

```
$ scan --target random-website.com
```

# Encontré tus datos en 5 minutos.

No soy hacker. Solo sé googlear.

@victorgalloo



context



# La apunté a un sitio random.

OpenClaw es un escaner web gratis y open source. Cualquiera lo puede usar. Lo que encontré:

```
● ● ●  
$ found: nombres completos  
$ found: correos  
$ found: teléfonos  
$ found: historial de compras  
// todo sin contraseña
```

STATUS: EXPOSED



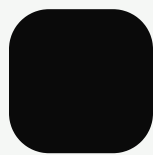
**barreras**

`login` — no había

`auth` — no existía

`firewall` — nada

cualquiera con wifi podía ver todo



**Esa empresa tiene clientes reales.  
Con datos reales.  
Datos como los tuyos.**

Y ni ellos sabían que estaban expuestos.

let that sink in

# Te lo explico sin choro:



## API sin auth

Tu casa sin llave. Entra quien quiera.



## HTTPS ≠ seguridad

El candadito protege el camino, no tu info.



## Token filtrado

Tu llave digital. Se filtra y ya eres otro.

# Haz esto hoy. **Neta.**

1

## Activa doble factor de autenticación

En todo. No mañana. Hoy.

2

## Deja de reciclar contraseñas

Una diferente para cada cuenta.

3

## Usa un password manager

Bitwarden es gratis y funciona.

4

## Revisa permisos de tus apps

Checa qué tiene acceso a tus cuentas.

5

## Googlea "OWASP Top 10"

Si tienes negocio digital, es básico.

No es paranoia. Es no ser negligente.

# Tus datos son **tu pedo.**

Las empresas la van a cagar. Los sistemas se van a romper. Lo único que controlas es no poner las cosas fácil.

GRATIS

Te reviso tu sitio → DM

Sin costo. Sin compromiso. Puro valor.

---

**@victorgalloo**