# Wordus (MEDIUM)

### Auteur(s):

Hokanosekai

## Catégorie:

Misc

## Description:

Voici le site web créé par des étudiants de la promo lors d'une gamejam. Ils ont caché un flag quelque part, saurez-vous le retrouver ?

wordus.xyz

Note: Uniquement pour ce challenge, les joueurs sont autorisés à utiliser des outils d'énumération sur le serveur (rattaché au nom de domaine wordus.xyz). (Toute autre attaque non autorisée sera sanctionnée)

Flag UHOCTF{Fake\_flag}

### Solution:

Pour commencer nous pouvons éxécuter des outils d'énumerations sur le serveur. Tel sue gobuster, pour énumérer les sous-domaines ainsi que les fichiers et répertoires.

Il faut par exemple pour les sous domaine chercher une liste des plus commun, comme celle-ci :

MR-pentestGuy/dns-wordlist

PROF

Found: imap.wordus.xyz
Found: mail.wordus.xyz
Found: mc.wordus.xyz

Progress: 473 / 22978 (2.06%)

On peut y voir plusieurs sous-domaines intéressants :

- ftp.wordus.xyz
- imap.wordus.xyz
- · mail.wordus.xyz
- mc.wordus.xyz

On peut donc commencer par regarder le sous domaine le plus intéressant, mc.wordus.xyz.

On peut donc éxécuter un scan de port sur le sous domaine.

```
hoka@hoka ~> nmap -p 25565 mc.wordus.xyz

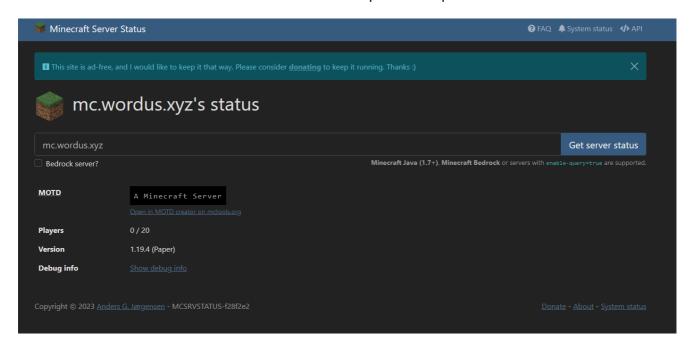
Nmap scan report for mc.wordus.xyz (172.67.163.27)
Host is up (0.015s latency).
Other addresses for mc.wordus.xyz (not scanned): 104.21.15.159
2606:4700:3031::ac43:a31b 2606:4700:3030::6815:f9f

PORT STATE SERVICE
25565/tcp filtered minecraft

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
```

On peut donc confirmé que le sous domaine est bien un serveur minecraft.

Grace au site Minecraft Server Status Checker on peut voir que le serveur est en 1.19.4.



PROF

On s'y connecte avec un client minecraft et on se retrouve dans un monde vanilla en 1.19.4.

On remarque deux commandes :

- /wordus
- /flag

La commande /flag:flag nous kick du serveur.

Enfin la commande /wordus:wordus nous donne le flag.

Et oui, le jeu Wordus n'était qu'un leurre.

Flag UH0CTF{w0rdus\_1s\_4w3s0m3}

PROFESSEUR : M.DA ROS + 3 / 3 + BTS SIO BORDEAUX - LYCÉE GUSTAVE EIFFEL