

Write-up - Un agent pas comme les autres

Auteur : Wa0k

CTF Flag'Malo 2022

Le titre du challenge nous oriente vers une caractéristique des navigateurs : le user-agent.

Pour information : L'**user-agent** est une chaîne de caractères générées généralement par un navigateur lors de la visite d'une page quelconque : celle-ci contient des informations notamment son nom, sa version, le système d'exploitation...

Après avoir compris ce qu'est un user-agent, nous pouvons essayer de voir à quoi ressemble son user-agent via ce [site](#).

En s'inspirant du résultat et de l'hint donné dans l'énoncé, nous pouvons construire notre propre user-agent pour remplir les conditions : Nokia 3310 Chrome/60.0.3110.70.

Plusieurs façons s'offrent alors à nous pour visualiser la page en modifiant le user-agent original par celui-ci.

1. La première méthode consiste à le modifier dans l'en-tête de la requête HTTP via l'outil d'inspecteur d'éléments (F12).
2. La deuxième méthode est d'utiliser la commande `curl` qui permet de faire des requêtes HTTP simples en ligne de commande.
3. La troisième méthode est d'utiliser l'outil [Burpsuite](#) qui permet d'intercepter des requêtes HTTP pour ensuite modifier le contenu à sa guise et renvoyer la requête.

Pour ce write-up, j'ai décidé d'utiliser la commande `curl`, et grâce à l'option `A` nous pouvons spécifier l'user-agent à utiliser.

Parfait ! Nous obtenons alors la commande : `curl -A "Nokia 3310 Chrome/60.0.3110.70" http://10.100.1.201:5004/`

Nous obtenons donc le flag : `FMCTF{U$3r_4g3Nts_R_n0t_4_$3CuR1ty}`.