HW2

Q1

1.

Stack Object	Address of stack object
return address	`&buf[0]` +12
old `%rbp`	`&buf[0]` +4
`&buf[3]`	`&buf[0]` +3
`&buf[2]`	`&buf[0]` +2
`&buf[1]`	`&buf[0]` +1
`&buf[0]`	`&buf[0]` +0

2. `0 0 0 0 0 0 0 0 0 0 0 0 39`

Q2

空格	值
(1)	`7`
(2)	`leaq`
(3)	`16`
(4)	`840`

Q3

1. 因为 `x` 是带符号整数, 如果 `x` 是负数也需要进入 `default` 的情况.
2.

空格	値
(1)	`.L4`
(2)	`%r8`
(3)	`%r8`
(4)	`%rdi`
(5)	`addq`
(6)	`$1`

Q4

空格	値
(1)	`%rdi`
(2)	callee saved
(3)	`8`
(4)	`16`
(5)	`7`
(6)	`8`
(7)	`15`
(8)	`16`

Q5

1.

```
int Q() {
    char buf[64];
    fgets(buf, 64, stdin); // 漏洞!
    ...
    return ...;
}
```

2. i. 这样的话, 栈上的恶意代码将不可能被执行, 就算注入代码了也将无效.
   ii. 将一个特殊值放在缓冲区之上的栈内, 并在退出函数之前检查该值是否被破坏.
3. 可以绕过 NX , 但必不可以绕过金丝雀.