PIE Memory Protection

PIE (Position-Independant Executable), also known as PIC (Position-Independant Code), is a type of memory protection

PIE Memory Protection

```
└─$ ./vuln
Address of main: 0×5582242833d
```

```
└─$ ./vuln
Address of main: 0×5556905b733d
```

PIE ensures that program code can be executable no matter where it is located in program memory, and will load instructions in different memory addresses each time the binary is run

PIE Memory Protection

```
0×557b3fb3d2a7    6     150 sym.win
0×557b3fb3d33d    3     204 main
```

However, program function will still retain their relative offsets, which means that if we can determine the memory address of one function during execution, we can locate others

PIE Memory Protection

```
0×557b3fb3d2a7    6     150 sym.win
0×557b3fb3d33d    3     204 main
```

Since the difference between the main function's address and the sym.win function's address is 0x96--

PIE Memory Protection

```
└─$ python3 -c "print(hex(0×5574350ce33d - 0×96))"
0×5574350ce2a7
```

If we have the main function's address, we can subtract 0x96 from it to determine the address of the sym.win function