Off by one:

off by one occurs because strlen ignores 0x00 when calculating the length of a string. For example, payload= "A" *1024+0x00 and strlen(payload)=1024, storing the payload in array[1024] using strcpy will result in a single-byte overwrite of the adjacency variable at the final terminal 0x00. There are three cases:

1. rip cannot be overridden, but rbp can be manipulated to modify control flow. For little endianned computers, when stack frame optimization is not enabled and the old rbp stored in the adjacent stack of the variable is overflowed, the low bit modification of the old rbp can be 0x00, after which the first function returns, pop rbp raises the rbp, when the second function returns, mov rsp, rbp raises the rsp. Therefore, the rbp and the return address saved during pop operation can be modified, and the modified value is in the stack space controlled by the attacker, which can achieve control flow hijacking.
2. When the compiler turns on stack frame optimization and overflows the rip stored in the adjacent stack of a variable, the lower rip value can be overwritten to 0x00, which will change the control flow.
3. When overflow variables are not adjacent to rbp and rip, consider overwriting their adjacency variables. If the adjacency variables are Pointers, control flow changes may be implemented in the future.