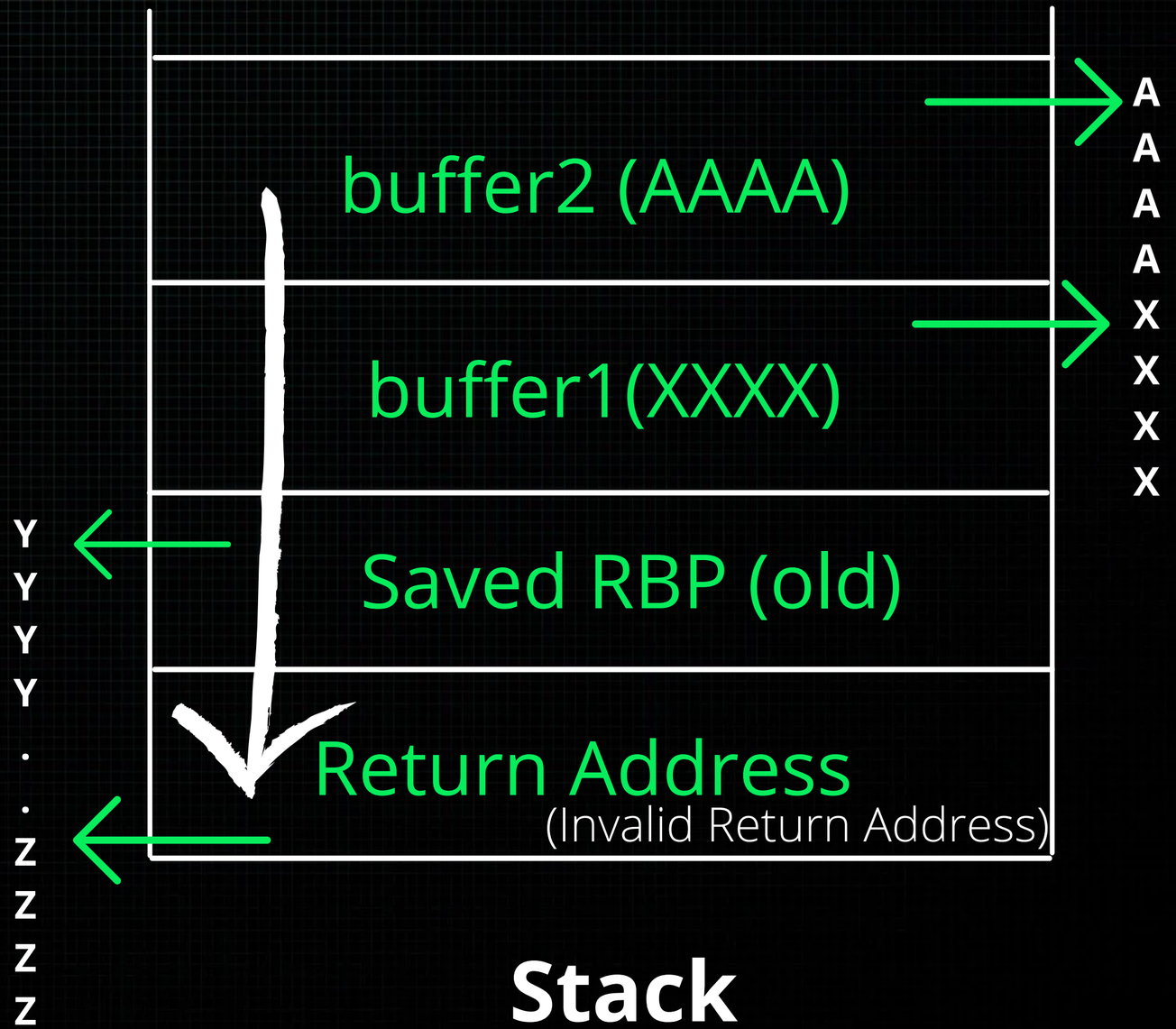

Manipulation of Instruction Pointer

Overwriting Return Address

Input : AAAAXXXXYYYYYYYYZZZZZZZZ

Output: ?????????

IO



Stack

Stack Smashing

+ Canary

- Canary
+ Stack Overflow

Endianess

Little Endian

0x1337c0de

\xde \xc0 \x37 \x13

Big Endian

0x1337c0de

\x13 \x37 \xc0 \xde

Buffer Overflow Functions

fgets(stdin,buffer,500)

sizeof(buffer) << 500

strcpy(buffer,inp_buffer)

gets(buffer)

scanf("%s",buffer)

Basically any function that triggers input of more data than a buffer can hold !

Shellcodes

BEBFBGBHCACBCDGT
AGTRBEBFBGBHNQRC
BEBFBGBNHJQYXZ12
$H3LL C0de ACC3p7

```
anonymous@vulnerable: ~
$ cat flag.txt
  GLUG{$H311_C0D3_1S_C00L}

anonymous@vulnerable: ~
$ exit
```

Shellcode Deployment

Instruction Pointer
(RIP or EIP)

Find Shellcodes in shell-storm website !


Thank you for watching