Exfil - Web 300

Descripción:

Encuentra la vulnerabilidad en el siguiente sitio web y lee la flag que está en /app/app/flat.txt

http://3.19.72.219:3130

El reto nos proporciona la IP y el número de puerto para acceder a la página. Al entrar al sitio web, se nos mostraba una página la cual nos permitía subir un archivo con extensión **xml**. El propósito de esta función era introducir los datos de contactos para que la página los imprimiera de forma ordenada.

A partir de lo anterior sabíamos que debíamos explotar dicha funcionalidad de la página a partir de una payload entregada en un archivo **xml** el cual nos permitiera extraer el archivo acceder al directorio /app/app y extraer el archivo flag.txt.

Investigando encontramos un ataque de nombre **XML External Entity (XEE) Processing.** Donde, debido a un mal manejo de archivos, podemos acceder a los archivos locales del servidor, como en el que se encuentra la flag.

Para crear nuestra payload tomando como ejemplo y punto de partida partiendo del siguiente código:

A partir de ahí creamos nuestro archivo **xml** modificado el cual nos permitiría tener acceso al archivo deseado.

```
<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE own [
   <!ELEMENT own ANY >
   <!ENTITY xxe SYSTEM "file:///app/app/flag.txt" >]>
<directorio>
<contacto>
<nombre>&xxe;</nombre>
<telefono>111-111-1111</telefono>
</contacto>
```

Debido a que el nombre era uno de los campos que se imprimían en la página, se coloca en ese espacio la variable creada anteriormente, la cual, hace referencia al archivo de flag.txt.

Al subir el archivo, se imprimía en pantalla el siguiente texto el cual contenía la flag:

```
Se importaron correctamente los siguientes contactos:
hackdef{d0_n0t_tru5t_xml_f1l3s}
```