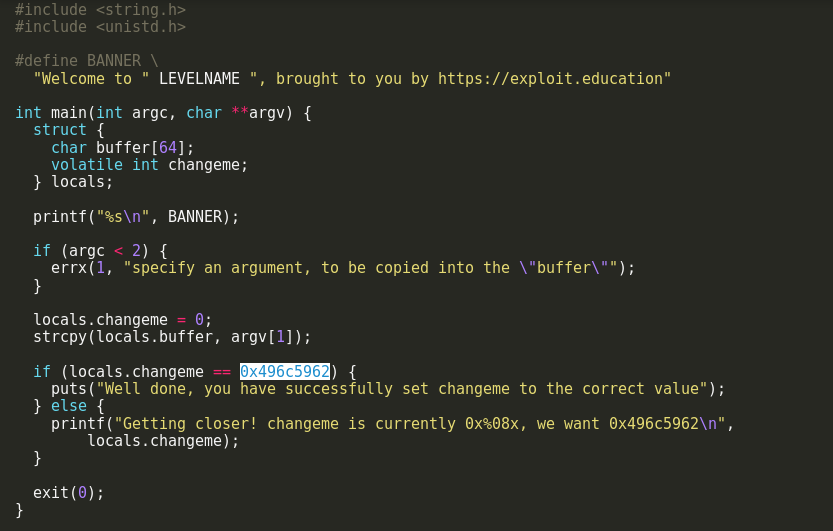
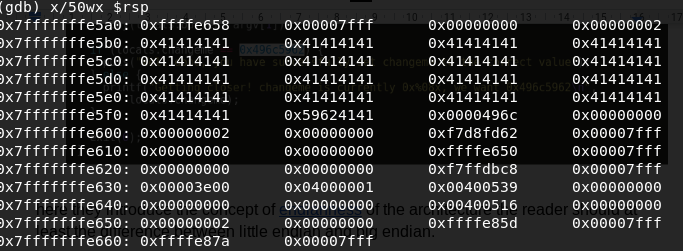
Pheonix stack-one write-up

**Intro**

This level is the same as the previous level but here we will overflow locals.changeme with this address 0x496c5962 so we will approach this problem the same as [stack-zero](https://github.com/3esawe/Phoenix/blob/master/pheonix_stack-zero.docx) here’s a picture of the source code 

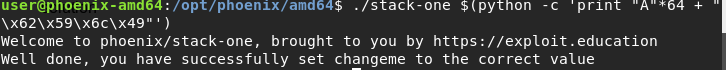
here they introduce the concept of [endianness](https://en.wikipedia.org/wiki/Endianness) of the architecture the reader should at least the difference between little endian and big endian.

**Solution**



I approached this the same as before so first i calculated the address of the start of the buffer starts at 

and the address of locals.changeme starts at $rbp-0x10 which is 0x7fffffffe600 we already discussed how to get these address in the previous write-up, here’s the final solution



I hope you enjoyed my write-up any comment or suggest is appreciated you can contact me via my e-mail address: omaroobaniessa@gmail.com