Benjamin Efron
Alexis Fink
Austin Niccum
Misato Morino

Milestone One Topic Proposal

       For our project we have decided to research different types of code injection. Code injection is a powerful exploit which can give an attacker full control of the victim's system. We are interested in researching how code injection attacks work, and how to stop them. We will be researching different types of injection attacks over multiple languages, probably including Javascript and PHP, as both of these are popular backend languages. Other possibilities include Bash, C, Ruby, Java, Python, and Go. We also want to potentially research where most code injection attacks take place (i.e. file uploads, sent as requests, in images, etc.), and the possible differences between interpreted and compiled code injections. Ultimately, we plan on demonstrating some code injection attacks in addition to our research.

Questions:
1. How does code injection work?
2. Which backend languages are generally most vulnerable to code injection?
3. Where are the most vulnerable places to code injection?
4. What are some famous code injection attacks and what was the outcome?
5. What are common trends in protection against code injection?