CS 458 A1 Milestone

Tom Yan

Buffer Overflow Exploit

1. Buffer overflow exploit found in buf[4000] inside the copy_file function. It overflows when you write to the buffer from a text file that exceeds its length.

2. When it overflows, my program overwrites the contents after the buffer, namely the return address of the previous stack (main). The return address gets replaced with the address of the shellcode, stored in the 3rd argument.

3. The overflow can be fixed by adding a check for the counter not exceeding the buffer length inside the while loop condition. This way there is no chance of writing to indexes outside the buffer range thus a buffer overflow is not possible.

Format String Exploit

1. Format string exploit found in printf(version_info) inside the print_version function. A string containing %n could be inserted which can lead to overwriting contents of the stack.

2. My program exploits this by writing to the return address of the main function 1 byte at a time, with the address of the shellcode, stored in the 3rd argument. The 4th argument contains the addresses for each of the 4 bytes to be overwritten, which the %n's point to.

3. The vulnerability can be fixed by simply changing the line from printf(version_info) to printf("%s", version_info). This prevents version_info from scanning for %'s as it will simply be part of the string being substituted in.