> diagnostico --whitebox --solo-lectura_

VSSN CYBER

DIAGNÓSTICO · LANDING VISSIONARIES V2

Objetivo landing estática de VISSION (sitio propio)
Fecha 03-11-2026 · **Método** white-box manual · 9 pasos · sin ejecutar su código · sin red
Naturaleza muestra sobre un sitio propio de VISSION, no el trabajo de un cliente

[VER HALLAZGOS]_

01 RESUMEN

SIN CRÍTICOS. UN MEDIO.

0	1	4	2
CRÍTICOS · ALTOS	MEDIO	BAJOS	INFORMATIVOS

Ningún secreto, ninguna URL externa, ningún sumidero XSS alcanzable. Lo más importante es de disponibilidad: **sin JavaScript, casi toda la página queda invisible.**

02 HALLAZGOS

CADA UNO, CON ARCHIVO Y LÍNEA.

#	SEV.	CONF.	DÓNDE	HALLAZGO
01	MEDIO	Alta	generador de la página :236, :337-338 landing.html:120	**Contenido invisible sin JS.** `.rv{opacity:0}` oculta cada bloque y solo un `IntersectionObserver` lo muestra. Sin JS, con scripts bloqueados o en previsualizadores, todo lo que está bajo el hero queda oculto, consola y CTA de cierre incluidos. Solo `prefers-reduced-motion` lo evita (:242). Sin `<noscript>`. El comentario de :262 («sin JS = se lee todo») es falso por esto.
02	BAJO	Alta	generador de la página :132	**Sin CSP, sin referrer, sin noindex** en una pieza aún sin publicar. No carga nada externo (0 URLs), así que una CSP estricta es viable: `default-src 'none'`, hashes para el `<style>` y el `<script>` en línea, `img-src 'self' data:`. Mejor como cabecera HTTP que como `<meta>`.
03	BAJO	Alta	4 scripts de captura (líneas 1-8)	**Ruta absoluta del equipo** `<RUTA LOCAL REDACTADA>` en 4 scripts: revela el usuario de Windows y no es portable. Cargan `playwright-core` con dependencias tomadas de **otro proyecto del equipo**, con la versión sin fijar. Uno de esos scripts escribe fuera de su carpeta de trabajo. Sin secretos.
04	BAJO	Alta	carpeta completa	**Sin control de versiones.** El generador de la página, la fuente de verdad, no tiene commit (`git status: ?? ./`). La carpeta de capturas guarda copias idénticas byte a byte de `landing.html`, `flyer_4x5.html`, `fonts.css` y el PNG (mismo sha256): riesgo de deriva.

#	SEV.	CONF.	DÓNDE	HALLAZGO
05	BAJO	Alta	`assets/vission-chrome-drip_alpha.png` `assets/…` (copia)	**Activo muerto de 1,87 MB ×2.** 0 referencias en `landing.html` y flyers. Es un logo que se retiró del diseño; si se publica la carpeta tal cual, se sirve igual.
06	INFO	Media	generador de la página `:132, :263, :343`	**Inyección de plantillas: hoy no explotable.** Todo el contenido de los f-strings es constante propia. Pero `doc(titulo)` no escapa y `term_html()` escapa solo `<`. Como el producto promete «una versión por negocio», al entrar un nombre de cliente hay que pasar por `html.escape`. En el JS, `innerHTML=''` solo vacía; el texto entra por `textContent`.
07	INFO	Alta	`assets/fonts.css` generador de la página `:11-14`	**Fuentes locales, sin CDN** (privacidad y SRI: sin riesgo). Bebas y JetBrains en base64 dentro de `fonts.css` (53 KB, repetido en cada HTML); Fraunces 500/600 en `woff2` relativo. Falta el archivo de licencia OFL junto a las fuentes.

03 LOS 9 PASOS

LO QUE SE MIRÓ Y NO DIO NADA.

```
vssn@cyber: ~/landing

[ OK ] 01 puerta legal ..... sha256 fijados (código propio)
[ OK ] 02 inventario ..... 4 HTML · 1 .py · 4 .js · 4 PNG salida
[ OK ] 03 secretos ..... 0 coincidencias reales
[ -- ] 03 historia git ..... NO APLICA (sin versionar)
[ OK ] 04 dependencias ..... sin lockfile · .py solo stdlib
[ OK ] 05 sumideros ..... eval/write/Function: 0
[ -- ] 06 auth ..... NO APLICA (página estática)
[ !! ] 07 despliegue ..... sin cabeceras (hallazgo 02)
[ OK ] 08 logs con datos ..... solo medidas de captura
[ OK ] 09 2.ª revisión ..... hecha 03-11-2026 (segundo auditor independiente); esta copia es su corrección
```

Coherencia del contenido: 32/118, 14/24, NO PROBADO y SIN DATO coinciden con los documentos de trabajo internos. No las recalculé: la batería no se corrió aquí.

04 LÍMITES

LO QUE ESTO NO PROMETE.

× No prueba explotabilidad de nada.

× No ejecutó ni renderizó el código del objetivo: el desborde a 390 px y la carga real de fuentes quedan **SIN MEDIR**.

× Que el generador de la página reproduzca el `landing.html` actual es **SIN PROBAR** (semillas fijas, pero no se regeneró).

× Falsos positivos en tráfico real: **SIN DATO**.

SHA · `landing.html 17323971…cd1` · generador `68d9dbcd…966`