

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

The screenshot displays the Burp Suite Professional v2025.3.3 interface. The 'HTTP history' tab is active, showing a list of intercepted requests. The selected request is a POST to `https://int-api.bancsabadell.com:8443` with a status code of 204. The 'Original request' and 'Response' panels are visible. The request is a JSON object with the following fields: `contract`, `operationId`, `operationReference`, `reference`, `LODP#N#08#Protección de datos.Leído y aceptado`, `operationStatus`, and `operationNumber`. The response is a 204 status code with no content.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP
12...	https://wup-cycloptest.eu2.customers.biocatch.com	POST	/client/v3.1/web/wup?cid=cycloptest		✓	200	978	JSON				✓	51.105.1
13...	https://wup-cycloptest.eu2.customers.biocatch.com	POST	/client/v3.1/web/wup?cid=cycloptest		✓	200	978	JSON				✓	51.105.1
13...	https://int-api.bancsabadell.com:8443	POST	/front/web-app/channel-activity-history/v1/operations		✓	204	314	text				✓	10.209.1
13...	https://wup-cycloptest.eu2.customers.biocatch.com	POST	/client/v3.1/web/wup?cid=cycloptest		✓	200	978	JSON				✓	51.105.1

Original request

```
7 Accept: application/json
8 http-driver: P4
9 User-Agent: ANDROID 9 SM-N950F NATIVE_APP 25.4.0
10 STANDARD
11 HEADER: ENV: INT
12 Accept-Language: es
13 Content-Type: application/json; charset=utf-8
14 Host: int-api.bancsabadell.com:8443
15 Connection: keep-alive
16 Accept-Encoding: gzip, deflate, br
17 Content-Length: 194
18 {
  "contract": "XXXXXXXXXX",
  "operationId": "MOTW",
  "operationReference": "EVDN",
  "reference": "XXXXXXXXXX",
  "LODP#N#08#Protección de datos.Leído y aceptado",
  "operationStatus": "OK",
  "operationNumber": "mck66zntc000"
}
```

Response

```
1 HTTP/1.1 204
2 X-Request-Id: b006e1fe-50e5-4efe-9db1-1b995654c864
3 Strict-Transport-Security: max-age=31536000;
  includeSubDomains: preload
4 x-content-type-options: nosniff
5 Content-Type: text/plain; charset=utf-8
6 Date: Mon, 28 Apr 2025 11:44:42 GMT
7 Keep-Alive: timeout=60
8 Connection: keep-alive
9 Server: ---
10
11
```

Inspector: Request attributes (2), Request cookies (2), Request headers (15), Response headers (8).

Event log (41) All issues (141) Memory: 348.9MB

• Pantallazo de la petición editada

The screenshot displays the Burp Suite Professional v2025.3.3 interface. The 'HTTP history' tab is active, showing a list of intercepted requests. The selected request is a POST to `https://int-api.bancsabadell.com:8443` with a status code of 204. The 'Edited request' and 'Response' panels are visible. The request is a JSON object with the following fields: `contract`, `operationId`, `operationReference`, `reference`, `LODP#N#08#Protección de datos.Rechazado`, `operationStatus`, and `operationNumber`. The response is a 204 status code with no content.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP
12...	https://wup-cycloptest.eu2.customers.biocatch.com	POST	/client/v3.1/web/wup?cid=cycloptest		✓	200	978	JSON				✓	51.105.1
13...	https://wup-cycloptest.eu2.customers.biocatch.com	POST	/client/v3.1/web/wup?cid=cycloptest		✓	200	978	JSON				✓	51.105.1
13...	https://int-api.bancsabadell.com:8443	POST	/front/web-app/channel-activity-history/v1/operations		✓	204	314	text				✓	10.209.1
13...	https://wup-cycloptest.eu2.customers.biocatch.com	POST	/client/v3.1/web/wup?cid=cycloptest		✓	200	978	JSON				✓	51.105.1

Edited request

```
7 Accept: application/json
8 http-driver: P4
9 User-Agent: ANDROID 9 SM-N950F NATIVE_APP 25.4.0
10 STANDARD
11 HEADER: ENV: INT
12 Accept-Language: es
13 Content-Type: application/json; charset=utf-8
14 Host: int-api.bancsabadell.com:8443
15 Connection: keep-alive
16 Accept-Encoding: gzip, deflate, br
17 Content-Length: 186
18 {
  "contract": "XXXXXXXXXX",
  "operationId": "MOTW",
  "operationReference": "EVDN",
  "reference": "XXXXXXXXXX",
  "LODP#N#08#Protección de datos.Rechazado",
  "operationStatus": "KO",
  "operationNumber": "nvi217htg000"
}
```

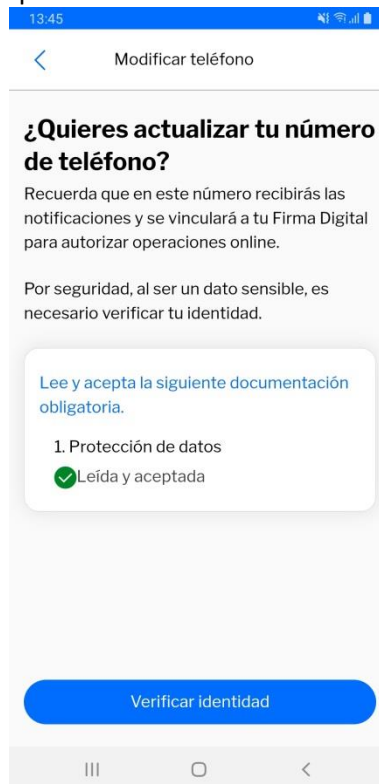
Response

```
1 HTTP/1.1 204
2 X-Request-Id: b006e1fe-50e5-4efe-9db1-1b995654c864
3 Strict-Transport-Security: max-age=31536000;
  includeSubDomains: preload
4 x-content-type-options: nosniff
5 Content-Type: text/plain; charset=utf-8
6 Date: Mon, 28 Apr 2025 11:44:42 GMT
7 Keep-Alive: timeout=60
8 Connection: keep-alive
9 Server: ---
10
11
```

Inspector: Request attributes (2), Request cookies (2), Request headers (15), Response headers (8).

Event log (41) All issues (141) Memory: 348.9MB

- 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.