EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://bh-onboarding.bancohipotecario.com.sv/portal/	Checks	9 pruebas
Dominio	bh-onboarding.bancohipotecario.com.sv	Hallazgos	47 totales
Fecha	12 de junio de 2026 a las 20:48	Problemas	8 detectados

B

79/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio bh-onboarding.bancohipotecario.com.sv/portal/ arroja una puntuación de 79/100, lo que equivale a una nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, uno generó una advertencia y dos fallaron debido a configuraciones ausentes. Aunque la comunicación cifrada y el manejo de cookies son excelentes, la falta de cabeceras de seguridad críticas y la exposición de puertos alternativos representan un riesgo. En su estado actual, el sitio se considera moderadamente seguro, pero presenta vulnerabilidades configurativas que podrían ser explotadas en ataques dirigidos al cliente.

Resumen de Riesgos

0	1	4	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 32 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	1 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 32 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  32 dias restantes (expira: 2026-07-15T05:28:36.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-16T04:28:38.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: ALLOWALL
- INFO **Strict-Transport-Security**
  Presente: max-age=15724800; includeSubDomains
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 308 redirige a https://bh-onboarding.bancohipotecario.com.sv:443
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15724800; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15724800 (182 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 404

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
  SameSite=none

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- INFO **Puerto 22 (SSH)**
  Cerrado — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- INFO **Puerto 3306 (MySQL)**
  Cerrado — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso por parte de terceros.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador puede intentar adivinar el tipo de contenido, lo que permite ataques de MIME-type sniffing.
[MEDIUM] Referrer-Policy: La falta de esta política puede causar que se filtre información sensible en la URL a través de la cabecera Referer al navegar hacia otros sitios.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones del navegador como la cámara o el micrófono, aumentando la superficie de ataque potencial.
[MEDIUM] Puerto 8080 (HTTP-Alt) ABIERTO: La exposición de un servidor web alternativo o proxy puede ser utilizada para evadir controles o explotar servicios no parcheados.
[LOW] Server header expuesto: Se revela el uso de Cloudflare, lo cual entrega información técnica a un atacante para perfilar la infraestructura de red.
[LOW] Ausencia de archivos robots.txt y sitemap.xml: El servidor responde con errores 404 para estos archivos, dificultando la indexación controlada y el rastreo estructurado.