Labyrinth Linguist

You and your faction find yourselves cornered in a refuge corridor inside a maze while being chased by a KORP mutant exterminator. While planning your next move you come across a translator device left by previous Fray competitors, it is used for translating english to voxalith, an ancient language spoken by the civilization that originally built the maze. It is known that voxalith was also spoken by the guardians of the maze that were once benign but then were turned against humans by a corrupting agent KORP devised. You need to reverse engineer the device in order to make contact with the mutant and claim your last chance to make it out alive.

How to play

This is a server side template injection challenge for apache velocity.

A search in web for `apache velocity server side template injection` will give all we need.

By looking at `Dockerfile` we can see the flag is in `flag.txt` file. But in the end the `entrypoint.sh` script will execute, and file name would be randomized.

So we need full shell execution.

We can make a simple payload request using python, first do a `ls /` to see the files in the root directory. Then we can do a `cat /flag.txt` to get the flag.

```
#set($process=$runtime.exec("ls /"))
```

The full payload.

Flag