Universidad Autónoma De Chiapas

Análisis de Vulnerabilidades

- **Alumnos:**
  - Tomás Álvarez Gómez A200369
  - Luis Gerardo Mendoza Gomez A200004
  - Néstor Horacio Zea Hernández A200727
  - José Ricardo Domínguez Calderón A200882

- **Actividad:** Aprendizaje 4.1

- **Tarea:** Documentación de pruebas de ataque y instalación de seguridad a la página web

- **Maestro:** Luis Gutiérrez Alfaro

- **Grupo:** 7 M

- **Fecha:** Tuxtla Gutiérrez a 13/11/23

- **Matricula:** A200369

INFORME DE EL PROYECTO DE LA PAGINA WEB CON TODOS LOS MECANISMO DE SEGURIDAD

INTRODUCCIÓN

El presente informe presenta un análisis detallado del desarrollo, implementación y seguridad de la nueva página web creada para Clínica Rojas. Este proyecto, concebido con el objetivo de fortalecer la presencia en línea de la clínica y mejorar la accesibilidad de la información para pacientes y personal, ha sido ejecutado con especial atención a los estándares de seguridad más rigurosos.

La primera sección del informe abordará el proceso de desarrollo, destacando las decisiones de diseño, la estructura de la página y la implementación de características específicas para optimizar la experiencia del usuario. Posteriormente, nos sumergiremos en el proceso de subida y alojamiento en un servidor, detallando la selección del proveedor de hosting y las consideraciones técnicas asociadas.

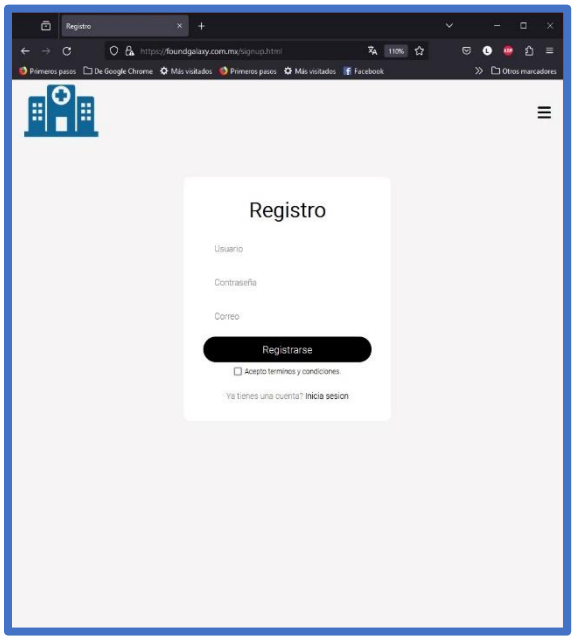
Un componente crítico de este informe se centrará en las medidas de seguridad implementadas para resguardar la integridad de la página web y la confidencialidad de los datos del paciente. Se discutirán en detalle los protocolos de cifrado, la configuración del cortafuegos, las actualizaciones regulares de software y cualquier medida adicional adoptada para prevenir posibles vulnerabilidades.

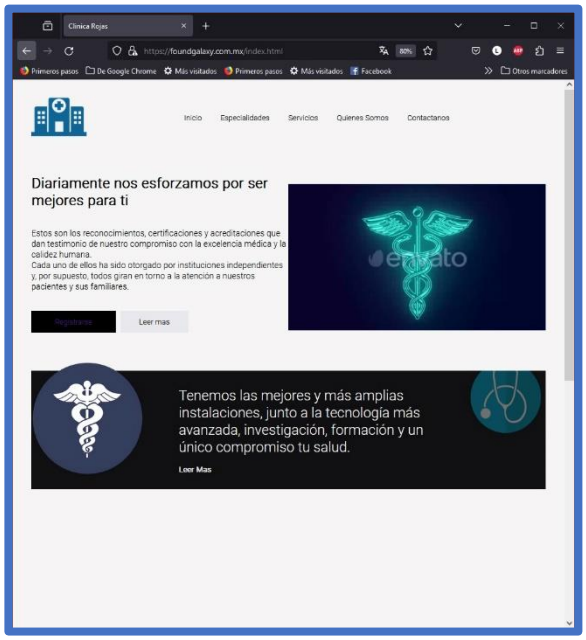
La seguridad de la información, especialmente la referente a los pacientes, es una prioridad fundamental en este proyecto. La implementación de un certificado SSL, medidas de autenticación robustas y el establecimiento de prácticas de respaldo regulares son aspectos clave que serán examinados exhaustivamente.

Este informe busca proporcionar una visión holística del proceso de desarrollo y seguridad de la página web de [nombre de la clínica], destacando los esfuerzos dedicados a garantizar que la plataforma no solo cumple con los estándares tecnológicos actuales, sino que también responde a las necesidades críticas de protección de datos en el ámbito de la atención médica.

Interfaz gráfica de la app

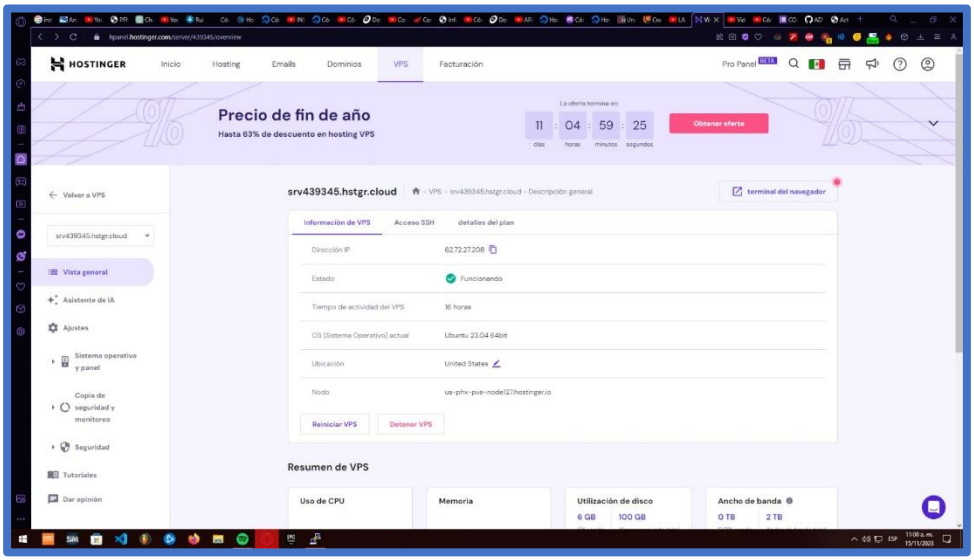
La interfaz de la página web de Clínica Rojas destaca por su diseño moderno y limpio. La disposición cuidadosa de elementos visuales y la paleta de colores elegante crean una experiencia visualmente atractiva. La funcionalidad intuitiva permite a los visitantes encontrar rápidamente la información que buscan, ya sea sobre servicios médicos, horarios de atención o detalles de contacto.

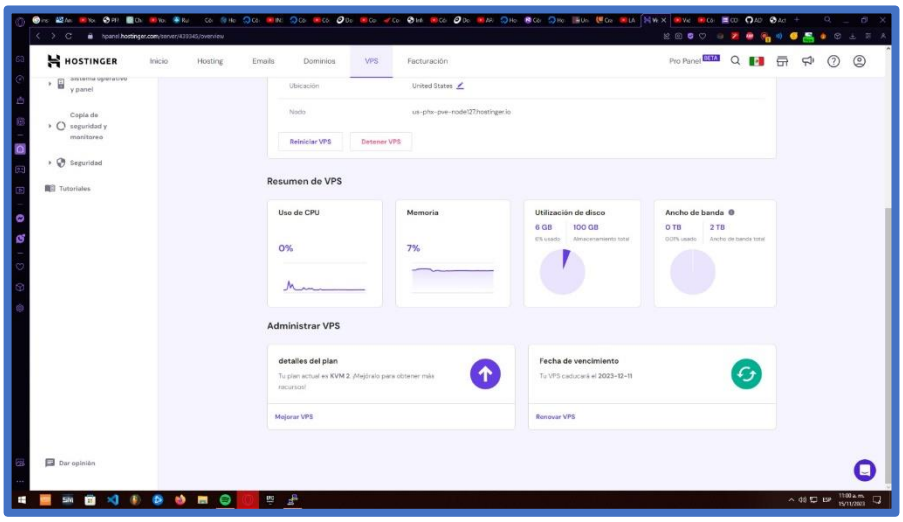




"¡Emocionados de compartir nuestra primer página web! Después de un arduo trabajo de desarrollo, hemos logrado subirla con éxito a un hosting de primera categoría.

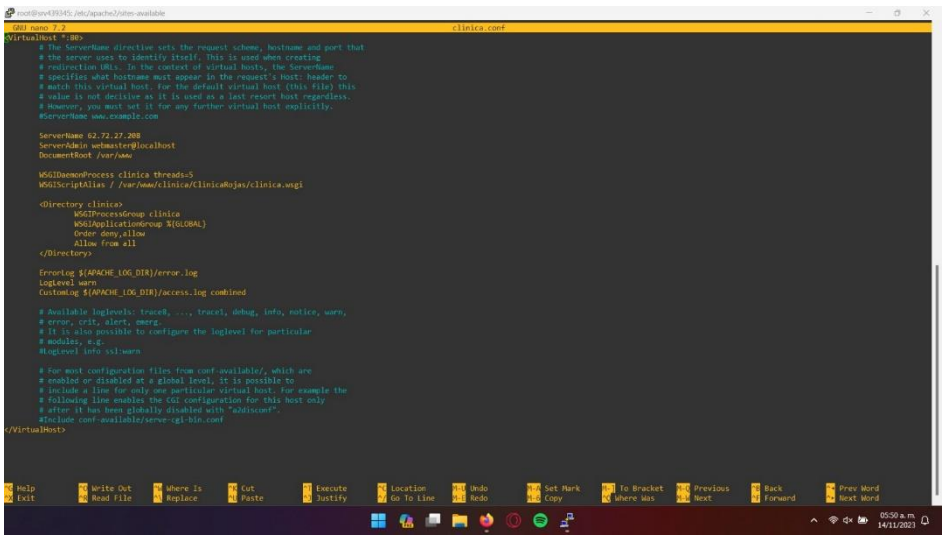
Para respaldar este logro, compartimos con entusiasmo capturas de pantalla que documentan el proceso



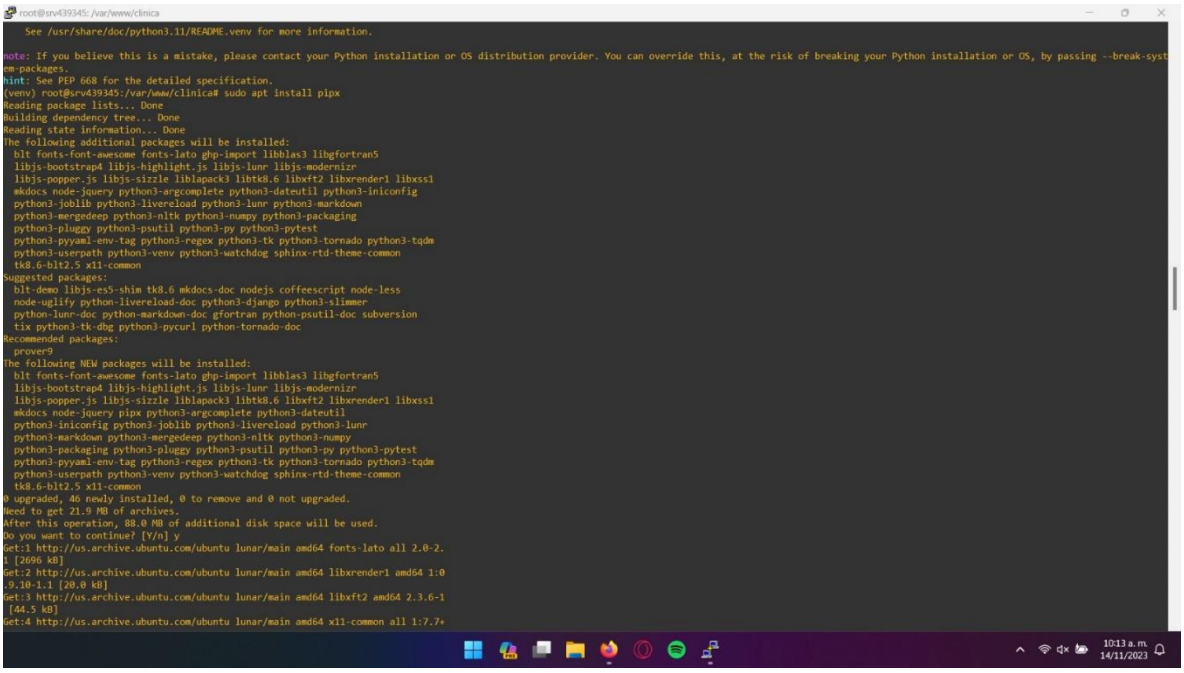


En el último avance técnico, he llevado a cabo la instalación de librerías en mi servidor a través del servicio PuTTY. Este proceso, que implica la conexión remota y la administración del servidor, ha fortalecido las capacidades de mi proyecto al integrar bibliotecas esenciales. Con PuTTY como mi herramienta principal, he ejecutado comandos precisos para descargar, instalar y configurar las librerías necesarias, mejorando así la funcionalidad y la eficiencia de mi aplicación. Este hito marca un paso crucial en la evolución de mi proyecto, respaldando su desarrollo con las últimas herramientas y recursos disponibles."

Se configura el virtual host

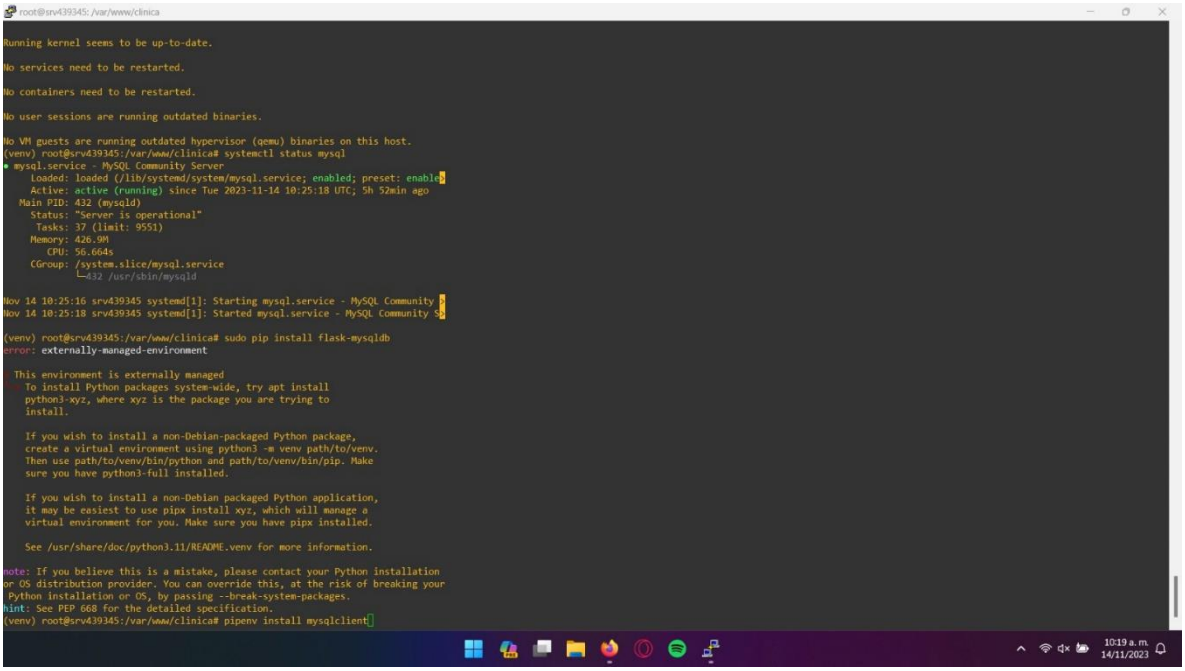


Se instalado pipx



Se instalo las librerías de MySQL para que la app funcionara, asi como también flask

Y otras librerías que nos ayudaron a que la pagina corriera sin problemas



SEGUIRIDAD INSTALADA AL SISTEMA

En la constante búsqueda de robustecer la seguridad de nuestro entorno digital, nos complace presentar las implementaciones clave que fortalecen la integridad y protección de nuestro sistema. Hemos adoptado un enfoque proactivo al instalar medidas de seguridad avanzadas, destacando la incorporación de Mod-Security, Mod-Evasive y un Firewall de Aplicaciones Web (WAF) Qo.

Mod-Security: Defensa Proactiva en Capas

Mod-Security emerge como un escudo proactivo ante amenazas cibernéticas, integrándose directamente en nuestro servidor web para filtrar tráfico malicioso. Este módulo de seguridad de aplicación web proporciona una barrera robusta, utilizando reglas personalizables para detectar y prevenir ataques comunes, brindando una capa adicional de protección a nuestros activos digitales.

Mod-Evasive: Protección Contra Ataques de Denegación de Servicio (DoS) y DDoS

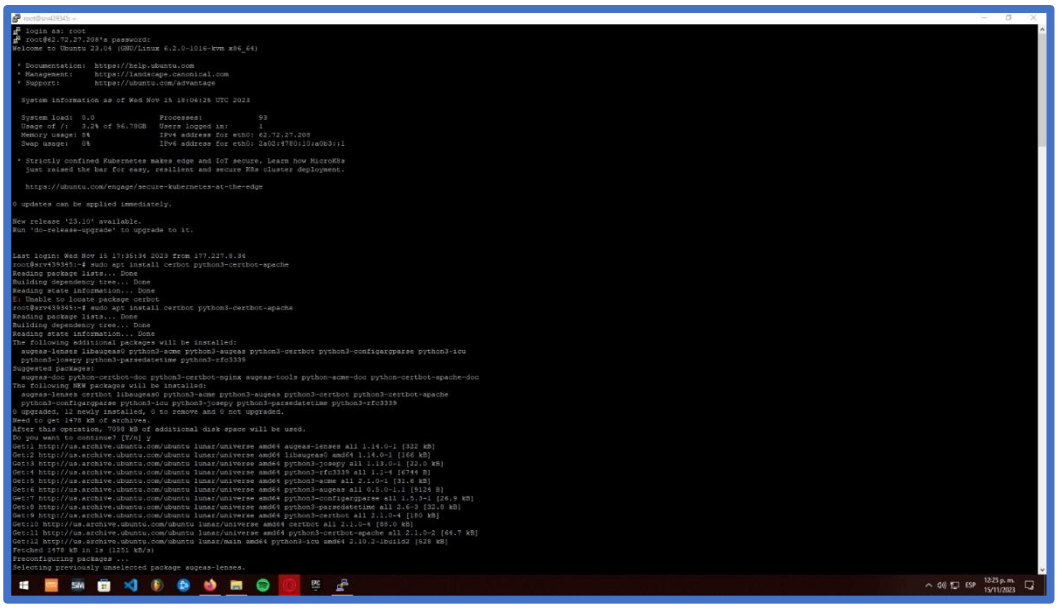
En nuestra búsqueda por garantizar la disponibilidad continua de nuestros servicios, hemos implementado Mod-Evasive para contrarrestar ataques de denegación de servicio y distribuidos. Este módulo detecta patrones de tráfico sospechoso y responde de manera dinámica, mitigando efectivamente posibles intentos de saturar nuestros recursos y asegurando la accesibilidad sin interrupciones.

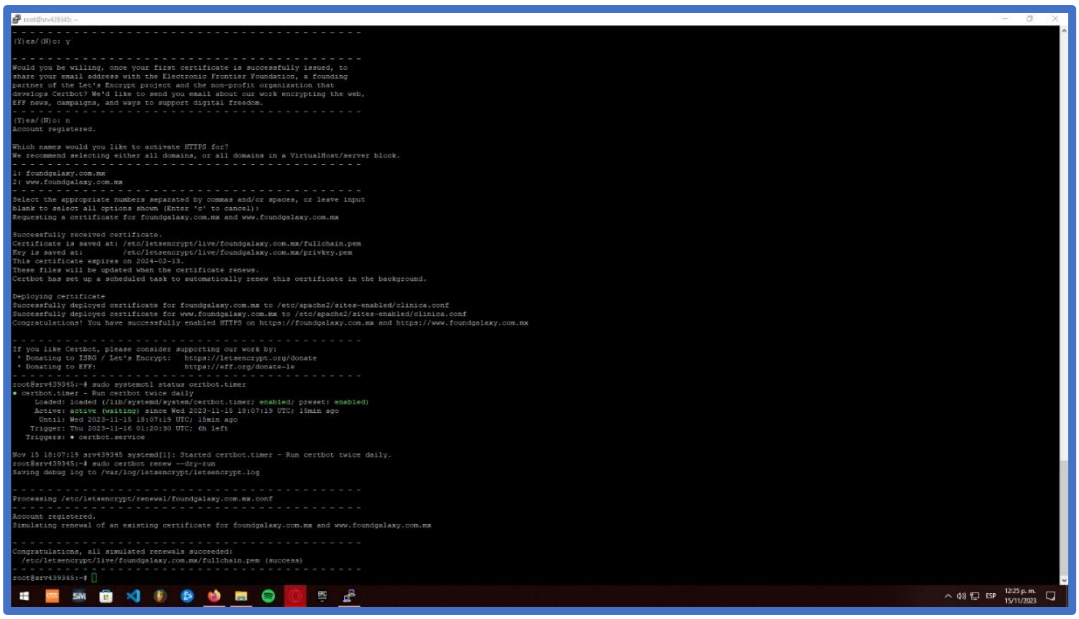
Firewall de Aplicaciones Web (WAF) Qo: Escudo Personalizado para Vulnerabilidades Específicas

El WAF Qo representa una barrera de seguridad altamente especializada, diseñada para proteger nuestra aplicación web contra amenazas específicas y vulnerabilidades conocidas. Con reglas personalizadas y actualizaciones periódicas, este componente se adapta continuamente al panorama de seguridad, garantizando una defensa eficaz contra las últimas amenazas.

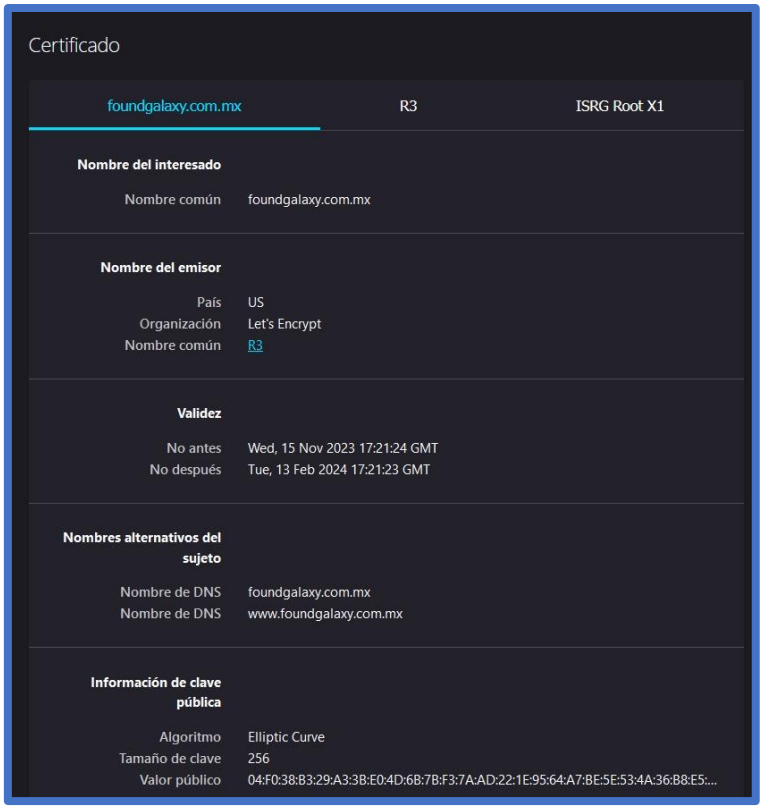
Estas implementaciones conjuntas refuerzan nuestro compromiso con la seguridad, creando un entorno digital resistente y preparado para enfrentar los desafíos del panorama cibernético actual. Al incorporar estas soluciones de vanguardia, reafirmamos nuestro compromiso con la integridad, confidencialidad y disponibilidad de nuestros servicios en línea.

Certificado SSL con cerbot

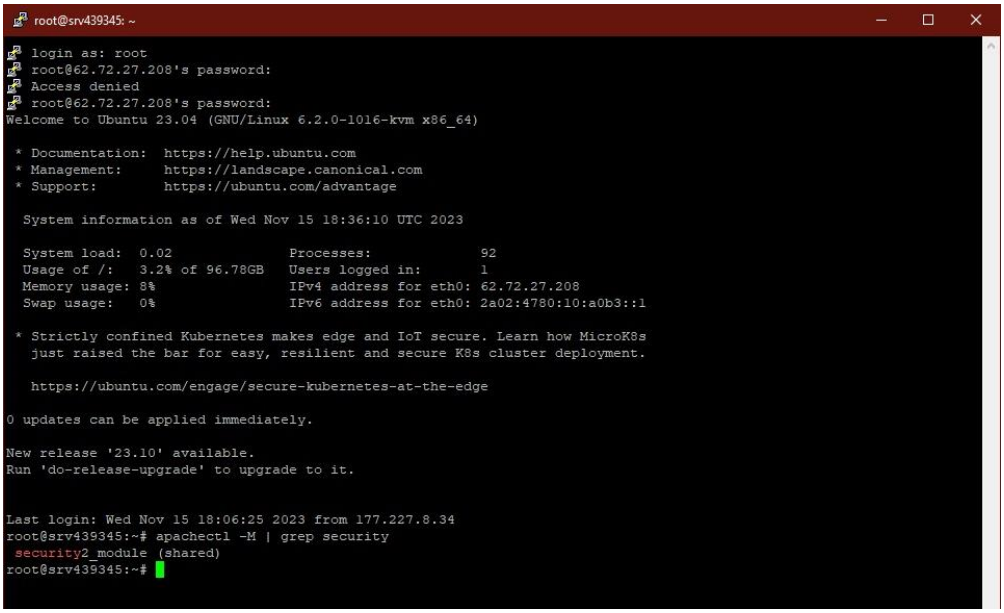




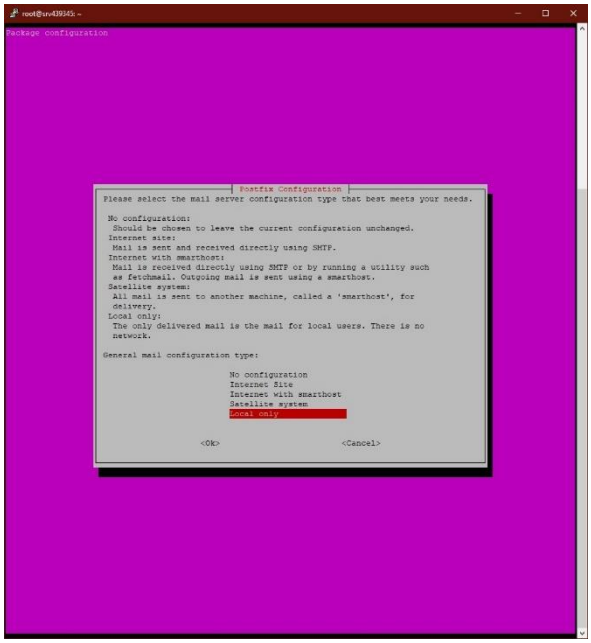
Información del certificado

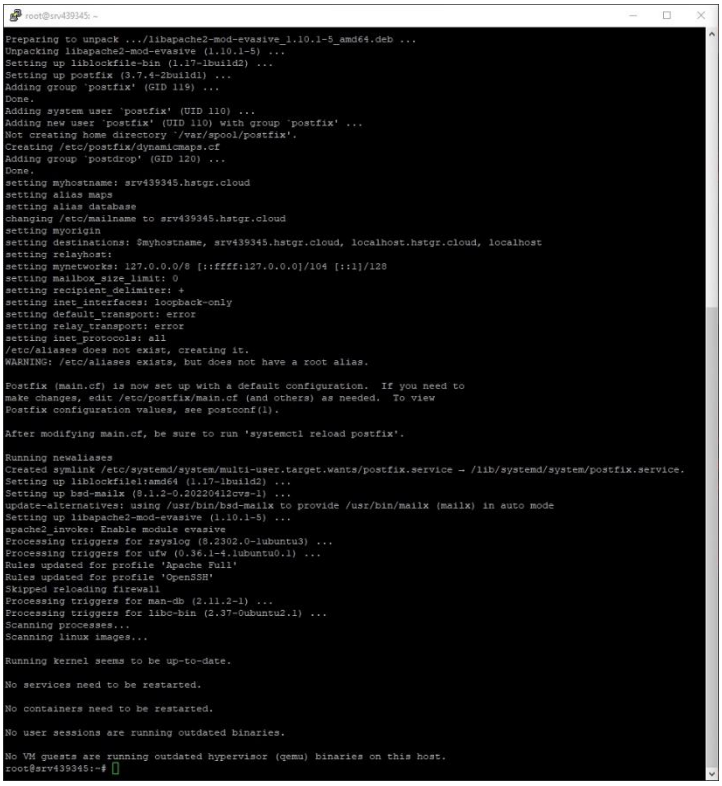


Mod-Security: Defensa Proactiva en Capas-instalado



Mod-Evasive: Protección Contra Ataques de Denegación de Servicio (DoS) y DDoS-instalado



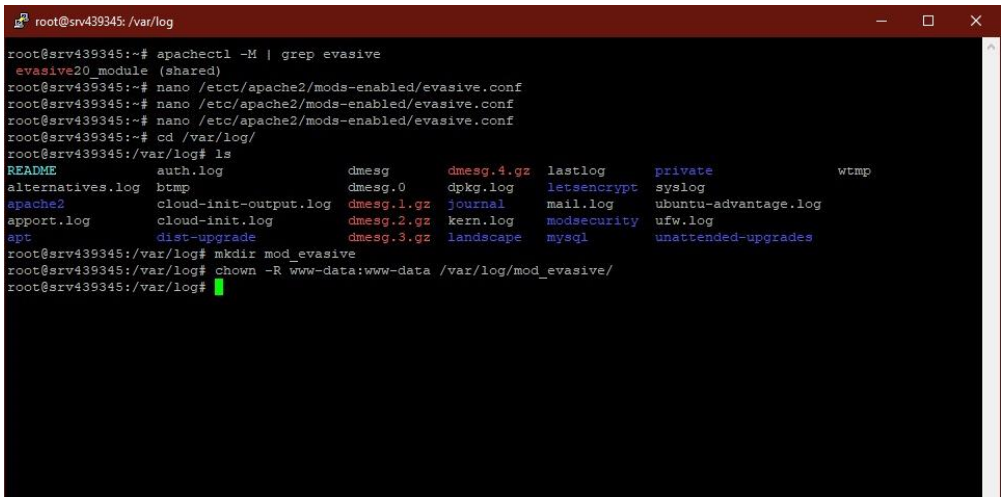


```
root@srv439345: ~
root@srv439345:~# apachectl -M | grep evasive
 evasive20_module (shared)
root@srv439345:~#
```

Configuración de los parámetros de mod evasive

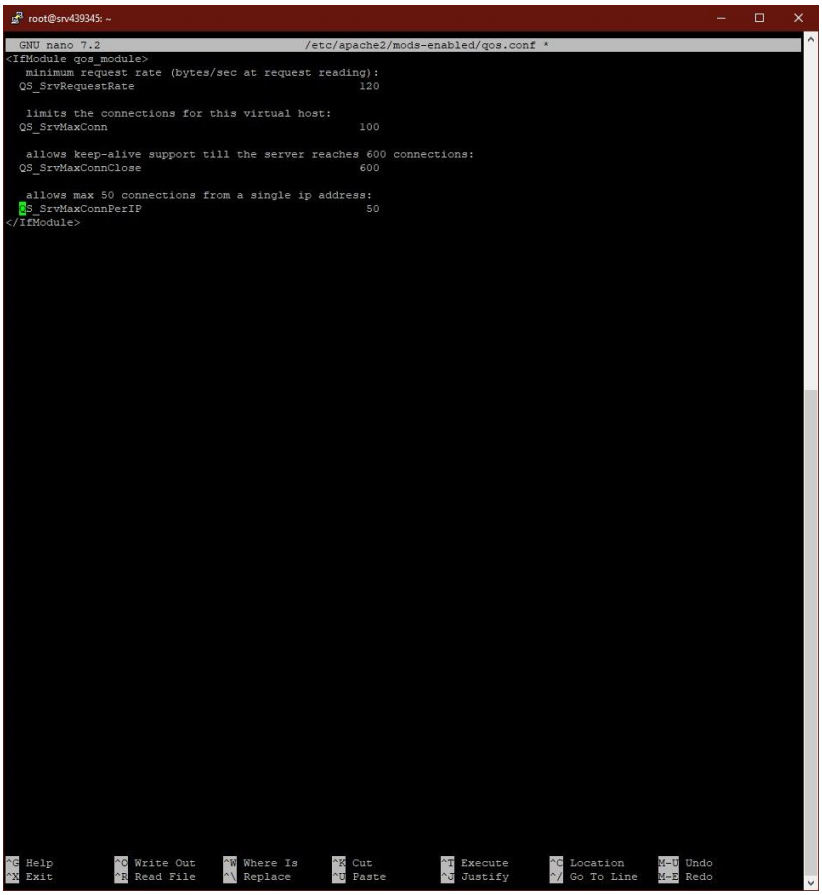
```
root@srv439345: ~
  GNU nano 7.2                          /etc/apache2/mods-enabled/evasive.conf
<IfModule mod_evasive20.c>
    DOSHashTableSize    3097
    DOSPageCount        2
    DOSSiteCount        50
    DOSPageInterval     1
    DOSSiteInterval     1
    DOSBlockingPeriod   10

    DOSEmailNotify      you@yourdomain.com
    DOSSystemCommand    "su - someuser -c '/sbin/... %s ...'"
    DOSLogDir           "/var/log/mod_evasive"
</IfModule>

                                [ Read 12 lines ]
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line   M-E Redo
```

Carpeta donde se alojaron los logs del mod evasive



Firewall de Aplicaciones Web (WAF) Qo: Escudo Personalizado para Vulnerabilidades Específicas-instalado y configurado

Archivo conf del mod qos



Instalación del mod qos