

# 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](http://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](http://wordus.xyz)). (Toute autre attaque non autorisée sera sanctionnée)

**Flag** `UH0CTF{Fake_flag}`

---

Solution :

Pour commencer nous pouvons exécuter des outils d'énumérations sur le serveur. Tel que [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](https://github.com/MR-pentestGuy/dns-wordlist)

```
hoka@hoka ~-> gobuster -m dns -u wordus.xyz -w my-wordlist.txt

=====
Gobuster v2.0.1                OJ Reeves (@TheColonial)
=====
[+] Mode           : dns
[+] Url/Domain     : wordus.xyz
[+] Threads       : 10
[+] Wordlist       : ctf/UnivCTF/UH0CTF/MISC/Wordus/wordlist.txt
=====
2023/06/10 19:08:29 Starting gobuster
=====
Found: autoconfig.wordus.xyz
Found: autodiscover.wordus.xyz
Found: ftp.wordus.xyz
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

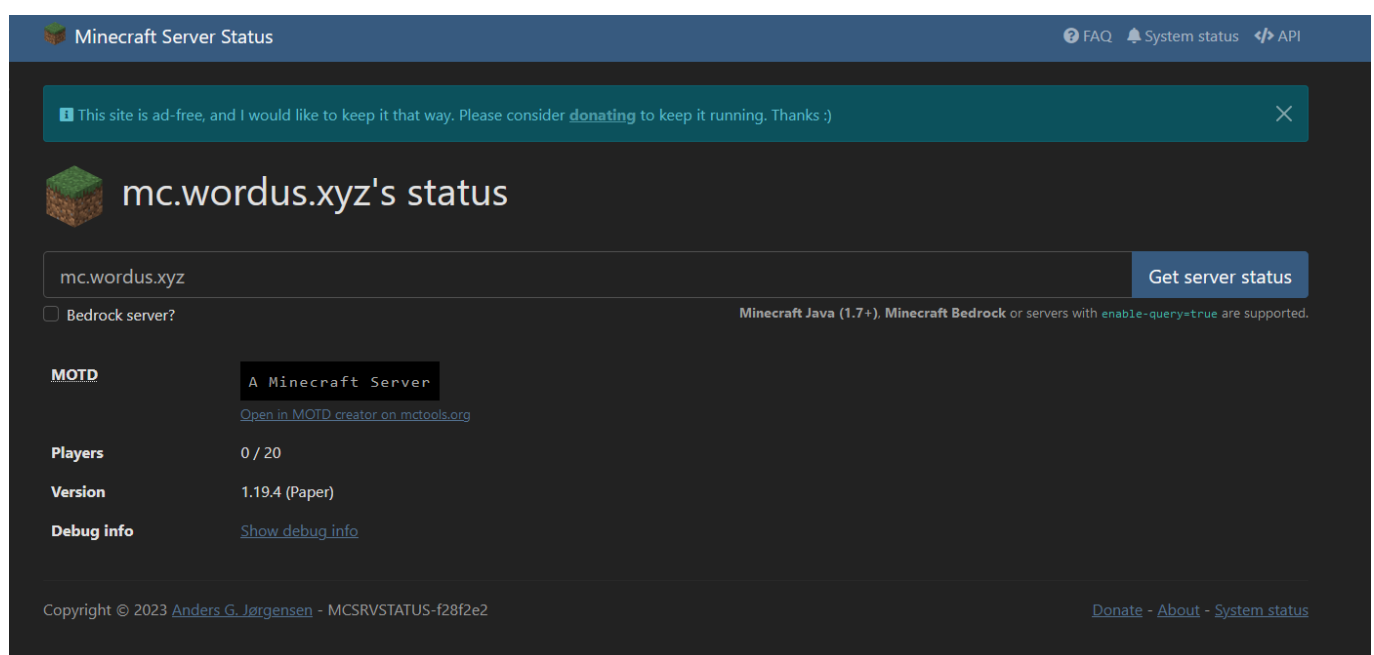
On peut donc commencer par regarder le sous domaine le plus intéressant, **mc.wordus.xyz**.

On peut donc exécuter 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.



The screenshot shows the 'Minecraft Server Status' website. At the top, there's a navigation bar with links for FAQ, System status, and API. A teal banner at the top states: 'This site is ad-free, and I would like to keep it that way. Please consider donating to keep it running. Thanks :)'. The main heading is 'mc.wordus.xyz's status'. Below this, there's a search bar containing 'mc.wordus.xyz' and a 'Get server status' button. A checkbox for 'Bedrock server?' is present, with a note: 'Minecraft Java (1.7+), Minecraft Bedrock or servers with enable-query=true are supported.' The server status is displayed as follows:

MOTD	A Minecraft Server
Players	0 / 20
Version	1.19.4 (Paper)
Debug info	Show debug info

At the bottom, there's a copyright notice: 'Copyright © 2023 Anders G. Jørgensen - MCSRVSTATUS-f28f2e2' and links for 'Donate', 'About', and 'System status'.

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}`