LAB

SQL injection

- http://sqlzoo.net/hack/

Integers in C

- int representation
  - sizeof(int)
- INT_MAX, INT_MIN, UINT_MAX
- Write a function detecting integer overflow
  - unsigned int plus(intigned int a, unsigned int b)

system(3) in UNIX

- Exploit the code to run arbitrary command
- Set the input variable to some value

```
#include <malloc.h>
#include <stdlib.h>


int main()
{

char *input = NULL;

// set input

input="Hi!";

//

char cmdbuf[512];
int len_wanted = snprintf(
  cmdbuf, sizeof(cmdbuf), "echo '%s'", input);
if (len_wanted >= sizeof(cmdbuf)) {
  perror("Input too long");
}
else if (len_wanted < 0) {
  perror("Encoding error");
}
else if (system(cmdbuf) == -1) {
  perror("Error executing input");
}

return 0;
}
```