


Team 8

Final Presentation

Cari Martinez, Dena Vigil, Anton Kuzmin, Stephen
Sagartz, Meisam Navaki, Cheng- En Ho
May 3, 2017



Security is a hard problem

- No matter how hard you try to protect the system, there will always be a way to exploit it.
- Exploits can be performed at every level of the software stack. The more you know about data at each level, the more tools are available to perform an exploit and program 'the weird machine.'
- Learning how to cheat involves knowing how the program functions in the intended way.
- When developing applications, user input must be treated with extreme care.

Command Line Injections

- Command injection attacks are extremely powerful; we can execute **any** command with moderator privileges.
- Be cautious with any kind of code that would have the potential to run a command, e.g. `popen` in python.
- You don't need a sophisticated script to cheat. A game this big can be undermined by a single line of code.

What we learned from playing the game

- Always protect passwords. Never leave your screen with login info visible to other, untrustworthy, teams!
- Knowledge of OS commands helps players exploit code. For example, stat command could be a handy tool for file permission vulnerability
- You don't need a lot of time to perform an exploit. A fraction of a second is more than enough to compromise a system (race condition exploit)

Team Dynamics of Group 8

- LoboGit, Google Docs, Gmail, and Google Chat enabled us to team effectively and, often remotely
- Each team member contributed unique knowledge and/or coaching to other team members