# Broken access control not indexed directory

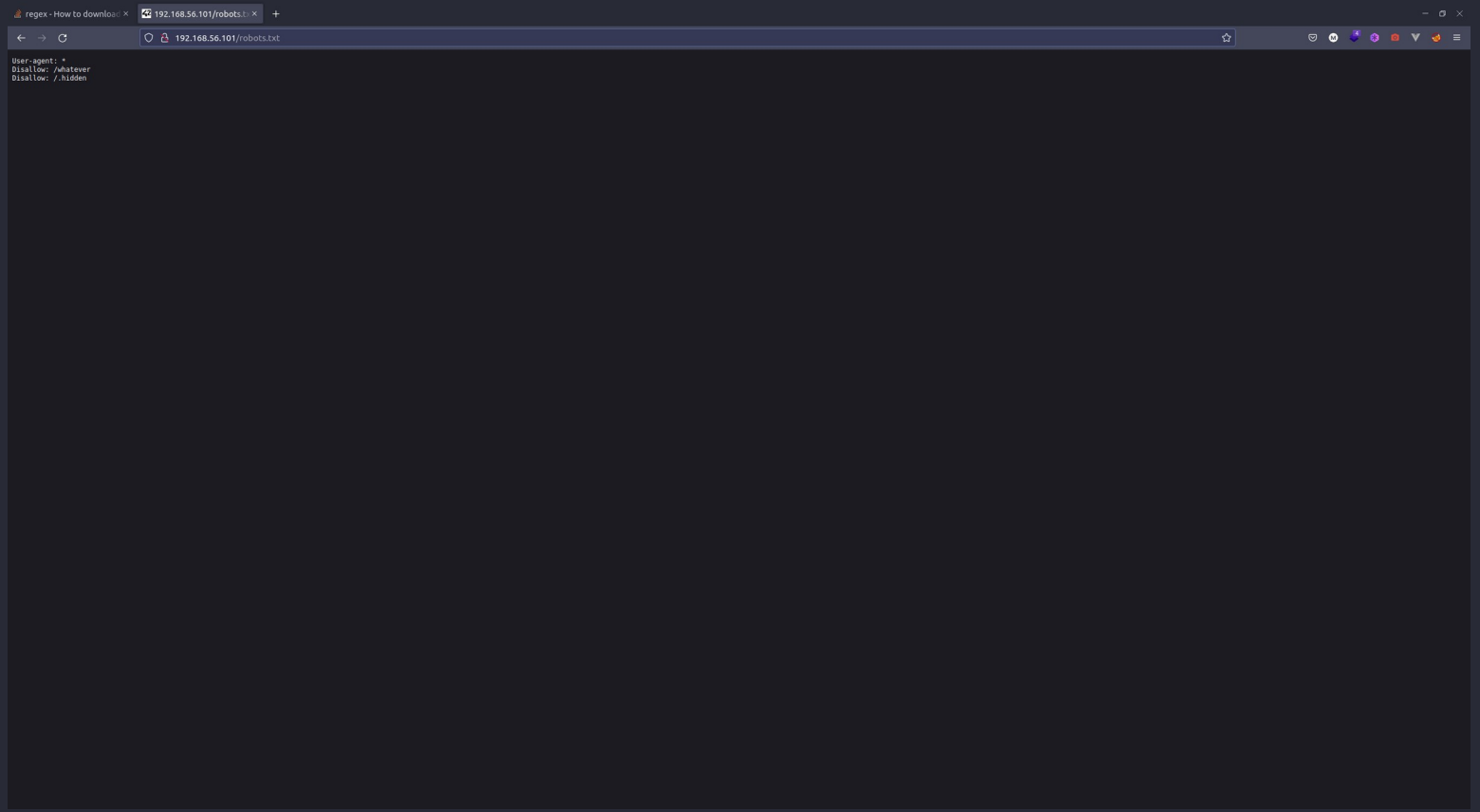
Moving up from the fifth position, 94% of applications were tested for some form of broken access control with the average incidence rate of 3.81%, and has the most occurrences in the contributed dataset with over 318k. Notable Common Weakness Enumerations (CWEs) included are CWE-200: Exposure of Sensitive Information to an Unauthorized Actor, CWE-201: Insertion of Sensitive Information Into Sent Data, and CWE-352: Cross-Site Request Forgery.

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

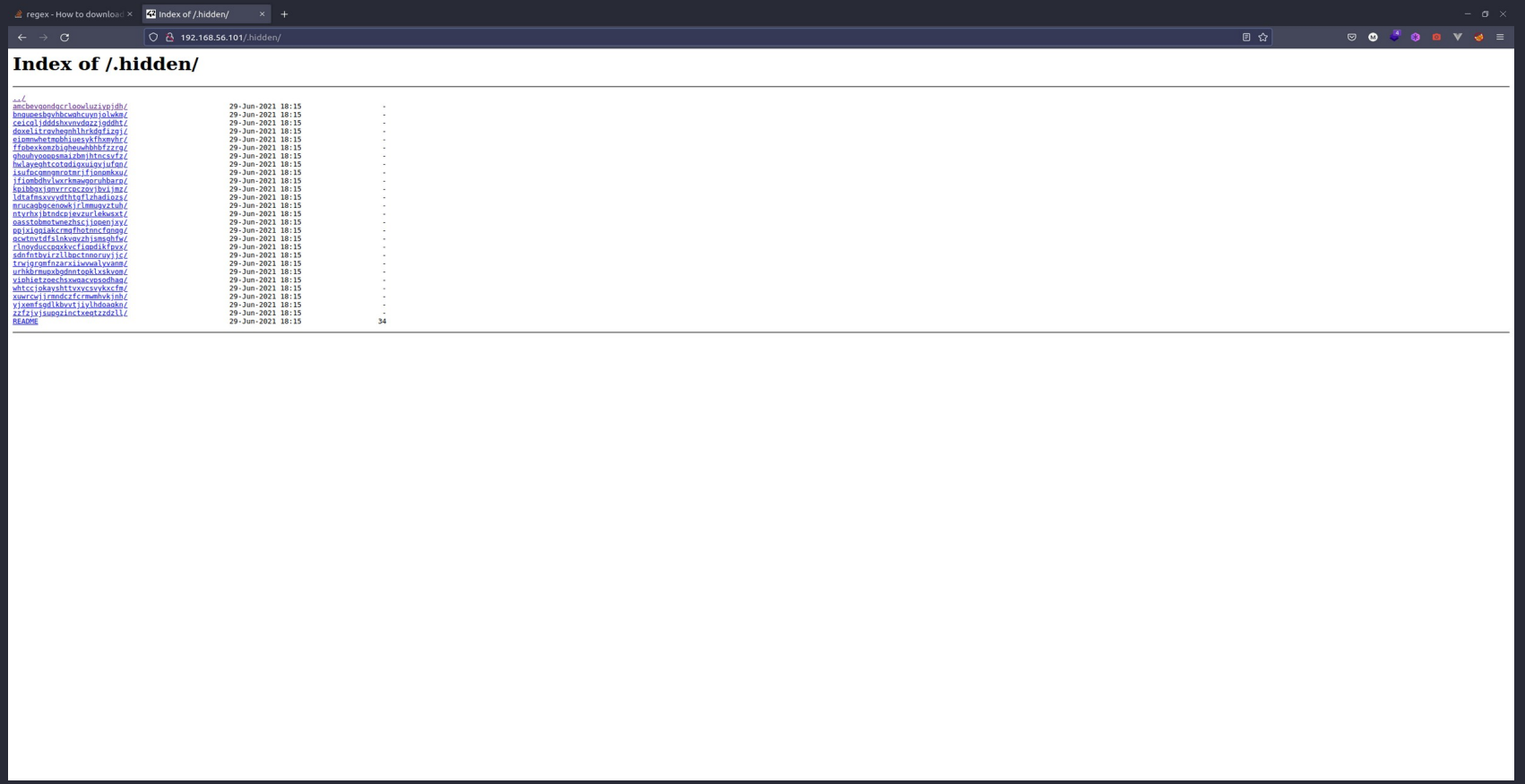
In this context we talk about an hidden directory

# Walk through

Step 1 : try to access to the robots.txt file we saw 2 not indexed directories

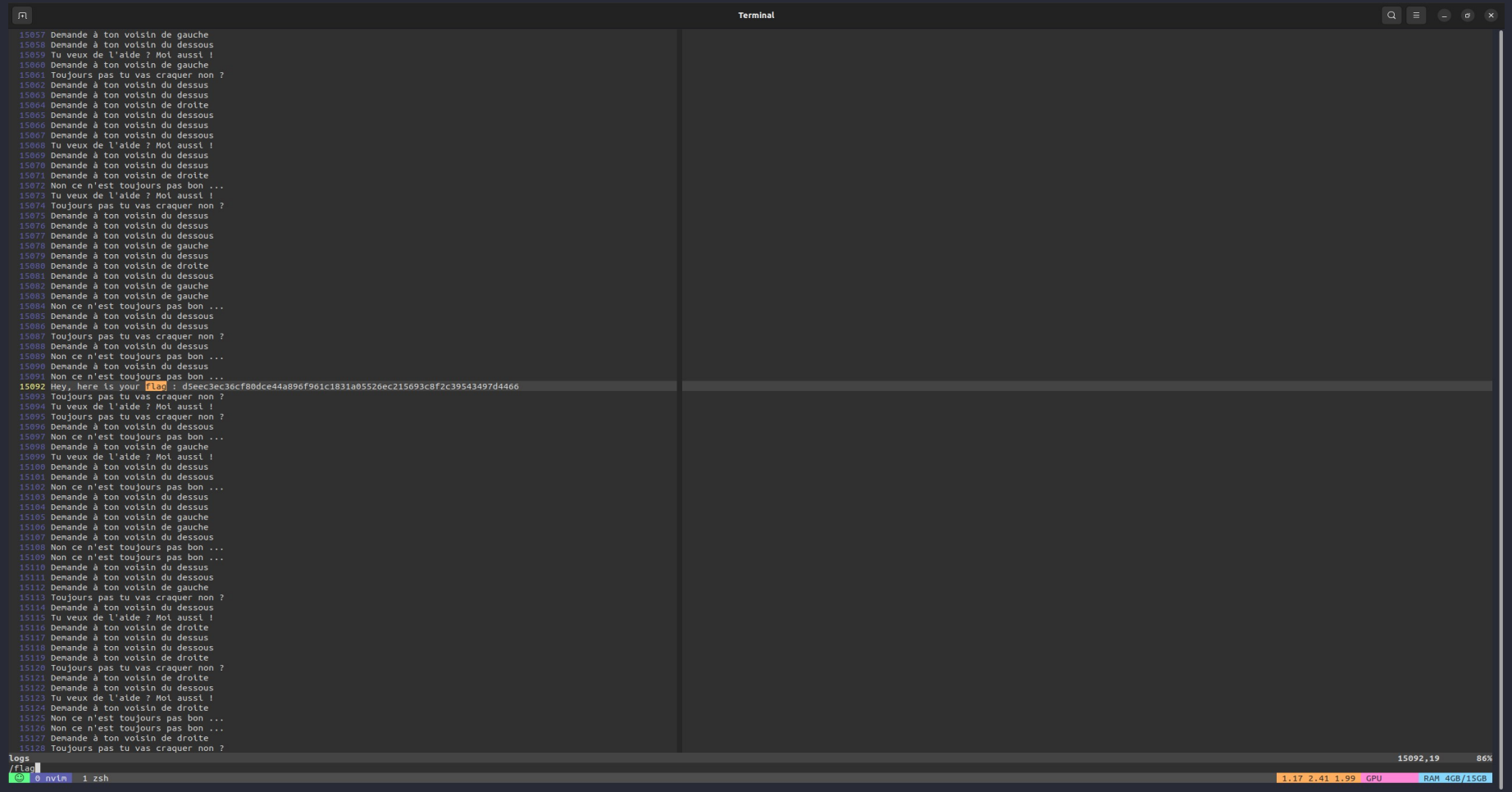


Step 2 : Try to access to the .hidden directory, they have a lot of directories/files, so download with the command '*wget -r –no-parent -e robots=off http://192.168.56.101/.hidden/*'



# Step 3 : Get the value of all the files with the command : cat */*/*/* > flag

Step 4 : search for the flag keyword in vim or with cat file | grep flag for example and get the flag !



# How to fix

- Disable directory listing in the webserver config
- Block access to the unindexed directories