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

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.

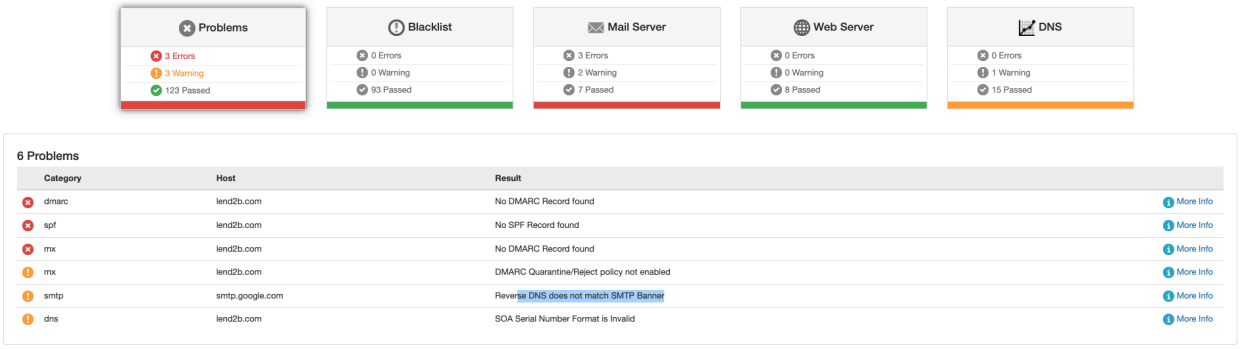
Pruebas de mail

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:



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:

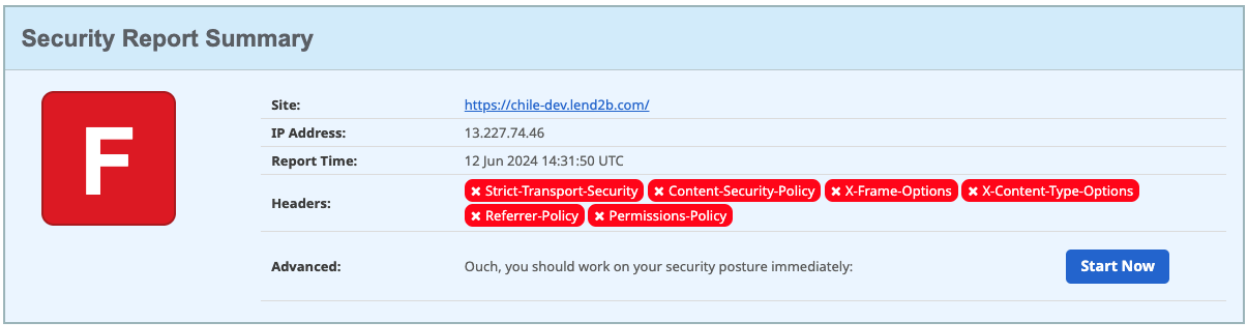
- Falta de autenticación: Los servidores de correo no pueden verificar la autenticidad de los mensajes, lo que facilita la suplantación de identidad.
- Rechazo o marcado como spam: Los correos pueden ser rechazados o marcados como spam por los servidores receptores, afectando la entrega de mensajes legítimos.
- 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

Cabeceras no configuradas.

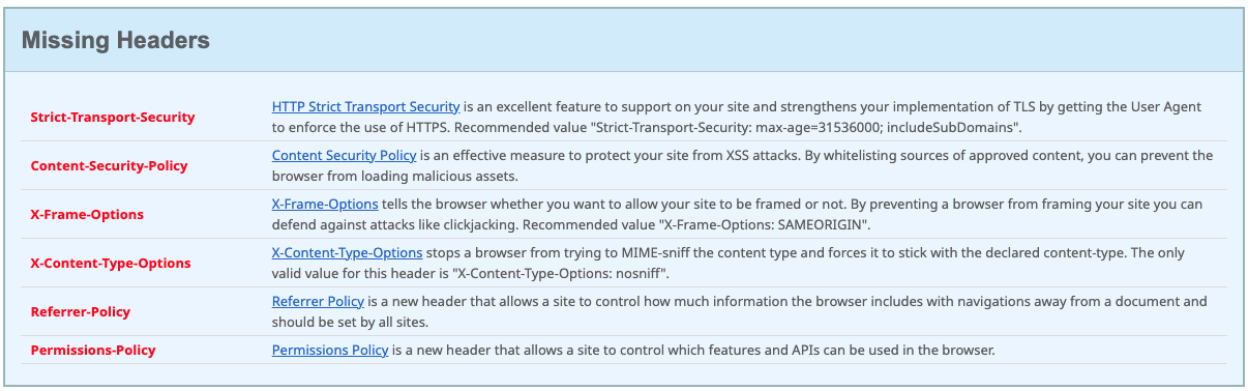
El estado de configuración de cabeceras a nivel de servidor web está mal configurado o no existe. Se debe revisar el estado de las mismas y repetir los test. A continuación se presenta evidencia del hallazgo.



Security Report Summary

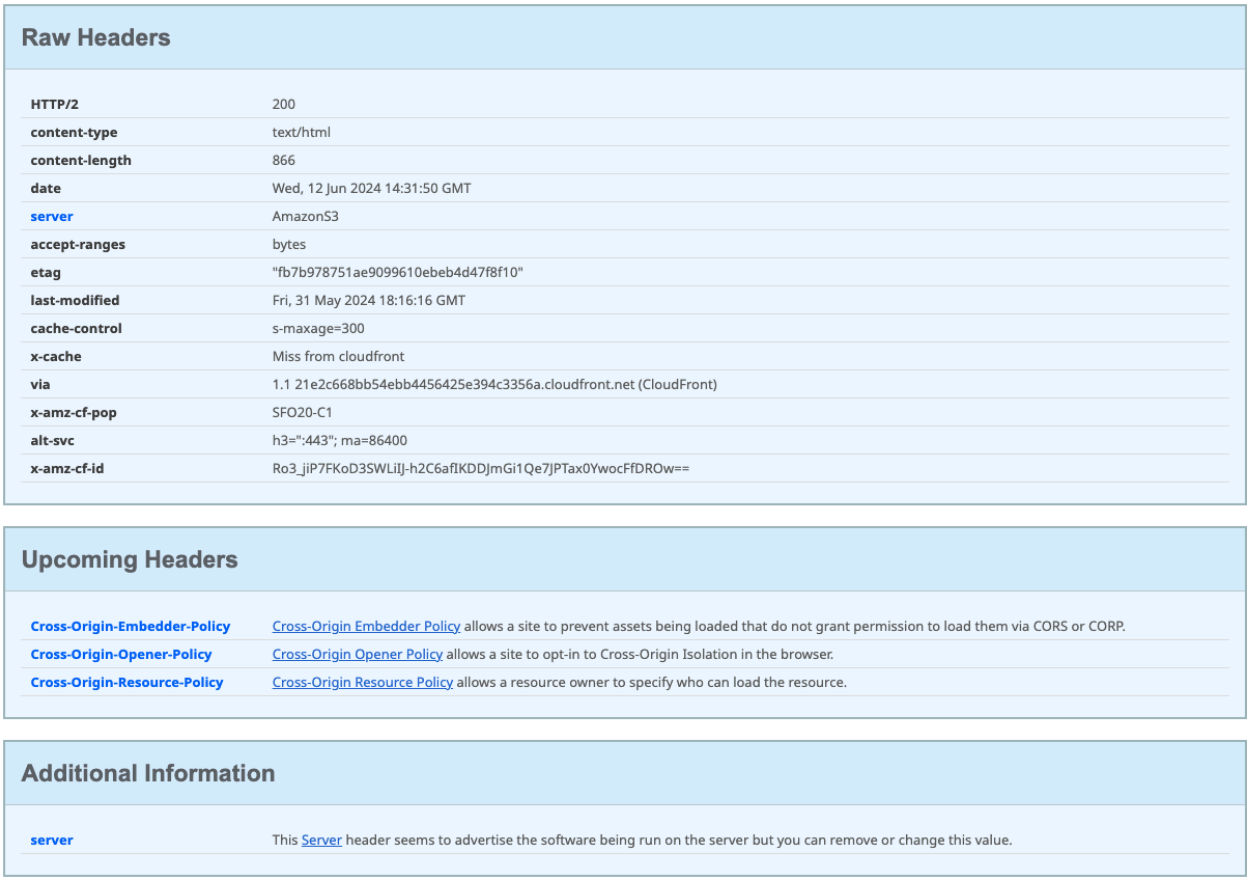
F

Site:	https://chile-dev.lend2b.com/
IP Address:	13.227.74.46
Report Time:	12 Jun 2024 14:31:50 UTC
Headers:	✖ Strict-Transport-Security ✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy
Advanced:	Ouch, you should work on your security posture immediately: Start Now



Missing Headers

Strict-Transport-Security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.



Raw Headers

HTTP/2	200
content-type	text/html
content-length	866
date	Wed, 12 Jun 2024 14:31:50 GMT
server	AmazonS3
accept-ranges	bytes
etag	"fb7b978751ae9099610ebeb4d47f8f10"
last-modified	Fri, 31 May 2024 18:16:16 GMT
cache-control	s-maxage=300
x-cache	Miss from cloudfront
via	1.1 21e2c668bb54ebb4456425e394c3356a.cloudfront.net (CloudFront)
x-amz-cf-pop	SFO20-C1
alt-svc	h3=":443"; ma=86400
x-amz-cf-id	Ro3_jiP7FKoD3SWLiIJ-h2C6afIKDDJmGi1Qe7JPTax0YwocFfDROw==

Upcoming Headers

Cross-Origin-Embedder-Policy	Cross-Origin Embedder Policy allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.
Cross-Origin-Opener-Policy	Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.
Cross-Origin-Resource-Policy	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

Additional Information

server	This Server header seems to advertise the software being run on the server but you can remove or change this value.

Seguridad perimetral:

Se realizaron pruebas de seguridad perimetral usando la herramienta OWASP ZAP y se encontraron vulnerabilidades especificadas en el informe de escaneo de vulnerabilidades.

Los temas más preocupantes están relacionados con cabeceras que se encuentran mal configuradas o no configuradas, esto ya fue parte de un caso anterior.

La siguiente tabla lista los temas más relevantes que no fueron descartados en dicho escaneo.

Tipo de alerta	Riesgo	Cantidad

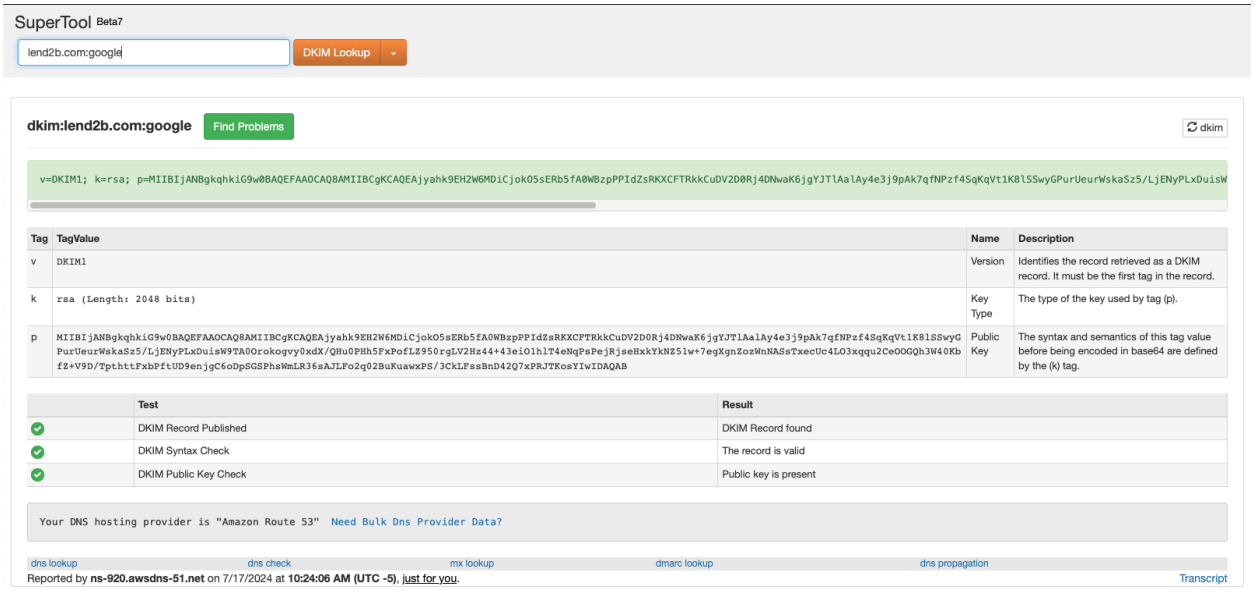
Content Security Policy (CSP) Header no configurado	Medio	4
Cross-Domain Misconfiguration	Medio	1
Missing Anti-clickjacking Header	Medio	2
X-Content-Type-Options Header Missing	Baja	6
.htaccess Information Leak	Informativa	1

Remediaciones

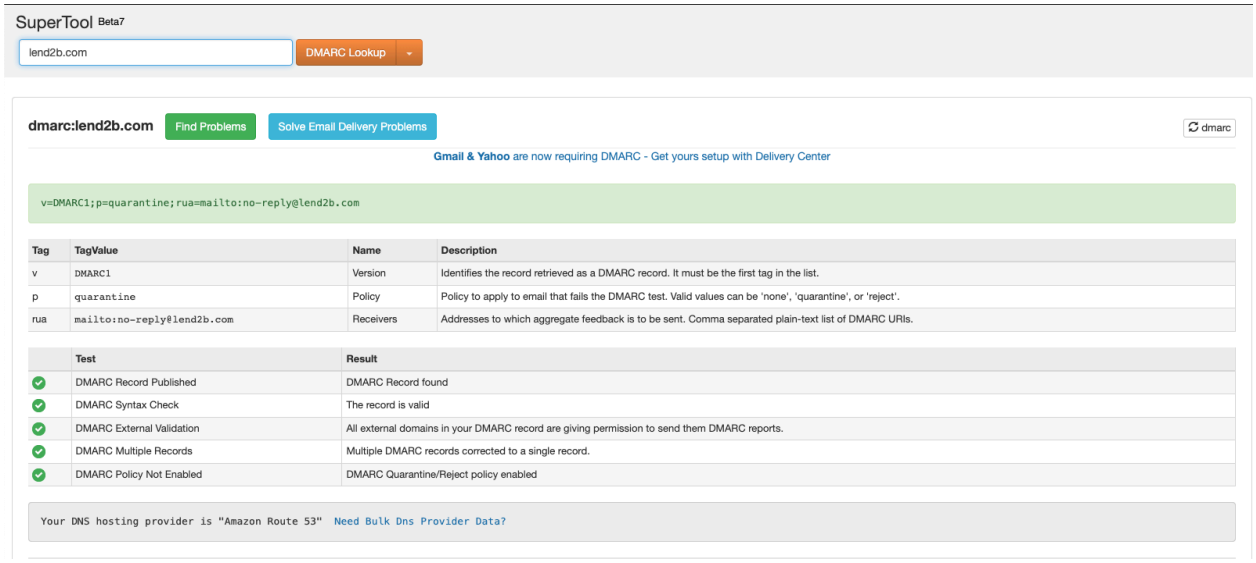
Luego de hacer varias entregas parciales de los hallazgos se hicieron una serie de reuniones y sesiones de seguimiento para la implementación de las remediaciones.

En las siguientes imágenes y comentarios se muestra la evidencia de las remediaciones adoptadas:

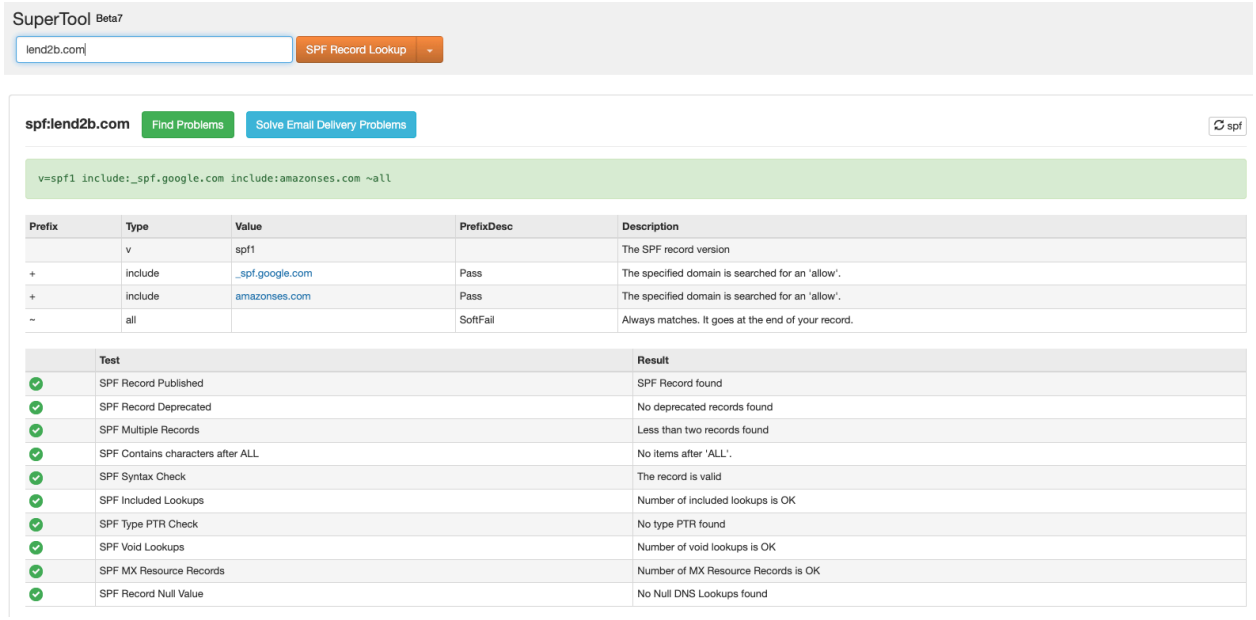
Configuración DKIM para el dominio lend2b.com



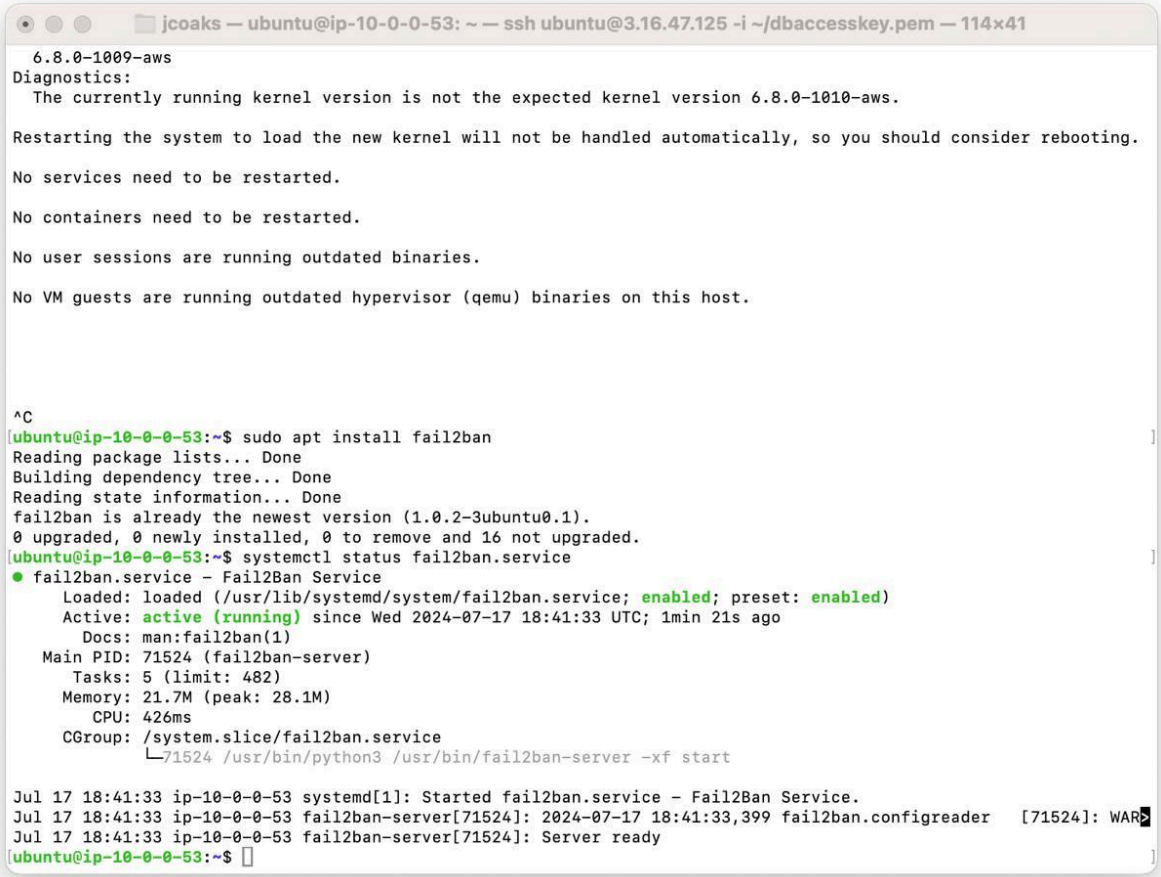
Configuración DMARC para el dominio lend2b.com



Configuración SPF para el dominio lend2b.com



Configuración de fail2ban en servidor bastión para conexión a base de datos.



Configuración de cabeceras

Conclusiones

Al tratarse de la primera aplicación del ejercicio de hacking ético al ambiente seleccionado se pudieron encontrar evidencias de vulnerabilidad. En este sentido se recomienda a Lend2b incluir en el procedimiento de manejo de directivas de seguridad.

También se recomienda verificar todas los orígenes de archivos fuentes que se pudieran incluir en los proyectos asi como las licencias bajo las que operan.

Como nota adicional también se encontraron hallazgos positivos:

- Los certificados TLS/SSL están bien configurados y vigentes.
- El WAF se encuentra bien configurado y las reglas parecen estar a punto.
- No hay evidencia de puertos expuestos de manera innecesaria.
- Existe una delegación de la responsabilidad sobre la seguridad física a AWS.
- La arquitectura serverless hasta cierto punto obliga a seguir lineamientos de seguridad y buenas prácticas.

Dicha información la hemos logrado confirmar en la realización de este ejercicio y el trabajo conjunto que se viene ejecutando con Lend2b en esta primera etapa como parte de su iniciativa de seguridad del software.

Como consecuencia de todo lo expuesto anteriormente y tomando como perspectiva los objetivos y alcance planteado para este ejercicio, se considera que los recursos estudiados durante esta prueba de penetración y análisis de vulnerabilidades de caja negra (Etapa 1) se pueden considerar seguros para los requerimientos expuestos luego de la aplicación de correcciones y el retesteo de dichas vulnerabilidades.

Sin embargo se recomienda a Lend2b hacer una revisión en inclusión en sus procedimientos de una politica que incluya revisiones periodicas escaneos programados por lo menos dos veces al año

Control de versiones

Versión	Responsable	Fecha	Detalle
1	José Pagola	29/05/2024	Revisión de cabeceras de correo electrónico.
2	José Pagola	11/06/2024	Evidencia de cabeceras
3	José Pagola	19/06/2024	Pruebas perimetrales Owasp
4	José Pagola	01/08/2024	Remediaciones