INFORME DE EVALUACIÓN DE SEGURIDAD

Banco Del Sol

Documento: corporate

Fecha: 2025-10-21

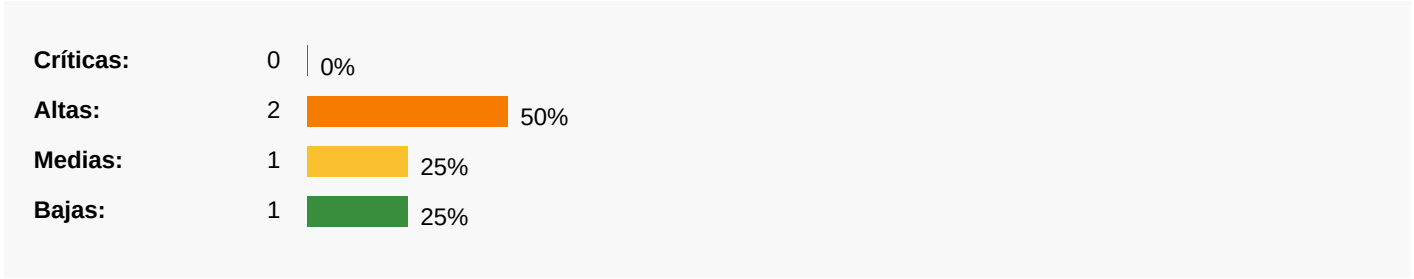
Estado: Finalizado

1. RESUMEN EJECUTIVO

Durante la evaluación de seguridad realizada a **Banco Del Sol**, se identificaron **4 vulnerabilidades**.

? ATENCIÓN PRIORITARIA: Se detectaron 0 críticas y 2 altas.

Distribución de Vulnerabilidades



Nivel	Cantidad	%	Impacto
Crítico	0	0%	Muy Alto
Alto	2	50%	Alto
Medio	1	25%	Moderado
Bajo	1	25%	Bajo

2. ALCANCE DE LA EVALUACIÓN

La evaluación se realizó sobre los siguientes sistemas:

ID	Sistema / URL
1	https://corporate-portal-uat.bdsdigital.com.ar/

3. VULNERABILIDADES IDENTIFICADAS

https://corporate-portal-uat.bdsdigital.com.ar/

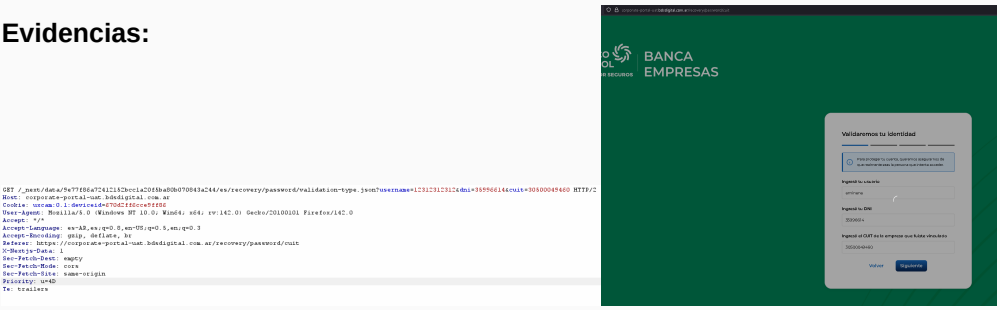
Exposición de datos sensibles en query string (GET)

ALTO

Descripción:

En la petición observada la API recibe identificadores personales en la URL: username=12312312312, dni=35996614, cuit=30500049460. Esos valores viajan en la query string de un GET.

Evidencias:



Solución:

Usar POST y enviar datos en el cuerpo JSON sobre TLS.

Falta de limitación de peticiones (rate limiting) y controles de uso en endpoints de recuperación

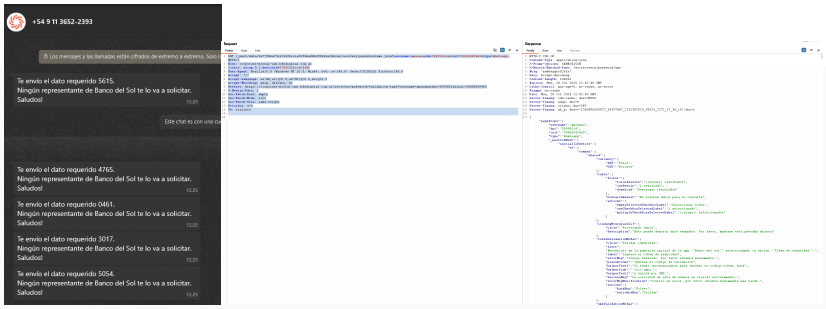
ALTO

Descripción:

El endpoint de recuperación (/…/recovery/password/sms.json whatsapp.json) acepta solicitudes repetidas sin límite ni freno. Puedes lanzar la misma petición en cualquier momento y tantas veces como se quiera.

Esto permite abuso sencillo: fuerza bruta, enumeración de usuarios, automatización de ataques lógicos, agotamiento de recursos.

Evidencias:



Solución:

Implementar límites por cliente, IP y por cuenta (rate limiting) y responder con 429 Too Many Requests cuando se exceda.
Añadir CAPTCHA
Forzar uso de métodos seguros:como post
Implementar tokens de un solo uso

Exposición de lógica y metadatos de la aplicación en respuesta JSON

MEDIO

Descripción:

En el JSON de respuesta, la API devuelve "pageProps" con datos de flujo de UI y campos de validación. En esta captura, no se vio ninguna Sensitive New PII pero sí, la estructura de lógica de la aplicación está filtrada, como nombres de campo, tipos de validación, texto de error, flujo de validación. Esta información facilita a los atacantes conocer los endpoint y construir ataques específicos.

Solución:

Minimizar datos devueltos por endpoints públicos. Devolver solo lo estrictamente necesario para la vista.

Eliminar cadenas de UI y textos de validación de respuestas API públicas. Mover textos a recursos cliente o a endpoints internos autenticados.

Restringir este endpoint a contextos autenticados o a sesiones temporales. Añadir controles de rate-limit y detección de enumeración.

Falta o configuración insuficiente de cabeceras HTTP de seguridad y política CSP

BAJO

Descripción:

La aplicación no envía o tiene mal configuradas las cabeceras HTTP de seguridad ni una política de Content Security Policy (CSP) adecuada. Esto debilita la defensa contra ataques como XSS, clickjacking, fuga de referer, inyecciones de contenido y caching inseguro.

Solución:

implementar los siguientes headers o politicas CSP:

content-security-policy
x-content-type-options
referrer-policy

4. CONCLUSIONES

Este informe muestra las principales áreas de mejora en seguridad del portal de Vendedores. Recomendamos realizar las correcciones detalladas y repetir evaluaciones periódicas para garantizar la protección continua.