EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://selecta.com.py	Checks	9 pruebas
Dominio	selecta.com.py	Hallazgos	49 totales
Fecha	25 de mayo de 2026 a las 20:06	Problemas	12 detectados

B

82/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio selecta.com.py ha arrojado una puntuación de 82/100, lo que corresponde a una calificación de grado B. El análisis se basó en la ejecución de 9 checks pasivos, de los cuales 7 resultaron satisfactorios, 1 presentó advertencias y 1 fue calificado como fallo crítico. Si bien el sitio demuestra una implementación sólida en cuanto al cifrado de datos y redirección segura, presenta carencias importantes en las cabeceras de seguridad que protegen al usuario final. Se concluye que el sitio es moderadamente seguro, pero se encuentra en un estado vulnerable ante ataques específicos de inyección y suplantación por falta de políticas de seguridad en el navegador.

Resumen de Riesgos

0	2	8	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 45 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 45 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  45 dias restantes (expira: 2026-07-10T04:37:22.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-11T04:37:23.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.23.3 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Express — Revela framework/lenguaje
- 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
- 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 301 redirige a https://selecta.com.py/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

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
- INFO **Tecnologias detectadas**
  Express

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (67 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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 permite la ejecución de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar presente, el sitio puede ser embebido en marcos de otras webs, lo que expone a los usuarios a ataques de clickjacking.
[MEDIUM] X-Content-Type-Options: La falta de la directiva nosniff permite que el navegador intente interpretar archivos con tipos MIME incorrectos, aumentando el riesgo de ejecución de malware.
[MEDIUM] Referrer-Policy: No se ha definido una política de referencia, lo que puede provocar la filtración de información sensible de las URLs en las peticiones enviadas a terceros.
[MEDIUM] Permissions-Policy: La falta de esta configuración permite que el sitio tenga acceso potencial a APIs sensibles del navegador como la cámara, micrófono o geolocalización sin restricciones explícitas.
[MEDIUM] Archivos informativos expuestos: Se detectó acceso público a /readme.html y /README.txt, los cuales pueden contener información técnica sobre la infraestructura o versiones de software.
[MEDIUM] Rutas administrativas accesibles: Las rutas /wp-login.php, /administrator/ y /user/login son visibles, lo que facilita ataques de fuerza bruta contra paneles de gestión.
[LOW] Server header expuesto: La cabecera revela que el servidor utiliza nginx/1.23.3, proporcionando datos específicos que un atacante puede usar para buscar exploits conocidos.
[LOW] X-Powered-By expuesto: El servidor indica el uso del framework Express, revelando la pila tecnológica y reduciendo el esfuerzo necesario para una fase de reconocimiento.
[LOW] Falta de sitemap.xml: La ausencia de este archivo dificulta la auditoría de rutas indexadas y el rastreo estructurado del sitio.