Remote and Local File Inclusion (RFI/LFI) is a vulnerability that occurs when a file is included without sanitizing the data. Remote File Inclusion involves a file hosted on another server where an attacker will lure them through websites to run malicious code. Local File Inclusion involves files that are intended to be included on the same web server or system that the target web application is hosted on.

I’m going to be completing the example LetsDefend lab “Detecting RFI & LFI Attacks”.

Opening the log file, we find that the attack starts at 11:58 on March 1st 2022 as the attacker tries to access the root directory. Fortunately, the attacker was likely unsuccessful when viewing the HTTP responses. While 200 is successful, the amount of data received is too small for something like a list of passwords. The attacker possible received error codes, which it why the size variable was only 50.

