Writeup – Flag 3 (Planned-Flags-signed-2.pdf)

Contexto del reto

- El PDF fue publicado por la ley alemana de libertad de información (Informationsfreiheitsgesetz), con información “redactada”.
- Hay **6 flags ocultas** en el mismo archivo (6 retos distintos).
- **Objetivo de este reto:** entregar la flag que **contiene un "3"** (Submit here the flag containing a 3).

Herramientas usadas

- **mutool** (MuPDF) – extracción de imágenes y recursos del PDF
- **pdftotext** – extracción de texto visible
- **strings / grep** – búsqueda de cadenas en el binario
- **qpdf** – descompresión de objetos del PDF (opcional, para anotaciones/URIs)

Metodología

1. Análisis inicial del texto visible

Con `pdftotext Planned-Flags-signed-2.pdf -` se ve que:

- En la **sección 3.4** aparecen en claro flags como `ENO{stability gradient 1 disrupted}` (contienen "1", no "3").
- En **3.3** (Applied Cryptanalytic Methodologies and Information Obfuscation Studies) el texto de las flags está **redactado**: solo se ven las llaves vacías `{ }` y el resto tapado.

Por tanto, la flag con "3" no está en el texto extraíble directamente; hay que buscar dónde quedó el contenido “redactado”.

2. Búsqueda en metadatos y anotaciones

- **Metadatos (exiftool / XMP):** el campo Producer contiene `ENO{secureflaghidingsystem76}` — contiene 7 y 6, no 3.
- **Anotaciones (qpdf --qdf + grep):** solo aparecen URIs con `ENO{input_sanitization_2_is_overrated}` — contiene 2, no 3.

Ninguna de estas es la flag que pide el reto.

3. Extracción de recursos del PDF

El contenido sensible a menudo se oculta **sustituyendo texto por una imagen** (por ejemplo borrosa). Conviene extraer todas las imágenes:

```
mutool extract Planned-Flags-signed-2.pdf
```

Se obtienen, entre otras, **image-0080.png** (objeto 80) e **image-0117.png**. La primera es una imagen de **1042×337 píxeles** que corresponde al **bloque de texto redactado de la página 2**, es decir, a la sección **3.3** donde se listan las seis flags de “Applied Cryptanalytic Methodologies and Information Obfuscation Studies”.

4. Análisis de la imagen (contenido redactado)

En **image-0080.png** el texto está **intencionadamente borroso**, pero aún se distingue la estructura del párrafo:

- "The first flag is ..."
- "The second flag is ..."
- **"The third flag is ENO{semantic_3_inference_initialized}, ..."**
- y el resto de flags (fourth, fifth, sixth).

La **tercera** flag es la que **contiene el carácter "3"** en su cuerpo: **semantic_3_inference_initialized**. El formato del documento (palabras en inglés separadas por guion bajo dentro de `ENO{...}`) se respeta con esta forma.

Solución

La flag que contiene un "3" y corresponde a este reto es:

```
ENO{semantic_3_inference_initialized}
```

Resumen de pistas descartadas

Origen	Contenido	Motivo de descarte
Producer (metadatos)	ENO{secureflaghidingsystem76}	Contiene 7 y 6, no 3
URIs (anotaciones)	ENO{input_sanitization_2_is_overrated}	Contiene 2, no 3
Sección 3.4 (texto)	ENO{stability gradient 1 disrupted}	Contiene 1; patrón distinto

Conclusiones

- En PDFs “redactados”, el contenido no siempre se elimina: a veces se **reemplaza por una imagen** (p. ej. borrosa) que sigue siendo analizable.
- **Extraer y revisar todas las imágenes** del PDF (`mutool extract` o herramientas equivalentes) es un paso estándar en análisis forense de documentos.
- La flag que “contiene un 3” era la **tercera** flag de la sección 3.3, oculta en esa imagen de contenido redactado.