CSE 351

Buffer Overflows and Lab3

Bufbomb Introduction

- Several stages
- Practice analyzing stack organization
- Practice with buffer overflows

Bufbomb Introduction

- GDB commands
  - `set args -u <username>`
    - Set the argument to the program
  - `x/40wx ($rsp - 40)`
    - Show the 40 bytes above rsp
    - Change `w` to `g` to check the value in 8 byte chunks.
  - `b *(&getbuf + 12)`
    - Create a breakpoint at 12 bytes away after the start of getbuf

Lab 3: Buffer Overflow

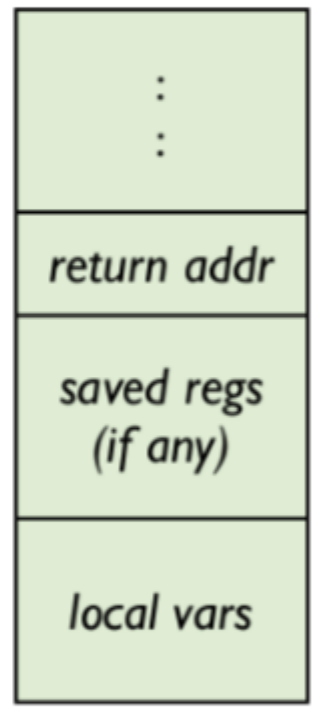
This has a buffer overflow

```
int getbuf() {
  char buf[36];
  Gets(buf);
  return 1;
}
```

Why?

- `Gets()` doesn't check the length of the buffer

The Stack in getbuf()

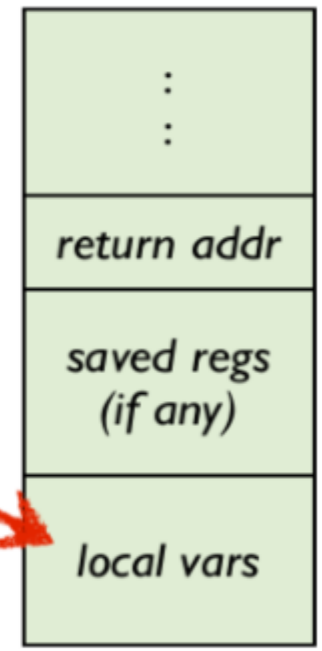


Lab 3: Buffer Overflow

This has a buffer overflow

```
int getbuf() {
  char buf[36];
  Gets(buf);
  return 1;
}
```

The Stack in getbuf()



Why?

- `Gets()` doesn't check the length of the buffer

Lab 3: Buffer Overflow

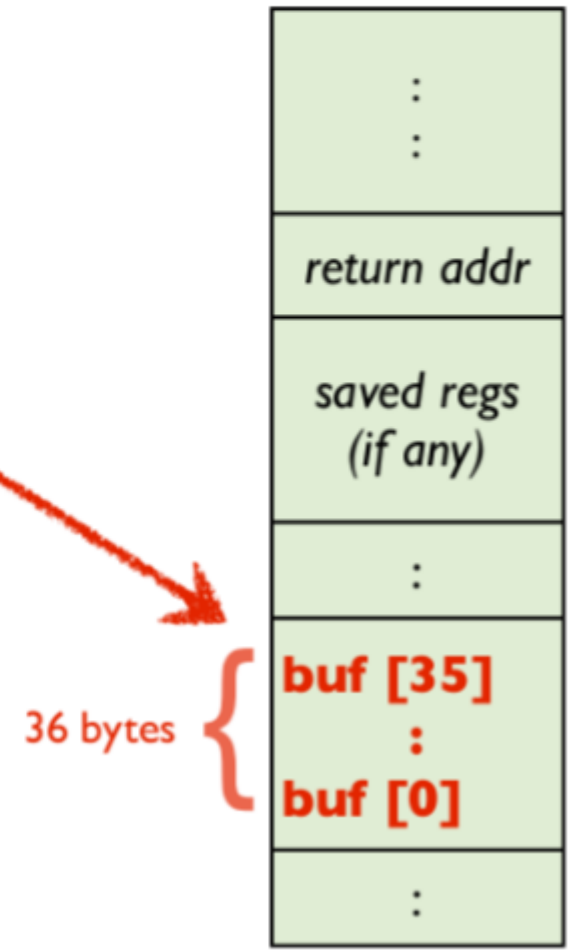
This has a buffer overflow

```
int getbuf() {
  char buf[36];
  Gets(buf);
  return 1;
}
```

Why?

- `Gets()` doesn't check the length of the buffer

The Stack in getbuf()



Level 0: Call `smoke()`

Goal: call the smoke() function from getbuf()

```
int getbuf() {
  char buf[36];
  Gets(buf);
  return 1;
}
```

How?

- overwrite the return address so we "return" to smoke()

The Stack in getbuf()