Sploit1: In the function copyFile() in backup.c, from line 37 to line 42, the program uses **fgetc()** to get one character at a time from source file to a buffer in a while loop. The buffer size is limited to 2048 characters, and there is no boundary check when filling the buffer in this while loop. If source contains more characters than the buffer size, there is a buffer overflow. We can fix this vulnerability by adding boundary check.

Sploit2: In main function, there is a buffer of size 200. From line from line 225 to 237, there are several **strcat()** and **strcpy()** used. If we write more than 200 characters to the buffer (but actually less than that, since there are already 18 characters in the buffer), it will overwrite the return address and cause trouble. As a solution, we can add boundary check when using these two functions.