KittenWarrior: CS557 Project 2

Thomas Le Baron
Computer Science
Worcester Polytechnic Institute
Worcester MA, USA
tlebaron@wpi.edu

Brittany Lewis
Computer Science
Worcester Polytechnic Institute
Worcester MA, USA
bfgradel@wpi.edu

***Abstract*—In this work we introduce a vulnerable binary "KittenWarrior" which has a vulnerable buffer overflow. We also prove that this binary can be explioted to launch shell code. We do this through overwriting the global offset table using a buffer overflow, and then using return oriented program to call mprotect and make our stack executable so that we can run our shell code.**