

CS557 Project 4: Screen 4.5

Thomas Le Baron
Team 1008
Computer Science
Worcester Polytechnic Institute
Worcester MA, USA
tlebaron@wpi.edu

Brittany Lewis
Team 1008
Computer Science
Worcester Polytechnic Institute
Worcester MA, USA
bfgradel@wpi.edu

Abstract—

I. FINDING SCREEN

- **Program:**
- **Exploit:** `/home/user/exploit.sh`
- **md5sum hash of the binary file:**
- **md5sum hash of the source file:**

II. INTRODUCTION

GNU Screen is a terminal multiplexer which allow the user to access multiple processes from an unique terminal. It is the shell version of a window manager. In 2017, Screen 4.5 presented a vulnerability allowing a user to get root privileges in the local machine running the program. The vulnerability of this version of the program came from the fact that it opened logfiles in root privileges. In this work we show a proof of concept of how this vulnerability can be used to get root privileges.

III. DESIGN

IV. IMPLEMENTATION

V. EXPLOITATION

VI. CONCLUSION