RELRO (RELocation Read-Only)

To prevent the above exploitation technique, we can tell the linker to resolve all dynamically linked functions at the beginning of execution and make the GOT read-only. Note that we are operating on a different binary below compiled from the same source code.

> ```
> now When generating an executable or shared library, mark it to
> tell the dynamic linker to resolve all symbols when the program
> is started, or when the shared library is linked to using
> dlopen, instead of deferring function call resolution to the
> point when the function is first called.
> ```

This exploitation mitigation technique is known as RELRO which stands for RELocation Read-Only. The idea is simple, make the relocation sections that are used to resolve dynamically loaded functions read-only. This way, they cannot overwrite them and we cannot take control of execution like we did above.

Canary

插入一个值在 stack overflow 发生的高危区域的尾部。当函数返回之时检测 Canary 的值是否经过了改变，以此来判断 stack/buffer overflow 是否发生。

NX (non-execute)

NX(Non-execute) 位是一种针对 shellcode 执行攻击的保护措施，意在更有效地识别数据区和代码区。通过在内存页的标识中增加" 执行" 位，可以表示该内存页是否执行，若程序代码的 EIP 执行至不可运行的内存页，则 CPU 将直接拒绝执行" 指令" 造成程序崩溃。

PIE (Position-Independent Executable)

技术与 ASLR 技术类似，ASLR 将程序运行时的堆栈以及共享库的加载地址随机化，而 PIE 技术则在编译时将程序编译为位置无关 , 即程序运行时各个段加载的虚拟地址也是在装载时才确定。