EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.baccredomatic.com/sites/default/files/2026-05/F_HON_0000394_41_F_HON_SOLICITUD_DE_PRODUCTOS_VISTA_PERSONAL_HON_0000394_Version_no.41_2.pdf?bacid=HONG-EMPR--000003-BO-AW-CD-00-000-00-00000/	Checks	9 pruebas
Dominio	www.baccredomatic.com	Hallazgos	35 totales
Fecha	22 de mayo de 2026 a las 17:12	Problemas	7 detectados

B

78/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el activo digital evaluado arroja una puntuación de 78/100, lo que equivale a una nota B. Durante la auditoría se ejecutaron un total de 9 checks pasivos, obteniendo 5 resultados satisfactorios, 0 advertencias y 1 fallo crítico relacionado con la configuración de seguridad. Cabe destacar que no se realizó un pentest activo, por lo que los resultados se limitan a la superficie de exposición pública inmediata. Debido a la ausencia de múltiples cabeceras de seguridad fundamentales, el sitio se clasifica actualmente como vulnerable ante ataques de inyección y manipulación de interfaz.

Resumen de Riesgos

0	2	2	3	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Deteccion CMS	100	OK	No se detecto un CMS conocido
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

Cabeceras de Seguridad — 35/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: nginx — Revela tecnologia del servidor
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000 ; includeSubDomains ; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

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

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (844 bytes)
- INFO **Reglas robots.txt**
  14 Disallow, 4 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "backup" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.baccredomatic.com/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — 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 la ejecución de ataques XSS y la inyección de contenido malicioso por parte de terceros.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a ataques de clickjacking, permitiendo que atacantes carguen la página en marcos invisibles para engañar al usuario.
[MEDIUM] Referrer-Policy: No se detectó esta cabecera, lo que impide controlar qué información de navegación se envía a otros sitios web al seguir enlaces.
[MEDIUM] Permissions-Policy: La falta de esta configuración no restringe el acceso del navegador a APIs sensibles como la cámara o el micrófono, aumentando la superficie de riesgo.
[LOW] Server header expuesto: El servidor revela el uso de nginx, proporcionando información técnica valiosa que un atacante podría usar para buscar vulnerabilidades específicas del software.
[LOW] Ruta sensible en robots.txt: Se identificó una referencia a la ruta admin, lo cual puede guiar a atacantes hacia paneles de administración.
[LOW] Ruta sensible en robots.txt: El archivo robots.txt menciona una ruta de backup, exponiendo posibles puntos de fuga de información o respaldos desprotegidos.