



# **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.

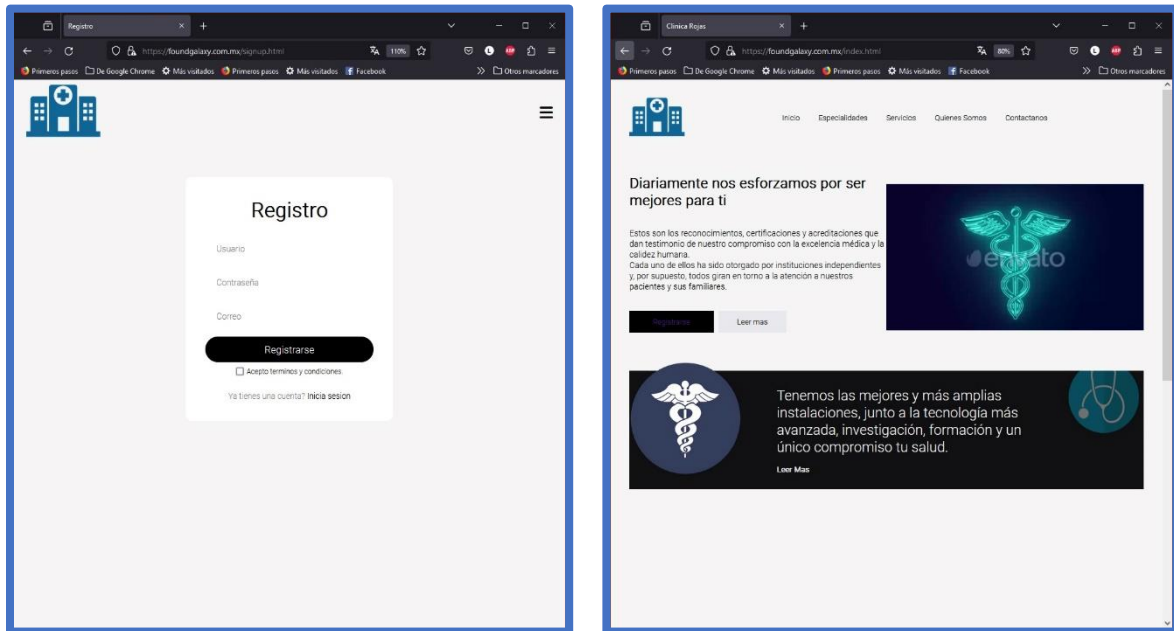
Un componente crítico de este informe se centrará en las medidas de seguridad implementadas para resguardar la integridad de la página web y la confidencialidad de los datos del paciente. Se discutirán en detalle los protocolos de cifrado, la configuración del cortafuegos, las actualizaciones regulares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

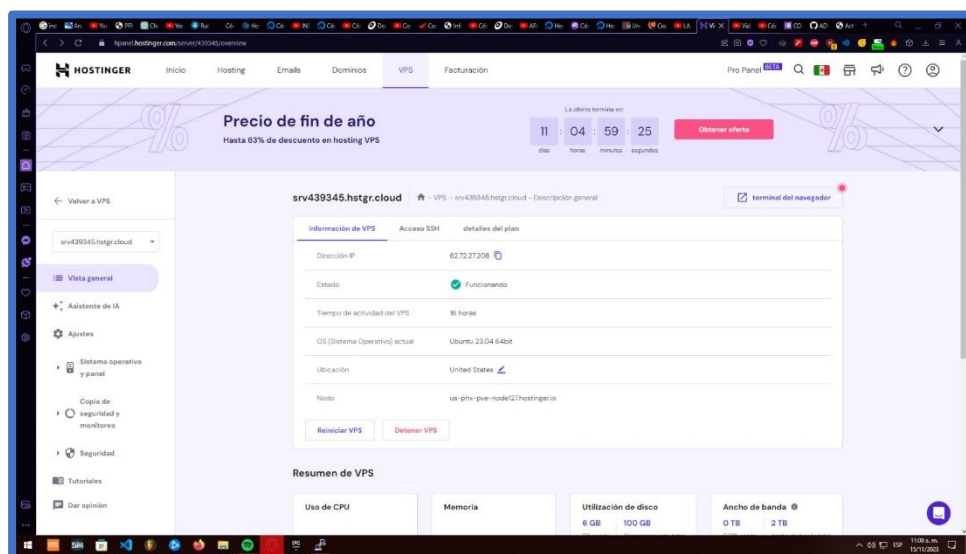
## Interfaz gráfica de la app

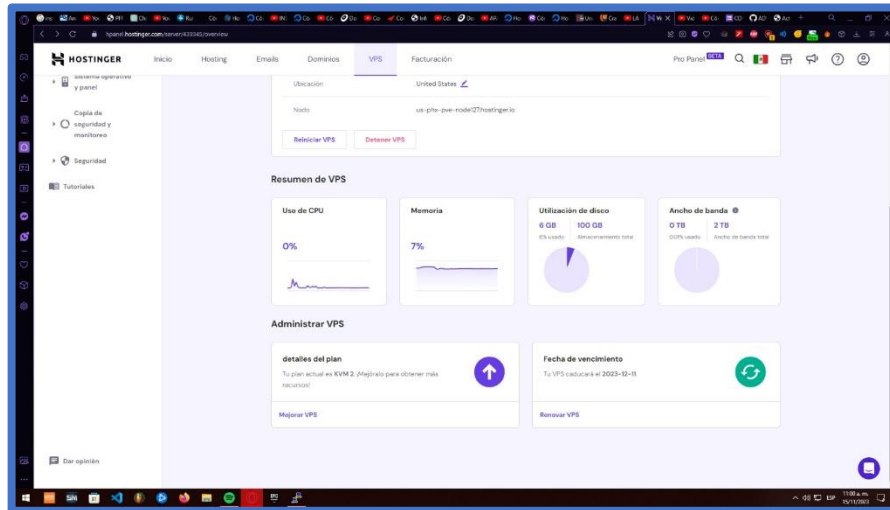
La interfaz de la página web de Clínica Rojas destaca por su diseño moderno y limpio. La disposición cuidadosa de elementos visuales y la paleta de colores elegante crean una experiencia visualmente atractiva. La funcionalidad intuitiva permite a los visitantes encontrar rápidamente la información que 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

```
root@royal95145: /etc/apache2/sites-available# nano /etc/apache2/sites-available/clinica.conf
# VirtualHost 7.7
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection (URLs in the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's host header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerName 62.72.27.208
ServerAdmin webmaster@localhost
DocumentRoot /var/www

WSGIDaemonProcess clinica threads=5
WSGIScriptAlias / /var/www/clinica/clinica.wsgi

<Directory clinica>
    WSGIScriptAlias /var/www/clinica/clinica.wsgi
    WSGIProcessGroup clinica
    WSGIApplicationGroup %{GLOBAL}
    Order deny,allow
    Allow from all
</Directory>

[ErrorLog ${APACHE_LOG_DIR}/error.log
LogLevel warn
CustomLog ${APACHE_LOG_DIR}/access.log combined

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the ssl configuration for this host only
# after it has been globally disabled with "disallow".
#Include conf-available/ssl.conf

#VirtualHost
```

## Se instalado pipx

```
root@srv439345: /var/www/clinica
See /usr/share/doc/python3.11/README.venv for more information.

note: If you believe this is a mistake, please contact your Python installation or OS distribution provider. You can override this, at the risk of breaking your Python installation or OS, by passing --break-system-packages.
hint: See PEP 668 for the detailed specification.
(venv) root@srv439345: /var/www/clinica# sudo apt install pipx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  blt fonts-font-awesome fonts-lato ghp-import libblas3 libgfortran5
  libjs-bootstrap4 libjs-highlight.js libjs-lunr libjs-modernizr
  libjs-popper.js libjs-sizzle liblapack3 libtk8.6 libxft2 libxrender1 libxss1
  mako node-jquery python3-argcomplete python3-datetutil python3-iniconfig
  python3-joblib python3-livereload python3-lunr python3-markdown
  python3-mergedeep python3-nltk python3-numpy python3-packaging
  python3-pluggy python3-psutil python3-py python3-pytest
  python3-pyyaml-env-tag python3-regex python3-tk python3-tornado python3-tqdm
  python3-userpath python3-venv python3-watchdog sphinx-rtd-theme-common
  tk8.6-blt2.5 x11-common
Suggested packages:
  blt-demo libjs-es5-shim tk8.6 mako-doc nodejs coffeescript node-less
  node-uglify python-livereload-doc python3-django python3-slimmer
  python-lunr-doc python-markdown-doc gfortran python-psutil-doc subversion
  tix python3-tk-dbg python3-pycurl python-tornado-doc
Recommended packages:
  prover9
The following NEW packages will be installed:
  blt fonts-font-awesome fonts-lato ghp-import libblas3 libgfortran5
  libjs-bootstrap4 libjs-highlight.js libjs-lunr libjs-modernizr
  libjs-popper.js libjs-sizzle liblapack3 libtk8.6 libxft2 libxrender1 libxss1
  mako node-jquery pipx python3-argcomplete python3-datetutil
  python3-joblib python3-livereload python3-lunr python3-markdown
  python3-iniconfig python3-nltk python3-numpy python3-packaging
  python3-markdown python3-mergedeep python3-nltk python3-numpy
  python3-packaging python3-pluggy python3-psutil python3-py python3-pytest
  python3-pyyaml-env-tag python3-regex python3-tk python3-tornado python3-tqdm
  python3-userpath python3-venv python3-watchdog sphinx-rtd-theme-common
  tk8.6-blt2.5 x11-common
0 upgraded, 46 newly installed, 0 to remove and 0 not upgraded.
Need to get 21.9 MB of archives.
After this operation, 88.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu lunar/main amd64 fonts-lato all 2.0-2.1 [2696 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu lunar/main amd64 libxrender1 amd64 1:0.9.10-1.1 [20.0 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu lunar/main amd64 libxft2 amd64 2.3.6-1 [44.5 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu lunar/main amd64 x11-common all 1:7.7+~
```

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

```
root@srv439345: /var/www/clinica
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
(venv) root@srv439345: /var/www/clinica# systemctl status mysql
● mysql.service - MySQL Community Server
   Loaded: loaded (/lib/systemd/system/mysql.service; enabled; preset: enabled)
   Active: active (running) since Tue 2023-11-14 10:25:18 UTC; 5h 52min ago
     Main PID: 432 (mysqld)
    Status: "Server is operational"
      Tasks: 37 (limit: 9551)
     Memory: 426.0M
        CPU: 56.464s
    CGroup: /system.slice/mysql.service
            └─432 /usr/sbin/mysqld

Nov 14 10:25:16 srv439345 systemd[1]: Starting mysql.service - MySQL Community
Nov 14 10:25:18 srv439345 systemd[1]: Started mysql.service - MySQL Community
(venv) root@srv439345: /var/www/clinica# sudo pip install flask-mysqldb
error: externally-managed-environment

This environment is externally managed
  To install Python packages system-wide, try apt install
  python3-xyz, where xyz is the package you are trying to
  install.

  If you wish to install a non-Debian-packaged Python package,
  create a virtual environment using python3 -m venv path/to/venv.
  Then use path/to/venv/bin/python and path/to/venv/bin/pip. Make
  sure you have python3-full installed.

  If you wish to install a non-Debian packaged Python application,
  it may be easiest to use pipx install xyz, which will manage a
  virtual environment for you. Make sure you have pipx installed.

  See /usr/share/doc/python3.11/README.venv for more information.

note: If you believe this is a mistake, please contact your Python installation
or OS distribution provider. You can override this, at the risk of breaking your
Python installation or OS, by passing --break-system-packages.
hint: See PEP 668 for the detailed specification.
(venv) root@srv439345: /var/www/clinica# pipenv install mysqlclient
```

## SEGURIDAD 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

```
root@srv12541b1:~# sudo apt install certbot python3-certbot-apache
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package certbot
root@srv12541b1:~# sudo apt install python3-certbot-apache
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  suprema-lenses libaugeas0 python3-some python3-suprema python3-certbot python3-configargparse python3-icu
  python3-josepy python3-parsedatetime python3-rfc3339
Suggested packages:
  suprema-doc python-certbot-doc python-certbot-nginx suprema-tools python-amer-doc python-certbot-nginx-doc
The following NEW packages will be installed:
  suprema-lenses libaugeas0 python3-some python3-suprema python3-certbot python3-configargparse python3-icu
  python3-josepy python3-parsedatetime python3-rfc3339
0 upgraded, 12 newly installed, 0 to remove and 0 not upgraded.
Need to get 1479 kB of archives.
After this operation, 7098 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu lunar/universe amd64 suprema-lenses all 1.14.0-1 [222 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu lunar/universe amd64 libaugeas0 amd64 1.14.0-1 [104 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu lunar/universe amd64 python3-josepy all 1.14.0-1 [12.0 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu lunar/universe amd64 python3-suprema all 1.14-1 [1474 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu lunar/universe amd64 python3-some all 2.1.0-1 [11.4 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu lunar/universe amd64 python3-certbot all 1.4.0-1 [1424 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu lunar/universe amd64 python3-configargparse all 1.5.3-1 [14.3 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu lunar/universe amd64 python3-parsedatetime all 2.6-3 [32.6 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu lunar/universe amd64 python3-certbot all 2.1.0-1 [145 kB]
Get:10 http://us.archive.ubuntu.com/ubuntu lunar/universe amd64 python3-icu amd64 certbot all 2.1.0-1 [80.0 kB]
Get:11 http://us.archive.ubuntu.com/ubuntu lunar/main amd64 python3-icu amd64 2.10.2-1build1 [128 kB]
Get:12 http://us.archive.ubuntu.com/ubuntu lunar/main amd64 python3-icu amd64 2.10.2-1build1 [128 kB]
Fetched 1479 kB in 1s (1481 kB/s)
Preconfiguring packages ...
Selecting previously unselected package suprema-lenses.
(Reading database ... 17781 files and directories currently installed.)
Preparing to unpack .../suprema-lenses_1.14.0-1_all.deb ...
Unpacking suprema-lenses (1.14.0-1) ...
Setting up suprema-lenses (1.14.0-1) ...
Setting up libaugeas0:amd64 (1.14.0-1) ...
Setting up python3-josepy (1.14.0-1) ...
Setting up python3-suprema (1.14-1) ...
Setting up python3-some (2.1.0-1) ...
Setting up python3-certbot (1.4.0-1) ...
Setting up python3-configargparse (1.5.3-1) ...
Setting up python3-parsedatetime (2.6-3) ...
Setting up python3-certbot (2.1.0-1) ...
Setting up python3-icu:amd64 (2.10.2-1build1) ...
Setting up python3-icu:amd64 (2.10.2-1build1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
```

```
root@srv12541b1:~# sudo certbot --nginx
[TITLE] (Info) y

-----
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a 501(c)(3)
non-profit organization that
- defends digital rights for all;
- works on legal challenges to help protect your privacy and security;
- EFF news, campaigns, and ways to support digital freedom.
-----
[TITLE] (Info) n
Account registered.

Which name would you like to activate HTTPS for?
0. www.foundpaly.com.mx
1. www.foundpaly.com.mx
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel):
Generating a certificate for www.foundpaly.com.mx and www.foundpaly.com.mx
Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/www.foundpaly.com.mx/fullchain.pem
Key is saved at: /etc/letsencrypt/live/www.foundpaly.com.mx/private.pem
This certificate expires on 2024-02-13.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for www.foundpaly.com.mx to /etc/apache2/sites-enabled/000011.conf
Successfully deployed certificate for www.foundpaly.com.mx to /etc/apache2/sites-enabled/000011.conf
Congratulations! You have successfully enabled HTTPS on https://www.foundpaly.com.mx and https://www.foundpaly.com.mx

-----
If you like Certbot, please consider supporting our work by:
* Donating to EFF: https://letsencrypt.org/donate
* Donating to EFF: https://eff.org/donate-us

root@srv12541b1:~# sudo systemctl status certbot.timer
* certbot.timer - Run certbot twice daily.
Loaded: loaded (/lib/systemd/system/certbot.timer; enabled; preset: enabled)
Active: active (waiting) since Wed 2023-11-15 18:07:13 UTC; 1min ago
Trigger: Tue 2023-11-15 01:00:00 UTC; 4h left
Trigger: * certbot.service

Nov 15 18:07:13 srv12541b1 systemd[1]: Started certbot.timer - Run certbot twice daily.
root@srv12541b1:~# sudo certbot renew --dry-run
Saving debug log to /var/log/letsencrypt/letsencrypt.log

-----
Processing /etc/letsencrypt/renewal/www.foundpaly.com.mx.conf
Account registered.
Simulating renewal of an existing certificate for www.foundpaly.com.mx and www.foundpaly.com.mx
Congratulations, all simulated renewals succeeded:
  /etc/letsencrypt/live/www.foundpaly.com.mx/fullchain.pem (success)
-----
root@srv12541b1:~#
```



## Información del certificado

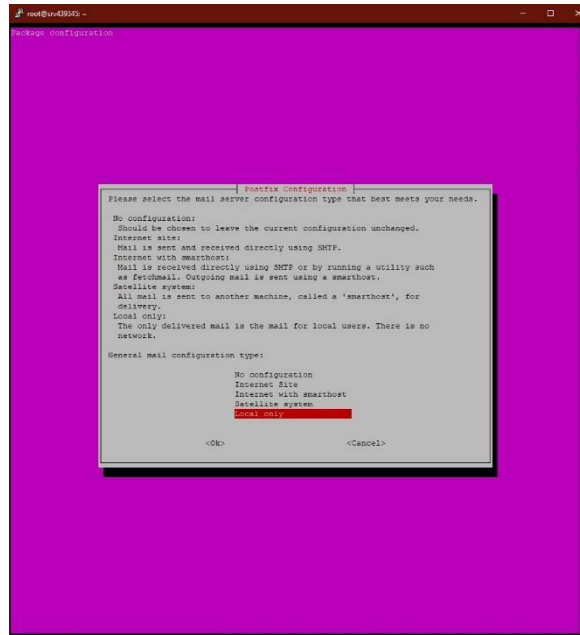
Certificado		
foundgalaxy.com.mx	R3	ISRG Root X1
Nombre del interesado		
Nombre común	foundgalaxy.com.mx	
Nombre del emisor		
País	US	
Organización	Let's Encrypt	
Nombre común	R3	
Validez		
No antes	Wed, 15 Nov 2023 17:21:24 GMT	
No después	Tue, 13 Feb 2024 17:21:23 GMT	
Nombres alternativos del sujeto		
Nombre de DNS	foundgalaxy.com.mx	
Nombre de DNS	www.foundgalaxy.com.mx	
Información de clave pública		
Algoritmo	Elliptic Curve	
Tamaño de clave	256	
Valor público	04:F0:38:B3:29:A3:3B:E0:4D:6B:7B:F3:7A:AD:22:1E:95:64:A7:BE:5E:53:4A:36:B8:E5:...	

## Mod-Security: Defensa Proactiva en Capas-instalado

```
root@srv439345: ~  
login as: root  
root@62.72.27.208's password:  
Access denied  
root@62.72.27.208's password:  
Welcome to Ubuntu 23.04 (GNU/Linux 6.2.0-1016-kvm x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Wed Nov 15 18:36:10 UTC 2023  
  
System load:  0.02          Processes:           92  
Usage of /:   3.2% of 96.78GB Users logged in:       1  
Memory usage: 8%          IPv4 address for eth0: 62.72.27.208  
Swap usage:  0%           IPv6 address for eth0: 2a02:4780:10:a0b3::1  
  
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s  
  just raised the bar for easy, resilient and secure K8s cluster deployment.  
  
  https://ubuntu.com/engage/secure-kubernetes-at-the-edge  
  
0 updates can be applied immediately.  
  
New release '23.10' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Last login: Wed Nov 15 18:06:25 2023 from 177.227.8.34  
root@srv439345:~# apachectl -M | grep security  
security2_module (shared)  
root@srv439345:~#
```



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



```
root@srv439345:~  
Preparing to unpack .../libapache2-mod-evasive_1.10.1-5_amd64.deb ...  
Unpacking libapache2-mod-evasive (1.10.1-5) ...  
Setting up liblockfile-bin (1.17-1build2) ...  
Setting up postfix (3.7.4-2build1) ...  
Adding group 'postfix' (GID 119) ...  
Done.  
Adding system user 'postfix' (GID 119) ...  
Adding new user 'postfix' (GID 119) with group 'postfix' ...  
Not creating home directory '/var/spool/postfix'.  
Creating /etc/postfix/dynamicmaps.cf  
Adding group 'postdrop' (GID 120) ...  
Done.  
Setting myhostname: srv439345.hstgr.cloud  
Setting alias maps  
Setting alias database  
Changing /etc/mailname to srv439345.hstgr.cloud  
Setting myorigin  
Setting destinations: $myhostname, srv439345.hstgr.cloud, localhost.hstgr.cloud, localhost  
Setting relayhost:  
Setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128  
Setting mailbox_size_limit: 0  
Setting recipient_delimiter: +  
Setting inet_interfaces: loopback-only  
Setting default_transport: error  
Setting relay_transport: error  
Setting inet_protocols: all  
/etc/aliases does not exist, creating it.  
WARNING: /etc/aliases exists, but does not have a root alias.  
  
Postfix (main.cf) is now set up with a default configuration. If you need to  
make changes, edit /etc/postfix/main.cf (and others) as needed. To view  
Postfix configuration values, see postconf(1).  
  
After modifying main.cf, be sure to run 'systemctl reload postfix'.  
  
Running newaliases  
Created symlink /etc/systemd/system/multi-user.target.wants/postfix.service → /lib/systemd/system/postfix.service.  
Setting up liblockfile:amd64 (1.17-1build2) ...  
Setting up bad-mailx (0.1.2-0.20200429~1) ...  
update-alternatives: using /usr/bin/bad-mailx to provide /usr/bin/mailx (mailx) in auto mode  
Setting up libapache2-mod-evasive (1.10.1-5) ...  
apache2_invoke: Enable module evasive  
Processing triggers for rsyslog (8.2302.0-1ubuntu3) ...  
Processing triggers for ufw (0.36-1~4.1ubuntu0.1) ...  
Rules updated for profile 'Apache Full'  
Rules updated for profile 'OpenSSH'  
Stripped reloading firewalld  
Processing triggers for man-db (2.11.2-1) ...  
Processing triggers for libc-bin (2.37-0ubuntu2.1) ...  
Scanning processes...  
Scanning linux images...  
  
Running kernel seems to be up-to-date.  
  
No services need to be restarted.  
  
No containers need to be restarted.  
  
No user sessions are running outdated binaries.  
  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
root@srv439345:~#
```

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

Configuración de los parámetros de mod evasive

```
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 ]

<b>^G</b> Help	<b>^O</b> Write Out	<b>^W</b> Where Is	<b>^R</b> Cut	<b>^H</b> Execute	<b>^C</b> Location	<b>M-U</b> Undo
<b>^X</b> Exit	<b>^R</b> Read File	<b>^N</b> Replace	<b>^U</b> Paste	<b>^J</b> Justify	<b>^_</b> Go To Line	<b>M-R</b> Redo

Carpeta donde se alojaron los logs del mod evasive

```
root@srv439345: /var/log
root@srv439345:~# apachectl -M | grep evasive
evasive20_module (shared)
root@srv439345:~# nano /etc/apache2/mods-enabled/evasive.conf
root@srv439345:~# nano /etc/apache2/mods-enabled/evasive.conf
root@srv439345:~# nano /etc/apache2/mods-enabled/evasive.conf
root@srv439345:~# cd /var/log/
root@srv439345:/var/log# ls
README      auth.log      dmesg         dmesg.4.gz    lastlog       private       wtmp
alternatives.log  btmap        dmesg.0       dpkg.log      letsencrypt   syslog
apache2        cloud-init-output.log  dmesg.1.gz    journal       mail.log      ubuntu-advantage.log
apport.log     cloud-init.log  dmesg.2.gz    kern.log      modsecurity   ufw.log
apt            dist-upgrade   dmesg.3.gz    landscape     mysql         unattended-upgrades
root@srv439345:/var/log# mkdir mod_evasive
root@srv439345:/var/log# chown -R www-data:www-data /var/log/mod_evasive/
root@srv439345:/var/log#
```

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

Archivo conf del mod qos

```
GNU nano 7.2 /etc/apache2/mods-enabled/qos.conf *
<IfModule qos_module>
    minimum request rate (bytes/sec at request reading):
    QS_SrvRequestRate 120

    limits the connections for this virtual host:
    QS_SrvMaxConn 100

    allows keep-alive support till the server reaches 600 connections:
    QS_SrvMaxConnClose 600

    allows max 50 connections from a single ip address:
    QS_SrvMaxConnPerIP 50
</IfModule>
```

## Instalación del mod qos

```
root@srv439345: ~  
root@srv439345:~# apt install libapache2-mod-qos  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  libpcre3  
The following NEW packages will be installed:  
  libapache2-mod-qos libpcre3  
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.  
Need to get 476 kB of archives.  
After this operation, 1505 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://us.archive.ubuntu.com/ubuntu lunar/main amd64 libpcre3 amd64 2:8.39-15 [250 kB]  
Get:2 http://us.archive.ubuntu.com/ubuntu lunar/universe amd64 libapache2-mod-qos amd64 11.63-1build1 [226 kB]  
Fetched 476 kB in 1s (856 kB/s)  
Selecting previously unselected package libpcre3:amd64.  
(Reading database ... 95386 files and directories currently installed.)  
Preparing to unpack .../libpcre3_2%3a8.39-15_amd64.deb ...  
Unpacking libpcre3:amd64 (2:8.39-15) ...  
Selecting previously unselected package libapache2-mod-qos.  
Preparing to unpack .../libapache2-mod-qos_11.63-1build1_amd64.deb ...  
Unpacking libapache2-mod-qos (11.63-1build1) ...  
Setting up libpcre3:amd64 (2:8.39-15) ...  
Setting up libapache2-mod-qos (11.63-1build1) ...  
apache2_invoke: Enable module qos  
apache2_reload: Your configuration is broken. Not restarting Apache 2  
apache2_reload: apache2: Syntax error on line 146 of /etc/apache2/apache2.conf: Syntax error on line 1 of /etc/apache  
2/mods-enabled/qos.load: Cannot load /usr/lib/apache2/modules/mod_qos.so into server: /usr/lib/apache2/modules/mod_qo  
s.so: undefined symbol: pcre_free  
Processing triggers for man-db (2.11.2-1) ...  
Processing triggers for libc-bin (2.37-0ubuntu2.1) ...  
Scanning processes...  
Scanning linux images...  
  
Running kernel seems to be up-to-date.  
  
No services need to be restarted.  
  
No containers need to be restarted.  
  
No user sessions are running outdated binaries.  
  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
root@srv439345:~# nano /etc/apache2/mods-enabled/qos.conf  
root@srv439345:~#
```