Francis Delamerced

Computer Security - Assignment 2, Part 3 Writeup

There were a number of vulnerabilities I was able to fix, along with some that I was aware of but still not able to fix.

One was a NoneType error, which I discovered was just an inaccuracy in my code rather than a vulnerability. I had created a current\_data variable previously, but had not actually used it to store what the data before pending\_data actually was. So when someone tried to undo, it would attempt to rewrite the current\_data but there would be nothing in the current\_data causing a NoneType error.

One actual vulnerability I was able to resolve was the SeekPastEndOfFileError, in which attackers attempted to write past the end of the file. To fix this I created two new class attributes, self.current\_filesize and self.previous\_filesize. Through these attributes, I tracked the filesize of the file throughout. I would constantly changed the filesize if the offset and/or offset+length of the appended data was greater than the current filesize. However if the offset that an attacker used was ever more than 2 past this filesize then the code would raise a SeekPastEndOfFileError. Undos would also regress the filesize back to what it was previous.

One other vulnerability I was able to fix was attempts to write to the files when the file was closed. I also created a new class attribute ‘closed’ that would change based on if the file was open or not.

I wished to be able to address the threading vulnerabilities but errors in my code did not allow me to.