

**Manual de usuario**

**Web Application Firewall**

**Autores**: Hernández Estrada José María

Rossello Romero Jason Adair

**Versión**: 01.00

**Fecha**: 11/03/2020

|  |  |
| --- | --- |
| C:\Users\chema\OneDrive\Escritorio\img-manual\WAF_blanco.png | **WAF**  **Plantilla de Manual de usuario** |
| **Hoja de Control de Modificaciones** |

# Hoja de Control de Modificaciones

|  |  |
| --- | --- |
| Título | WAF  Manual de usuario |
| Versión | 01.00 |
| Realizado | Hernández Estrada José María  Rossello Romero Jason Adair |
| Fecha: | 11/03/2020 |

|  |  |  |
| --- | --- | --- |
| **CONTROL DE VERSIONES** | | |
| Versión | Descripción / Motivo versión | Fecha de presentación |
| 01.00 | Documento inicial | 11/03/2020 |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
|  | **WAF**  **Manual de usuario** |
| **Índice** |

**Índice**

Contenido

[Hoja de Control de Modificaciones 2](#_Toc34864258)

[Lista de Tablas 5](#_Toc34864259)

[1. Objeto del documento 6](#_Toc34864260)

[2. Participantes 6](#_Toc34864261)

[3. Objetivos 6](#_Toc34864262)

[4. Manual de usuario 6](#_Toc34864263)

[4.1. Pantalla Inicial 6](#_Toc34864264)

[4.2. Menú de configuraciones del WAF. 8](#_Toc34864265)

[4.2.1 Cargar Black List. 8](#_Toc34864266)

[4.2.2 Cargar White List. 9](#_Toc34864267)

[4.2.3 Desbloqueo de Ip. 9](#_Toc34864268)

[4.2.4 Comandos Back y Show. 10](#_Toc34864269)

[4.2.4 Generar Reporte. 10](#_Toc34864270)

[4.2.5 Modificar Password. 11](#_Toc34864271)

[4.2.6 Modificar número de ataques para notificación. 11](#_Toc34864272)

[4.2.7 Modificar tiempo de cuarentena. 11](#_Toc34864273)

[4.2.8 Modificar tiempo de vaciado de Black List. 11](#_Toc34864274)

[4.2.9 Modificar correo. 12](#_Toc34864275)

[4.2.9 Salir 12](#_Toc34864276)

[5. Glosario 13](#_Toc34864277)

|  |  |
| --- | --- |
|  | **WAF**  **Manual de usuario** |
| **Lista de Figuras** |

**Lista de Figuras**

[Ilustración 1.1: Configuraciones iniciales 7](#_bookmark1)

[Ilustración 1.2: Menú principal 7](#_bookmark1)

[Ilustración 1.3. Autenticación 8](#_bookmark2)

[Ilustración 1.4: Menú de configuraciones 8](#_bookmark2)

[Ilustración 1.5: Cargar una Ip en la Black List 9](#_bookmark3)

[Ilustración 1.6: Cargar Ips en la Black List, separadas por coma 9](#_bookmark3)

[Ilustración 1.7: Cargar rangos de Ip en la Black List 10](#_bookmark4)

[Ilustración 1.8: Menú para cargar White List. 10](#_bookmark4)

[Ilustración 1.9: Cargar White List 12](#_bookmark5)

[Ilustración 1.10: Desbloqueo de Ip 12](#_bookmark5)

[Ilustración 1.11: Comando Back 13](#_bookmark6)

[Ilustración 1.12: Comando Show 14](#_bookmark7)

[Ilustración 1.13: Generación de reporte 15](#_bookmark8)

[Ilustración 1.14: Modificación de contraseña 15](#_bookmark8)

[Ilustración 1.15: Modificación de límite de ataques 13](#_bookmark6)

[Ilustración 1.16: Modificación de tiempo de cuarentena 14](#_bookmark7)

[Ilustración 1.17: Modificación de tiempo de vaciado de la BlackList 15](#_bookmark8)

[Ilustración 1.18: Modificación de correo 15](#_bookmark8)

[Ilustración 1.19: Salir 15](#_bookmark8)

|  |  |
| --- | --- |
|  | **WAF**  **Manual de usuario** |
| **Lista de Tablas** |

# Lista de Tablas

[Tabla 1: Participantes 6](#_bookmark0)

[Tabla 2: Glosario 15](#_bookmark8)

|  |  |
| --- | --- |
|  | **WAF**  **Manual de usuario** |
| **Glosario** |

## Objeto del documento

El presente documento pretende mostrar y enseñar al usuario el funcionamiento del *Web Application Firewall*, su instalación, ejecución y configuraciones, con la finalidad de proteger a un servidor web de ataques *SQL injection* y *XSS*.

## Participantes

|  |  |
| --- | --- |
| **Participante** | Hernández Estrada José María  Rossello Romero Jason Adair |
| **Asignatura** | Trabajo Terminal II |
| **Teléfono** | 5543849896  5528888280 |
| **Rol** | Desarrollo |

Tabla 1: Participantes

## Objetivos

Se pretende mostrar de una manera clara y concisa para el usuario el funcionamiento del Web Aplication Firewall.

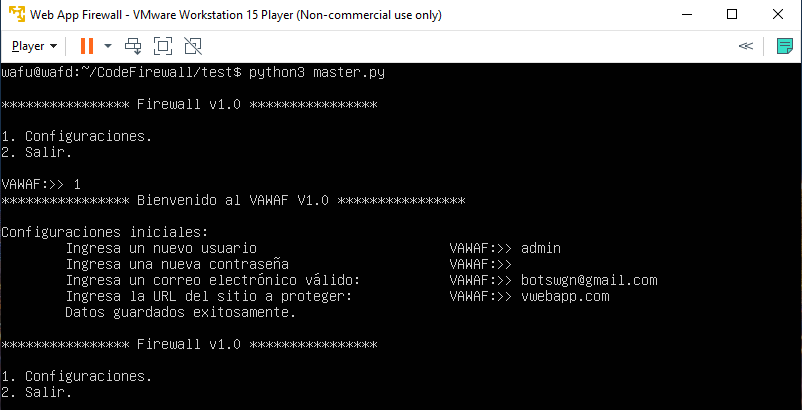
## Manual de usuario

## Pantalla Inicial

La pantalla inicial muestra dos opciones diferentes, la primera es cuando el sistema de seguridad se está configurando por primera vez, es decir pedirá al administrador las configuraciones iniciales, y el otro caso es cuando el sistema ya cuanta con las configuraciones iniciales, en este caso solo pedirá una autenticación de usuario y contraseña para dar acceso a las configuraciones.

**4.1.1 Configuraciones Iniciales.**

Se ejecuta cuando el sistema se inicia por primera vez, primero el sistema solicitara acceder un usuario valido (que tenga entre 4 y 30 caracteres), posteriormente solicitara una contraseña (que tenga entre 8 y 30 caracteres, al menos una mayúscula, al menos una minúscula, al menos un digito y al menos un carácter especial), posteriormente solicitara una Ip:Puerto introducidos en ese formato(127.0.0.1:8080) en los cuales trabajara el WAF y por ultimo solicitara un email, al cual el sistema enviara los reportes generados.



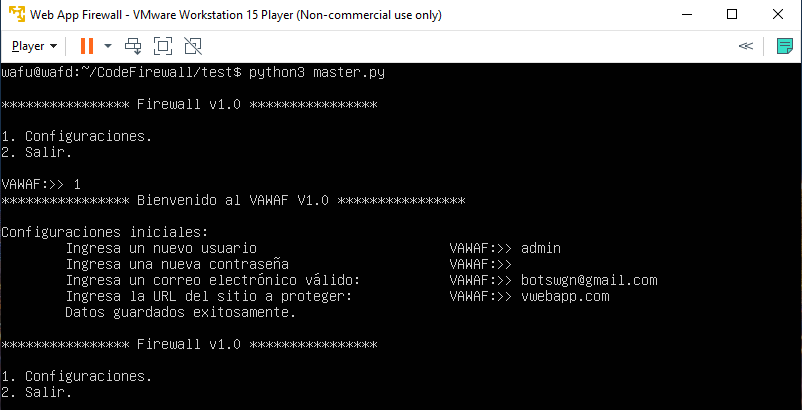
**Ilustración 1.1: Configuraciones iniciales**

**4.1.2 Login.**

Si el sistema ya cuenta con las configuraciones iniciales, ahora mostrara una pantalla en la cual se muestra un menú con las opciones:

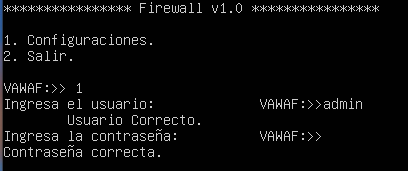
1. Configuraciones.

2. Salir.



**Ilustración 1.2: Menú principal**

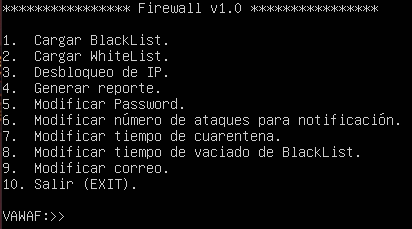
Si queremos acceder a las configuraciones el sistema nos solicitara una autenticación con el usuario y la contraseña que accedimos en las configuraciones iniciales para darnos acceso al menú de configuraciones del sistema.



**Ilustración 1.3: Autenticación**

## Menú de configuraciones del WAF.

Después de autenticarse correctamente el sistema mostrara un menú de configuraciones como el siguiente.

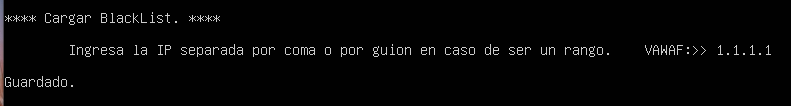


**Ilustración 1.4: Menú de configuraciones**

En este menú aparecen todas opciones configurables del sistema, así como funcionalidades como lo son generación de reporte, precargado de Black List y White List o Desbloqueo de una Ip, entro otros.

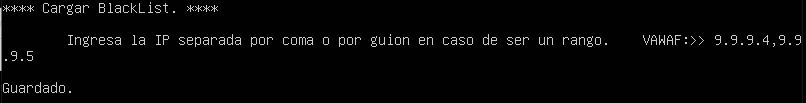
## 4.2.1 Cargar Black List.

En esta opción es posible cargar al sistema una o muchas Ips en la lista negra, es decir cargarlas a la lista de atacantes. Hay 3 formas diferentes de cargar esta lista, la primera es cargar una sola Ip, en este caso de insertará una Ip en su formato correcto, de no ser correcto el sistema informara el problema y solicitara nuevamente la Ip.



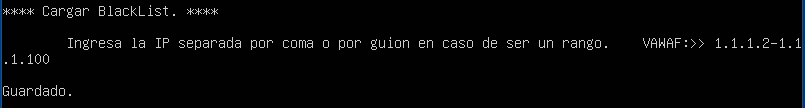
**Ilustración 1.5: Cargar una Ip en la Black List**

La segunda opción es cargar varias Ips separadas por comas, simplemente se introducen las Ips deseadas, separada por una coma y sin espacios, en caso de ser incorrecta la entrada, se notificara y se solicitara nuevamente.



**Ilustración 1.6: Cargar Ips en la Black List, separadas por coma**

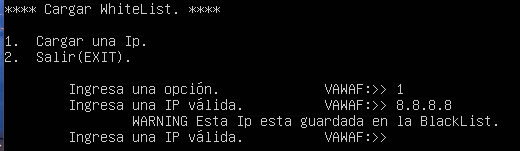
La tercera forma y ultima es introducir rangos, separados por un guion. La primera Ip debe ser mayor a la segunda y solamente puede haber cambios en los 2 últimos octetos de la Ip, debido a la enorme cantidad de Ips que en ese rango y superiores existe.



**Ilustración 1.7: Cargar rangos de Ip en la Black List**

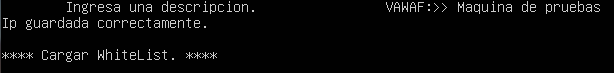
## 4.2.2 Cargar White List.

Cargar la White List es guardar en el sistema Ips que ya sabemos que son confiables para el sistema, como lo son Ips de proveedores, administradores, Ips internas a la empresa. Estas Ip solo pueden ser cargadas de una en una, primero se desplegara este pequeño menú:



**Ilustración 1.8: Menú para cargar White List**

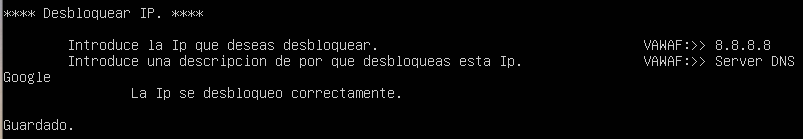
Y la Ip se carga de la siguiente manera:



**Ilustración 1.9: Cargar White List**

## 4.2.3 Desbloqueo de Ip.

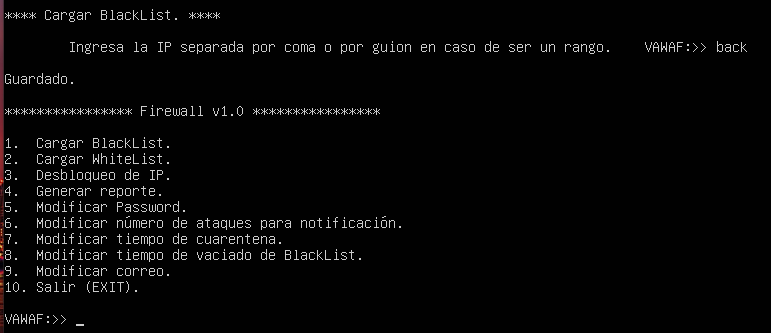
En esta opción se borra una Ip contenida en la Black List, es decir se deja de ver como atacante, simplemente basta con digitar la Ip, la cual debe estar guardada en la Black List y presionar la tecla enter, si no existe esta Ip o está mal escrita, se informara y solicitara nuevamente la Ip.



**Ilustración 1.10: Desbloqueo de Ip**

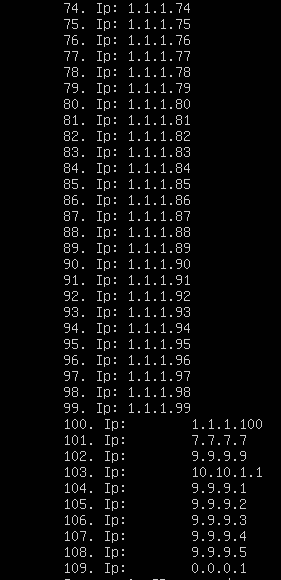
## 4.2.4 Comandos Back y Show.

Para poder navegar libremente en el menú de configuraciones se implementó el comando **back** en cual da un salto atrás al menú, es decir sale de la opción en la que nos encontremos y regresa al menú principal, es de mucha utilidad si nos equivocamos de opción o ya no queremos estar en esa opción.



**Ilustración 1.11: Comando Back**

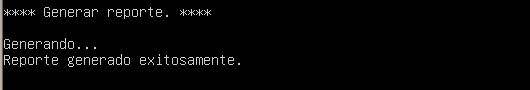
El comando Show muestra todas las Ips contenidas en la White list o en la Black List, dependiendo de la opción que nos encontremos, esto con la finalidad de que es administrador pueda saber que Ips están guardadas en estas listas. El comando funciona en Cargar Black List, Cargar White List y Desbloqueo de Ip.



**Ilustración 1.12: Comando Show**

## 4.2.4 Generar Reporte.

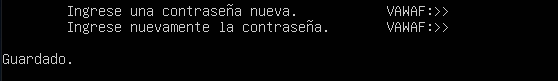
Esta opción genera un reporte en formato PDF, en el cual podemos ver todas las modificaciones que se han guardado en el sistema, modificaciones de correos, contraseñas, límites de ataques, tiempos de cuarentena, ataques detectados entre otra información.



**Ilustración 1.13: Generación de reporte**

## 4.2.5 Modificar Password.

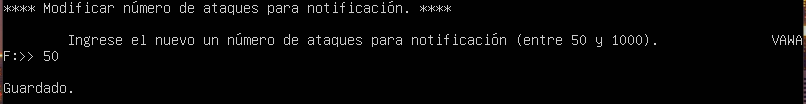
En esta opción se modifica la contraseña, para lograr el objetivo es necesario autenticarse primero con la contraseña vieja e introducir la contraseña nueva 2 veces para corroborar que es la misma.



**Ilustración 1.14: Modificación de contraseña**

## 4.2.6 Modificar número de ataques para notificación.

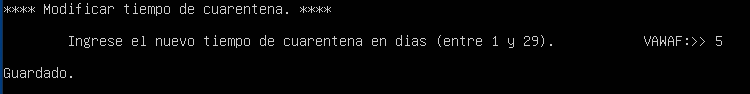
El sistema establece un valor de 100 ataques para este límite, es decir cuando detecte que se han hecho 100 ataques el sistema enviara una alerta al correo electrónico que se cargó en las configuraciones iniciales adjuntando el reporte actualizado hasta ese momento. En esta opción es posible modificar este límite desde 50 ataques hasta 1000.



**Ilustración 1.15: Modificación de límite de ataques**

## 4.2.7 Modificar tiempo de cuarentena.

El tiempo de cuarentena es un tiempo en días, en el cual se vaciara la Black List, desbloqueando automáticamente la Ip guardada que ha cumplido su tiempo de cuarentena. En esta opción se puede modificar este tiempo de cuarentena desde 1 hasta 60 días.



**Ilustración 1.16: Modificación de tiempo de cuarentena**

## 4.2.8 Modificar tiempo de vaciado de Black List.

El tiempo de vaciado de la Black List es un tiempo en días, en el cual se borra en su totalidad la Black List, con la finalidad de desbloquear todas las Ips bloqueadas para pasar por el analizador de ataques. En este apartado se puede modificar este tiempo desde 1 día hasta 60 días.



**Ilustración 1.17: Modificación de tiempo de vaciado de Black List**

## 4.2.9 Modificar correo.

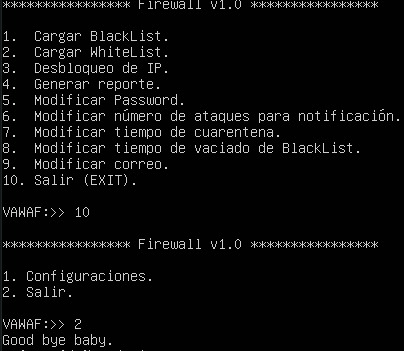
En esta opción se puede modificar el correo al cual llegaran las notificaciones de ataques y el reporte de modificaciones y ataques.

## C:\Users\chema\OneDrive\Escritorio\img-manual\c18.PNG

**Ilustración 1.18: Modificación de correo electrónico**

## 4.2.9 Salir

Para salir del menú de modificaciones se puede escribir el número correspondiente a la opción o bien escribir “EXIT” o “exit”.



**Ilustración 1.19: Salir**

## Glosario

A continuación se indican los términos utilizados, en el presente documento.

|  |  |
| --- | --- |
| **Término** | **Descripción** |
| Black List | Lista negra, donde se almacenan las Ip de los atacantes. |
| White List | Lista blanca, donde se almacenan las Ip confiables al sistema. |
| Ip | Conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red. Dirección lógica. |
| WAF | Web Application Firewall. |
| Firewall | Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad. |
| SQL Injection | Es una vulnerabilidad que permite al atacante enviar o “inyectar” instrucciones SQL de forma maliciosa y malintencionada dentro del código SQL programado para la manipulación de bases de datos. |
| XSS | Cross-site scripting (XSS) es un tipo de vulnerabilidad informática típica de las aplicaciones Web, que puede permitir a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar. |

Tabla 1: Glosario