Probability ---------------------------->

Severity		Frequent	Probable	Likely	Possible	Rare
|	Emergency					
|	Major		6. Leaving code open to editing and not in a executable file will make the code vulnerable. 7. No logging process of updates or changes to the files will leave attacks undetected.		1. Input data will be put at risk due to a lack of encryption or protection. 3. The IDLE used to run the code will leave the code vulnerable when it is not updated. 4. Outdated libraries used in the code will leave the code vulnerable to infiltration.	9. User data will be vulnerable when the data is not stored in a secure location after the program closes.
|	Moderate		2. Malicious users will take advantage of a lack of user input restriction. 10. No training or ongoing maintenance to the code will leave the project vulnerable.		8. Not following official code structure guidelines will leave hidden vulnerabilities in the code.	
|	Minor				5. Lack of careful construction of class properties will leave the code vulnerable.	
|	Negatable					
\/						