is 29 byte at first it copy into flag

