Ausencia de validación de parámetros	MEDIA

CATEGORIA	Improper Input Validation

TARGET

POST /front/web-app/cannel-activity-history/v1/operations

OPERATIVA	PLATAFORMA
Modificación Datos de Contacto Móvil	BSM

REFERENCIAS

https://cwe.mitre.org/data/definitions/20.html

RIESGO

Se ha detectado la posibilidad modificar la petición que indica si el cliente ha leído y acepta los términos y condiciones mostrados durante el flujo, de forma que se malverse el resultado, alegando así que no se hayan aceptado cuando realmente ha sido así entre otros escenarios.

DETALLES

USUARIO	Usuario dado de alta en Onfido
ENTORNO	ACC
VERSIÓN DE LA APP - WAR	Sabadell | Desarrollo (25.4.0) - https://acc.bancsabadell.mobi/bsmobil_GFT-0000/api
ACCESO A LA OPERATIVA	Desde la Posición Global, al acceder a “Perfil y configuración” > “Mis datos personales”, es posible visualizar el número de teléfono ofuscado y una flecha a su lado que indica por modificarlo.

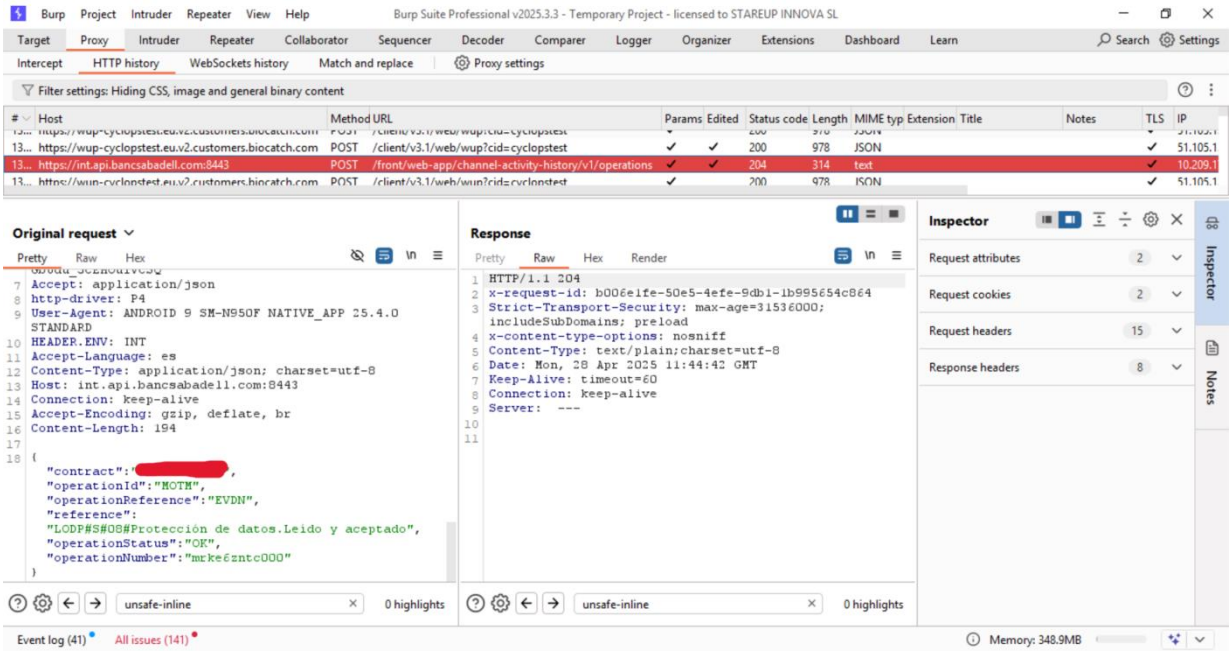
Al acceder al flujo de modificación del número de teléfono, se nos muestra la documentación de protección de datos y se le solicita al usuario aceptar los términos y condiciones.

Sin embargo, al pulsar sobre el botón, la petición que se envía y se registra en los logs puede ser modificada y no parece que su contenido sea correctamente validado, ya que es posible substituir el “body” por una petición de rechazo y el flujo sigue inalterado.

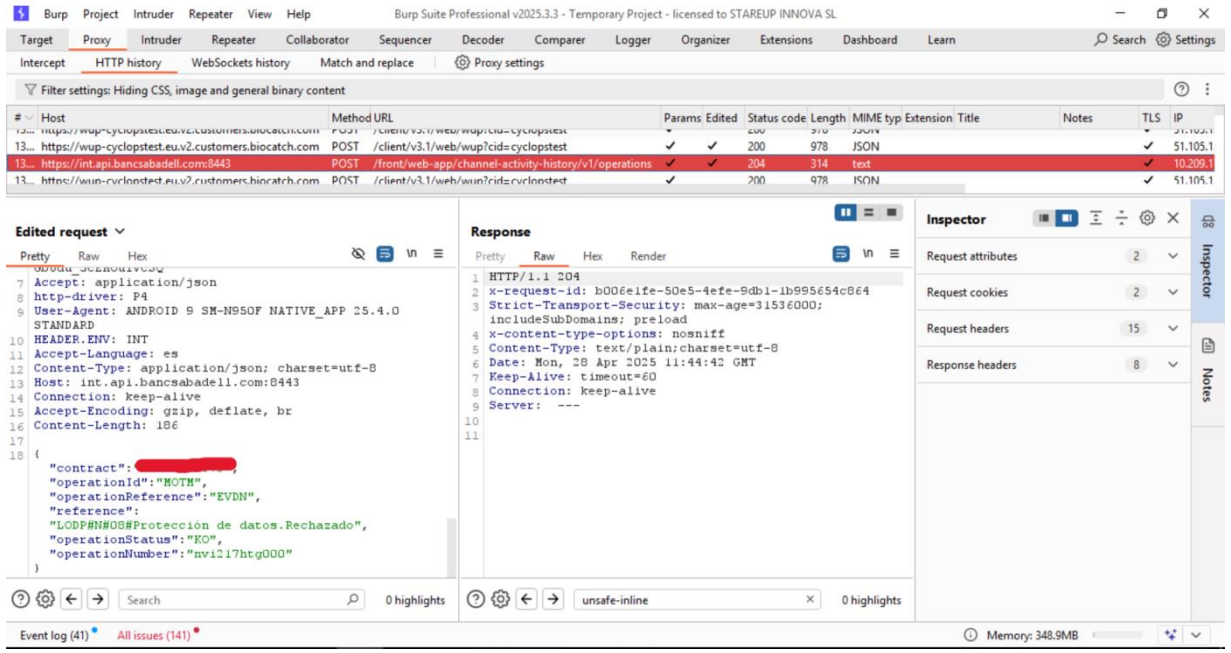
Según se ha podido comprobar, en los logs se guarda la petición modificada y no parece haber otra forma de confirmar si el proceso puede demostrar que el usuario aceptó o no la documentación.

EVIDENCIAS:

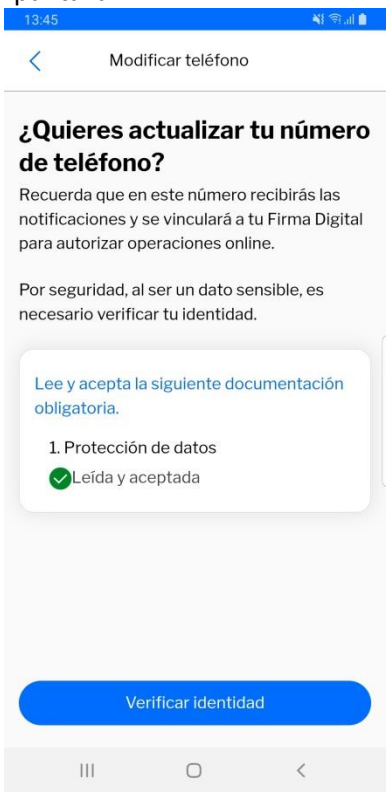
- Pantallazo de la petición original



- Pantallazo de la petición editada



- Pantallazo del resultado por pantalla



RECOMENDACIÓN

Realizar una validación por parte del backend de que el estado de la petición equivale al valor real y permitido de la acción, sin que éstos puedan ser modificados desde cliente. Validar y limpiar correctamente los campos que llegan al servidor de manera que solo acepte los valores que se esperan, en el formato que se espera y con un límite de caracteres en función del parámetro.