ISP assignment part 3

Vulnerabilities i found in the previous code are

1. not checking if the file is open or not before writing the data. But in the new code i have initialized a variable called file_status to check the current status of the file. The hacker can have access to the file if we don't put a lock when the file is closed

2. In the writeat i was directly writing the data without checking anything if the offset value is -ve or not … or if the file is opened or not… so i the new code i am actually checking the value of offset. No one can write in the -ve position of offset.

3. In the previous code i have stored everything directly to a permanent file but now i have created a variable called file_size(we can know the file of the size) and temp_file - where the just written is stored before storing in the file forever. Vulnerability in the previous code was that everything written using the writeat function is stored permanently.

4. Previous code's undo function does not work as intended for example…. When the first writeat is called and immediate undo is called… the result file should be empty but the results are not as expected … it just does not delete the data. I achieved that in the current code with the help file_status variable.

5. Calling undo multiple times after multiple writeats does not undo the data written properly.. Which means it only deletes some part of the data which is appropriate. The newer version of code can handle that situation.

6. Last version of the code could handle basic open and close statements in the test case a few times .. but the newer version can handle this in every situation.

These are the vulnerabilities of my precious code and I made the changes to the code accordingly to overcome them.