

Pruebas exploratorias de seguridad (Lend2b.com)

Preparado por:

José Pagola

A petición de:

Juan Carlos Robles.

29 de mayo de 2024 (versión 1)

Tabla de contenidos

Tabla de contenidos	1
Propósito del ejercicio.	2
Pruebas de mail	3
Registros SPF y Dmarc no configurado:	3
Evidencia:	3
Registro DKIM no configurado	3
Evidencia:	4
Control de versiones	5

Propósito del ejercicio.

El objetivo de las pruebas de seguridad en Lend2b.com es asegurar la integridad, confidencialidad y disponibilidad del sitio web y sus datos. Estas pruebas buscan identificar y mitigar vulnerabilidades, proteger contra ataques maliciosos y garantizar que el sistema sea resistente ante intentos de intrusión. Además, tienen como fin preservar la reputación de la plataforma y la confianza de los usuarios, asegurando que sus transacciones y la información personal se manejen de manera segura.

Pruebas de mail

Registros SPF y Dmarc no configurado:

Es crucial implementar y configurar correctamente DMARC y SPF para proteger la comunicación por correo electrónico y mantener la seguridad de la información. La falta de configuración de los registros DMARC y SPF en el correo electrónico puede tener consecuencias significativas:

- Vulnerabilidad al phishing y spam: Sin DMARC y SPF, los correos electrónicos pueden ser fácilmente falsificados, aumentando el riesgo de ataques de phishing y la distribución de spam.
- Problemas de entrega de correo: Los correos electrónicos pueden ser marcados como spam o incluso no entregarse, ya que los servidores receptores no pueden verificar su autenticidad.
- Daño a la reputación: La capacidad de los atacantes para enviar correos que parecen provenir de su dominio puede dañar la reputación de su empresa y la confianza de los clientes.
- Pérdida de información confidencial: Los ataques de phishing exitosos pueden resultar en la pérdida de datos sensibles o credenciales de acceso.

Evidencia:

Problems	Blacklist	Mail Server	Web Server	DNS
3 Errors 3 Warning 123 Passed	0 Errors 0 Warning 93 Passed	3 Errors 2 Warning 7 Passed	0 Errors 0 Warning 8 Passed	0 Errors 1 Warning 15 Passed

6 Problems			
Category	Host	Result	
✖️ dmarc	lend2b.com	No DMARC Record found	More Info
✖️ spf	lend2b.com	No SPF Record found	More Info
✖️ mx	lend2b.com	No DMARC Record found	More Info
⚠️ mx	lend2b.com	DMARC Quarantine/Reject policy not enabled	More Info
⚠️ smtp	smtp.google.com	Reverse DNS does not match SMTP Banner	More Info
⚠️ dns	lend2b.com	SOA Serial Number Format is Invalid	More Info

Registro DKIM no configurado

Configurar DKIM es esencial para proteger la comunicación por correo electrónico y mantener la confianza de los usuarios en la seguridad del dominio. La ausencia de registros DKIM configurados en el correo electrónico puede llevar a varios problemas:

- Falta de autenticación: Los servidores de correo no pueden verificar la autenticidad de los mensajes, lo que facilita la suplantación de identidad.
- Rechazo o marcado como spam: Los correos pueden ser rechazados o marcados como spam por los servidores receptores, afectando la entrega de mensajes legítimos.
- Riesgo de seguridad: Incrementa el riesgo de ataques de phishing y otros tipos de fraude por correo electrónico, ya que los atacantes pueden falsificar el dominio del remitente.
- Riesgo reputacional: La empresa puede sufrir daños en su reputación si se asocia con la distribución de spam o fraudes por correo electrónico.

Evidencia:

	Test	Result	
	DKIM Record Published	No DKIM Record found	 More Info

Control de versiones

Versión	Responsable	Fecha	Detalle
1	José Pagola	29/05/2024	Revisión de cabeceras de correo electrónico.