CS166 Computer Systems Security Spring 2018

Dropbox Pentesting

Due Date: 11:59 pm, Thursday May 10

Contents

1 Instructions

You will be pentesting three dropbox projects to grade (one CS162 project and two CS166 projects). These projects are old TA implementations of dropbox and your mission is to hack your TAs. :) The pentesting implementations are located in /course/cs1660/student/¡your-login¿/dropbox. There are two required projects you MUST pentest (Skyfall and FromRussiaWithLove). You are allowed to choose a third project from the options folder.

Please do the pentesting only in your assigned directory. You are not allowed to copy or redistribute the project files.

You will can submit vulnerabilities you find in the implementations you've been assigned to pentest through this google form: `https://goo.gl/forms/1fgRZbY5IQT58CrG2`.

When submitting a vulnerability, include a detailed report of how the vulnerability works, and how it can be exploited. This should include instructions sufficient to reproduce the exploit that would allow even a person completely unfamiliar with the system to reproduce the exploit on their own. There should be no question how the vulnerability or the exploit works after reading your explanations.

You should also document the severity of the vulnerability by choosing one of the provided options. If you feel there is no category that adequately suits your vulnerability, please choose other and include a detailed explanation of your suggested class of vulnerability.

If you wish to submit files (such as scripts, payloads, etc) with your vulnerability, please run the following script from a CS department machine in a directory containing the relevant files:

dropbox_pentesting_submit

After submitting, you'll receive a code identifying the submission which you can include in the google form.

2 Grading

Everyone is required to pentest two projects: Skyfall and FromRussiaWithLove. The third project you pentest is up to you.

We have target scores recorded from last year recorded below for you to reference. Your goal is to reach the target score for pentesting each project or above. (This means if the target score says 0 if you find at least one vulnerability you will get full credit for pentesting that project.)

The dropbox handout has more information on pentesting and scoring. Point values for each submission will be assigned based on the severity of the exploit that you are able to accomplish. They will be evaluated on the following scale:

- 10 pts - Remote code execution: This exploit is similar to arbitrary code execution from Handin, but this time you dont need code to execute with TA permissions
- 7 pts - Account takeover: having control of another user's account (which includes being able to arbitrarily manipulate their file system)
- 6 pts - File modification/exfiltration: being able to read or change another user's files (but not arbitrarily — this would be above)
- 5 pts - File deletion: Deleting a users file you should not be able to delete
- 5 pts - Password hash exfiltration: Recovering a passwords hash for a user. If you recover the password and know the login this would be account take over.
- 5 pts - Denial of service: Anything that crashes the server
- 4 pts - Metadata exfiltration: his is the same type of attack as in Handin, but to count here In order, the metadata you learn must be sensitive in some way (for example, the names of files or directories that other users have created). Metadata exfiltration does not include finding out whether or not a username already exists or not. Many websites, like Reddit and gmail, will tell you if a username is already taken, so this isn't considered a vulnerability in the real world.
- 2 pts - Metadata deletion: Deleting metadata

3 Target Scores

Team Codename	**Target Score**
Skyfall (CS162)**	7
FromRussiaWithLove (CS166)**	17
Goldfinger (CS166)	18
Thunderball (CS166)	12
CasinoRoyale (CS162)	0
Spectre (CS162)	0

**Required to pentest

Note, the TAs are human too and some of the functionality might be a little buggy. Your goal is not to test functionality but to pentest/break our projects. If youre unsure if its a bug or a feature or are having trouble running our code, feel free to ask us on Piazza!

Have fun hacking your TAs!