Project Writeup Act 6

CSEC-380 Project Group 13

Connor Leavesley, Joshua Niemann

**How would you fix your code so that this issue is no longer present?**

Input sanitization and not using vulnerable flask functions would fix the issue. In the case of our code, send\_file returns the file at an arbitrary path and file location. The send\_from\_directory function should be used instead, which provides some protection against accessing files outside of a directory, and the data should be sanitized.

**How does your test demonstrate SSRF as opposed to just accessing any old endpoint?**

The test demonstrates that /etc/passwd can be downloaded by abusing the /getVideo endpoint. /etc/passwd is an internal file and should not be able to be accessed. But due to the SSRF vulnerability it can be accessed by any user.