Buffer Overflow Exploit

Buffer overflow exploit happens in line 313 of submit.c file. The buf[2400] overflows when the length of scr_file exceeds the length of buf. When overflow happens, the contents that is out of the range (in this specific program, the 2nd variable, which is the return address of the method) of buf will be overwrites.

Note that when overwriting, counter is overwritten to 2403, so that the loop will not terminate when encountering \x00 before overwriting EIP.

To fix this, add a check for counter to make sure counter never exceed the length of buffer is enough. When the length exceeds, the loop will terminate, and no buffer overflow will happen.