Reto Hacker 2 – CTF (*Capture The Flag*)

Curso 2019-2020

Temática: Hacking Web

Amador Aparicio de la Fuente (https://mypublicinbox.com/AmadorAparicio)

Durante el proceso de desinfección de un ataque cibernético a una organización, se ha extraído la copia de una máquina virtual (fichero *.OVA*) con un fichero, *flag.txt*, con la información posible para poder desactivar el avance de la pandemia.
De manera parcial, se ha conseguido la extracción de un fichero *.php* con parte del código fuente que los especialista creen que puede ser útil para frenar los futuros contagios de la pandemia.

Contenido del fichero '`coronavirus.php`':

```
<?php
   $file = $_GET['file'];
   if(isset($file))
   {
       include("$file");
   }
   else
   {
       include("index.php");
   }
?>
```

El reto consiste en encontrar el fichero, `flag.txt`, y su contenido en 'texto claro' para intentar parar la pandemia que nos afecta.

ENTREGABLE

Se deberá de entregar un fichero en formato .pdf a la dirección de correo electrónico amador@centrodonbosco.es donde se expliquen todos los pasos desarrollados para que cualquier persona que lo tenga pueda reproducir todos sus pasos con éxito.

RECOMPENSA

Como recompensa, la cantidad de tiempo invertido para resolver un problema realista y en conocimiento adquirido. Además, la primera solución que cumpla con las condiciones anteriores

será publicado en un blog de Seguriad Informática de amplio espectro, y siempre se podrá presentar la solución en modo de portfolio en una entrevista de trabajo.

DESCARGA DE RECURSOS

Tanto el enunciado, cómo el fichero virtual *.OVA* para poder levantar levantar la máquina virtual, se encuentran en la siguiente URL de descarga:

https://bit.ly/2xxUCi0