CTF WriteUp: DigiKitkat

En este reto de hardware nos encontramos con un desafío relacionado con archivos Gerber (.gbr) que son utilizados en el diseño de circuitos impresos (PCB).

Descripción del reto

"Mi gran amigo Joe Grand ha diseñado un dispositivo hardware capaz de realizar ataques de Keylogging. Me ha dicho que ha guardado una sorpresa en él, pero no tengo ni idea de esto del hardware. ¿Me ayudas?"

Análisis inicial

El reto nos proporciona un archivo ZIP que contiene múltiples archivos con extensión .gbr. Estos son archivos Gerber, que son el estándar de la industria para la fabricación de PCB y contienen información sobre las diferentes capas del circuito.

La mención a Joe Grand es relevante, ya que es un conocido hacker de hardware y diseñador de productos electrónicos. El tema del keylogging también nos da una pista sobre el tipo de dispositivo que estamos analizando - un dispositivo que registra pulsaciones de teclas.

Herramientas utilizadas

Para visualizar los archivos Gerber, instalamos KiCad, que es un software de diseño electrónico de código abierto que permite ver y editar diseños de PCB.

Proceso de resolución

1. Instalamos KiCad para poder visualizar los archivos Gerber.
2. Abrimos KiCad y utilizamos el Visor de Gerber (GerbView) para cargar los archivos:
    - Seleccionamos **File -> Load Gerber File** y cargamos todos los archivos .gbr.
3. Una vez cargados los archivos, podemos ver el diseño del circuito PCB completo.

4. Notamos que diferentes archivos .gbr corresponden a diferentes capas del PCB. En KiCad, podemos controlar la visibilidad de estas capas mediante el panel de apariencia.
5. Comenzamos a experimentar activando y desactivando diferentes capas para ver si encontramos algo oculto. En KiCad, esto se hace haciendo clic en el icono de visibilidad junto a cada capa.
6. Después de probar con varias combinaciones, nos centramos en la capa 25 "BottomPaste", que estaba oculta debajo del circuito principal.
7. Al activar esta capa y desactivar las demás capas, descubrimos la flag oculta en el diseño del PCB.

Solución

La flag estaba escondida en la capa 25 "BottomPaste" del diseño PCB:

hfctf{¡B13nv3n1d0_A1_MuNd0_d3l_D1s3ño_h4ardwar3!}