Tab 1

Insecure Direct Object Reference (IDOR) is a vulnerability caused by the absence or improper use of an authorization mechanism. It allows one person to access an object that belongs to another. IDOR is also commonly known as Broken Access Control, and is considered the most common vulnerability according to OWASP 2021.

In this short lab from let's defend “Detecting Insecure Direct Object Reference (IDOR) Attacks”, I will analyze a log file for potential IDOR attacks.

Looking through the log file, I found a concerning pattern of receiving the id variable. In the log file the IP 192.168.31.174 starting March 1st at 11:42 AM, starts sending requests each for incrementing id values. This is likely a brute-force method to reach all potential objects. Unfortunately, their attack was likely successful when looking at the 200 value HTTP response code. It is unlikely an automated brute force attack, as there was some time between each request.

