🛡️ Reporte Técnico para SOC – Riesgos Detectados en Infraestructura Wicred

- Fecha: 30/10/2025
- Responsable: Alejandro Leone
- Proyecto: Wicred – Legacy

1. Exposición de Scripts sin Autenticación

Descripción: Se detectó que los scripts están accesibles públicamente tanto en servidores internos (VPN) como externos (sitio público).

Ejemplos:

- https://wicred.com.ar/api/mcript.php
- https://wicred.com.ar/modulos/cuenta_corriente.php

Riesgo: Estos scripts pueden ejecutarse directamente desde la URL sin autenticación, lo que permite potenciales ataques de ejecución remota, acceso no autorizado o manipulación de datos.

2. Acceso a Base de Datos sin Autenticación Interna

Descripción: El servidor de base de datos de producción (`192.168.44.12`) permite conexión sin contraseña si se accede desde el mismo servidor.

Comando utilizado:

```
mysql -u remotoBD -p bd_datos
```

Riesgo: Cualquier usuario con acceso SSH al servidor puede acceder a la base de datos sin credenciales individuales. Además, todos los desarrolladores usan las mismas credenciales que la aplicación, lo que impide trazabilidad y control de accesos.

3. Exposición de Credenciales y Datos Sensibles

Descripción: El archivo `api/conn.php` en el servidor `192.168.44.51` está accesible vía URL y contiene credenciales en texto plano.

Contenido expuesto (ejemplo para el reporte):

```php
<?php
$access_token = "ejemplo-para-reporte";
$db_host = "192.168.44.12";
$db_user = "remotoBD";
$db_pass = "secret-para-reporte";
$db_name = "bd_datos";

$conn = mysqli_connect($db_host, $db_user, $db_pass, $db_name);

if (mysqli_connect_errno()) {
    echo 'Error, no se pudo conectar a la base de datos: ' . mysqli_connect_error();
}
```

Riesgo: Si ocurre un error de conexión, se imprime directamente el mensaje de error con detalles técnicos, lo que puede revelar información sensible del entorno y facilitar ataques dirigidos.