Tabla de contenido

[FASE DE INICIO 3](#_Toc454748103)

[1. Captura de requisitos 3](#_Toc454748104)

[1.1. Identificar actores y casos de usos 3](#_Toc454748105)

[ Actores 3](#_Toc454748106)

[ Casos de uso 3](#_Toc454748107)

[1.2. Priorizar casos de uso 3](#_Toc454748108)

[1.3. Detallar caso de uso 3](#_Toc454748109)

[CU1. Gestionar contacto 3](#_Toc454748110)

[CU2. Gestionar cliente 4](#_Toc454748111)

[CU3. Gestionar evento 5](#_Toc454748112)

[CU4. Administrar tarifa 6](#_Toc454748113)

[1.4. Diagrama general de casos de usos 8](#_Toc454748114)

[FASE DE ANÁLISIS 8](#_Toc454748115)

[2. Análisis 8](#_Toc454748116)

[2.1. Análisis de casos de usos 8](#_Toc454748117)

[2.1.1. Diagrama general de comunicaciones 8](#_Toc454748118)

[CU1. Gestionar contacto 8](#_Toc454748119)

[CU2. Gestionar cliente 9](#_Toc454748120)

[CU3. Gestionar evento 9](#_Toc454748121)

[CU4. Administrar tarifa 9](#_Toc454748122)

[FASE DE DISEÑO 10](#_Toc454748123)

[3. Diseño 10](#_Toc454748124)

[3.1. Diseño conceptual de la base de datos 10](#_Toc454748125)

[3.2. Diseño lógica de la base de datos 10](#_Toc454748126)

[3.2.1. Mapeo 10](#_Toc454748127)

[3.3. Diseño físico de la base de datos 11](#_Toc454748128)

[3.3.1. Tablas de volumen 11](#_Toc454748129)

[3.4. Diagramas de secuencia 13](#_Toc454748130)

[CU1. Gestionar contacto 13](#_Toc454748131)

[CU2. Gestionar cliente 14](#_Toc454748132)

[CU3. Gestionar evento 15](#_Toc454748133)

[CU4. Administrar tarifa 16](#_Toc454748134)

[FASE DE PRUEBAS 16](#_Toc454748135)

[4. Pruebas 16](#_Toc454748136)

[ Pruebas de rendimiento con JMeter 16](#_Toc454748137)

[ Pruebas de eficiencia con Amazon CloudWath 18](#_Toc454748138)

[ Pruebas de seguridad 20](#_Toc454748139)

[Prueba de seguridad utilizando ZAP, para ataques contra bots, scripts, querys 20](#_Toc454748140)

[5. HERRAMIENTAS 21](#_Toc454748141)

[ Amazon EC2 (Elastic Compute Cloud) 21](#_Toc454748142)

[ Amazon RDS (Relational Database Service) 22](#_Toc454748143)

[ Amazon WAF (WEB APPLICATION FIREWALL) 23](#_Toc454748144)

[ Amazon CloudWatch 24](#_Toc454748145)

[ JMETER 25](#_Toc454748146)

[ Spawner 26](#_Toc454748147)

[ GitHub 26](#_Toc454748148)

[ SourceTree 26](#_Toc454748149)

[ SQLMap 27](#_Toc454748150)

[ ZAP (Zed Attack Proxy) 28](#_Toc454748151)

# FASE DE INICIO

# Captura de requisitos

## Identificar actores y casos de usos

## Actores

1. Administrador
2. Cliente

## Casos de uso

1. Gestionar contacto
2. Gestionar cliente
3. Gestionar evento
4. Administrar tarifa

## Priorizar casos de uso

|  |  |  |  |
| --- | --- | --- | --- |
| NRO. | CASO DE USO | ACTOR | PRIORIDAD |
|  | Gestionar contacto | Cliente | Media |
|  | Gestionar cliente | Cliente | Media |
|  | Gestionar evento | Cliente | Alta |
|  | Administrar tarifa | Cliente | Media |

## Detallar caso de uso

### Gestionar contacto



|  |  |
| --- | --- |
| Caso de Uso | CU1. Gestionar contacto |
| Propósito | Registrar, actualizar y dar de baja contactos del cliente |
| Descripción | Permite a los cliente realizar todas las acciones mencionadas para sus contactos |
| Actores | A1. Cliente |
| Actor Iniciador | A1. Cliente |
| Precondición | Ninguna |
| Proceso | 1. **El cliente registrar un contacto**    1. El caso de uso inicia cuando el cliente presiona el botón para añadir un contacto    2. El cliente debe registrar los datos personales de sus contacto como nombre, dirección, correo    3. La aplicación validará que el usuario haya ingresado correctamente los datos en los campos especificados    4. El contacto es guardado en la BD y actualiza su lista de contactos 2. **La Cliente desea actualizar o dar de baja un contacto**    1. Se inicia cuando el cliente selecciona la opción de actualizar un contacto    2. Se despliega una ventana con todos los campos que posee ese contacto y que se pueden actualizar    3. El cliente ingresa los datos que desea actualizar    4. La aplicación validará que el usuario haya ingresado correctamente los datos en los campos especificados    5. El contacto es actualiza en la BD y actualiza su lista de contactos |
| Postcondición | Ninguna. |
| Excepciones | 1.2. Los datos ingresados por el administrador son incorrectos.  1.4. Error en la conexión no se puede guardar el cliente  2.3. Los datos ingresados por el administrador son incorrectos.  2.5. Error en la conexión no se puede guardar el cliente |

### Gestionar cliente



|  |  |
| --- | --- |
| Caso de Uso | CU2. Gestionar cliente |
| Propósito | Registrar, actualizar y dar de baja clientes |
| Descripción | Permite al administrador realizar todas las acciones mencionadas para los clientes |
| Actores | A2. Administrador |
| Actor Iniciador | A2. Administrador |
| Precondición | Ninguna |
| Proceso | 1. **El administrador desea registrar un cliente**    1. El caso de uso inicia cuando el administrador presiona el botón para añadir un cliente    2. El administrador debe registrar los datos personales de sus clientes como nombre, dirección, correo    3. La aplicación validará que el administrador haya ingresado correctamente los datos en los campos especificados    4. El cliente es guardado en la BD y actualiza su lista de contactos 2. **La administrador desea actualizar o dar de baja un cliente**    1. Se inicia cuando el administrador selecciona la opción de actualizar un contacto    2. Se despliega una ventana con todos los campos que posee ese contacto y que se pueden actualizar    3. El administrador ingresa los datos que desea actualizar    4. La aplicación validará que el administrador haya ingresado correctamente los datos en los campos especificados    5. El cliente es actualiza en la BD y actualiza su lista de contactos |
| Postcondición | Ninguna. |
| Excepciones | 1.2. Los datos ingresados por el cliente son incorrectos.  1.4. Error en la conexión no se puede guardar el contacto  2.3. Los datos ingresados por el cliente son incorrectos.  2.5. Error en la conexión no se puede guardar el contacto |

### Gestionar evento



|  |  |
| --- | --- |
| Caso de Uso | CU3. Gestionar evento |
| Propósito | Registrar, administrar y dar de baja eventos |
| Descripción | Permite al administrador realizar todas las acciones mencionadas para los clientes |
| Actores | A1. Cliente |
| Actor Iniciador | A1. Cliente |
| Precondición | Ninguna |
| Proceso | 1. **El cliente desea registrar un evento**    1. El caso de uso inicia cuando el cliente presiona el botón para añadir un evento    2. El cliente debe registrar los datos del evento que desea registrar como nombre, dirección, fecha de inicio y fecha final    3. La aplicación validará que el cliente haya ingresado correctamente los datos en los campos especificados    4. El evento es guardado en la BD y actualiza su lista de eventos    5. La aplicación despliega una ventana para que el usuario invite sus contactos 2. **La cliente desea actualizar o dar de baja un evento**    1. El caso de uso inicia cuando el cliente presiona el botón para editar un evento    2. La aplicación desplegará todos los datos correspondiente a ese evento    3. El cliente debe actualizar los datos del evento solicitado    4. La aplicación validará que el cliente haya ingresado correctamente los datos en los campos especificados    5. El evento es actualizado en la BD y actualiza su lista de eventos |
| Postcondición | CU6. Invitar contacto |
| Excepciones | 1.2. Los datos ingresados por el cliente son incorrectos.  1.4. Error en la conexión no se puede guardar el contacto  1.5. No existe ningún contacto registrado  2.3. Los datos ingresados por el cliente son incorrectos.  2.5. Error en la conexión no se puede guardar el contacto |

### Administrar tarifa



|  |  |
| --- | --- |
| Caso de Uso | CU4. Administrar tarifa |
| Propósito | Registrar y administrar tarifas |
| Descripción | Permite al administrador registrar y administrar las tarifas. |
| Actores | A2. Administrador |
| Actor Iniciador | A2. Administrador |
| Precondición | Ninguna |
| Proceso | 1. **El administrador desea registrar una tarifa**    1. El caso de uso inicia cuando el administrador presiona el botón para añadir una nueva tarifa    2. El administrador debe registrar los datos de la tarifa que desea registrar como ser evento y contacto    3. La aplicación validará que el administrador haya ingresado correctamente los datos en los campos especificados    4. El evento es guardado en la BD y actualiza su lista de tarifas 2. **La cliente desea actualizar una tarifa**    1. El caso de uso inicia cuando el administrador presiona el botón para modificar una tarifa    2. La aplicación desplegará una ventana con la tarifa que se desee modificar    3. El administrador debe actualizar los datos de la tarifa que desea actualizar como ser evento y contacto    4. La aplicación validará que el administrador haya ingresado correctamente los datos en los campos especificados    5. El evento es actualizado en la BD y actualiza su lista de tarifas |
| Postcondición | Ninguna |
| Excepciones | 1.2. Los datos ingresados por el cliente son incorrectos.  1.4. Error en la conexión no se puede guardar el contacto  2.3. Los datos ingresados por el cliente son incorrectos.  2.5. Error en la conexión no se puede guardar el contacto |

## Diagrama general de casos de usos



# FASE DE ANÁLISIS

# Análisis

## Análisis de casos de usos

## Diagrama general de comunicaciones

### Gestionar contacto

### Gestionar cliente



### Gestionar evento

### Administrar tarifa

# FASE DE DISEÑO

# Diseño

## Diseño conceptual de la base de datos



## Diseño lógica de la base de datos

### Mapeo

|  |  |
| --- | --- |
| **TARIFA** | |
| **evento** | **contacto** |

|  |  |
| --- | --- |
| **INVITACION** | |
| **eventoC:\Users\i\Desktop\llave.png** | **contactoC:\Users\i\Desktop\llave.png** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CLIENTE** | | | | |
| **idC:\Users\i\Desktop\llave.png** | **nombre** | **apellidos** | **correo** | **usuario** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **EVENTO** | | | | | | |
| **idC:\Users\i\Desktop\llave.png** | **nombre** | **direccion** | **fechainicio** | **fechafin** | **cancelado** | **precio** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CONTACTO** | | | | | |
| **IDC:\Users\i\Desktop\llave.png** | **nombres** | **apellidos** | **correo** | **precio** | **baja** |

## Diseño físico de la base de datos

### Tablas de volumen

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TARIFA** | | | | | |
| **ATRIBUTOS** | **LLAVE** | **TIPO DE DATOS** | **AMPLITUD** | **NULO** | **DESCRIPCIÓN** |
| **evento** |  | Entero | 32 bits | NO | evento |
| **contacto** |  | Entero | 32 bits | NO | contacto |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **INVITACIÓN** | | | | | |
| **ATRIBUTOS** | **LLAVE** | **TIPO DE DATOS** | **AMPLITUD** | **NULO** | **DESCRIPCIÓN** |
| **eventoC:\Users\i\Desktop\llave.png** | PK,FK | Entero | 32 bits | NO | Id de evento |
| **contactoC:\Users\i\Desktop\llave.png** | PK,FK | Entero | 32 bits | NO | ID de contacto |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CLIENTE** | | | | | |
| **ATRIBUTOS** | **LLAVE** | **TIPO DE DATOS** | **AMPLITUD** | **NULO** | **DESCRIPCIÓN** |
| **idC:\Users\i\Desktop\llave.png** | PK | Entero | 32 bits | NO | ID del cliente |
| **nombres** | ░░░░░ | alfanumerico | 50 caracteres | NO | Nombre del cliente |
| **apellidos** | ░░░░░ | alfanumerico | 50 caracteres | NO | Apellidos del cliente |
| **correo** | ░░░░░ | Alfanumerico | 50 caracteres | NO | Correo del cliente |
| **usuario** | ░░░░░ | Alfanumerico | 50 caracteres | NO | Nombre de usuario |
| **pass** | ░░░░░ | Alfanumerico | 100 caracteres | NO | Contraseña del cliente |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **EVENTO** | | | | | |
| **ATRIBUTOS** | **LLAVE** | **TIPO DE DATOS** | **AMPLITUD** | **NULO** | **DESCRIPCIÓN** |
| **idC:\Users\i\Desktop\llave.png** | PK | Entero | 32 bits | NO | ID de evento |
| **nombre** | ░░░░░ | alfanumerico | 50 caracteres | NO | Nombre de evento |
| **direccion** | ░░░░░ | alfanumerico | 50 caracteres | NO | Dirección del evento |
| **Fechainicio** | ░░░░░ | long | 64 bits | NO | Fecha de inicio del evento |
| **fechafin** | ░░░░░ | long | 64 bits | NO | Fecha final del evento |
| **cancelado** | ░░░░░ | bit | 1 bit | NO | Estado del evento |
| **precio** | ░░░░░ | decimal | 16 enteros, 2 décimas | NO | Precio del evento |
| **idc** | FK | Entero | 32 bits | NO | Id del cliente |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CONTACTO** | | | | | |
| **ATRIBUTOS** | **LLAVE** | **TIPO DE DATOS** | **AMPLITUD** | **NULO** | **DESCRIPCIÓN** |
| **idC:\Users\i\Desktop\llave.png** | PK | Entero | 32 bits | NO | ID del contacto |
| **nombres** | ░░░░░ | alfanumerico | 50 caracteres | NO | Nombre del contacto |
| **apellidos** | ░░░░░ | alfanumerico | 50 caracteres | NO | Apellidos del contacto |
| **correo** | ░░░░░ | Alfanumerico | 50 caracteres | NO | Correo del contacto |
| **precio** | ░░░░░ | decimal | 16 enteros, 2 décimales | NO | Precio por ese contacto |
| **baja** | ░░░░░ | bit | 1 bit | NO | Estado del contacto |
| **idc** | FK | Entero | 32 bits | NO | Id del cliente |

## Diagramas de secuencia

### Gestionar contacto

### Gestionar cliente



### Gestionar evento

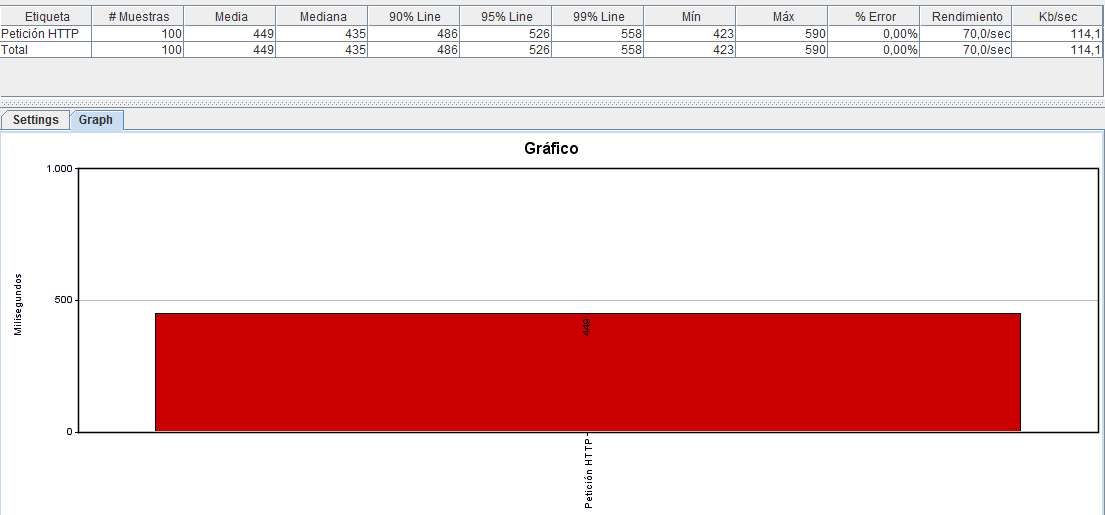


### Administrar tarifa

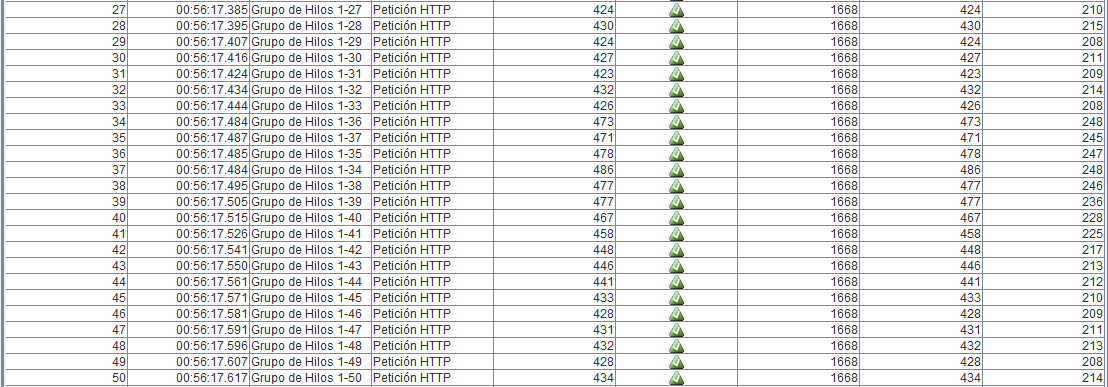
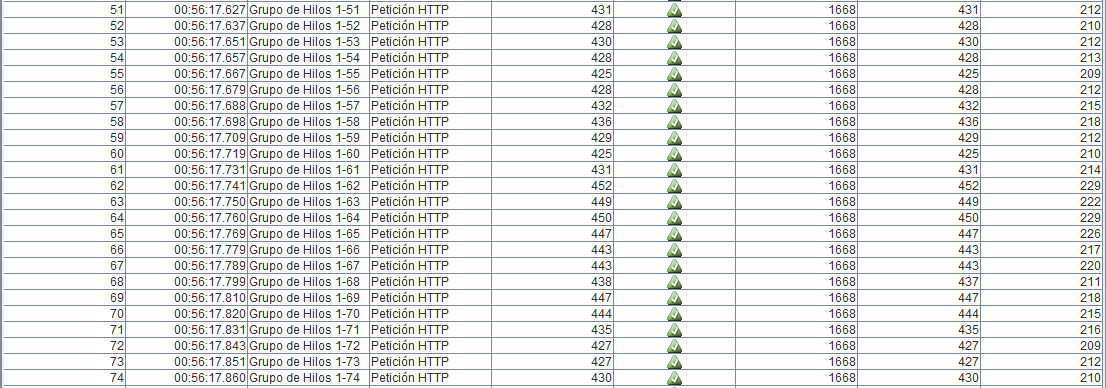
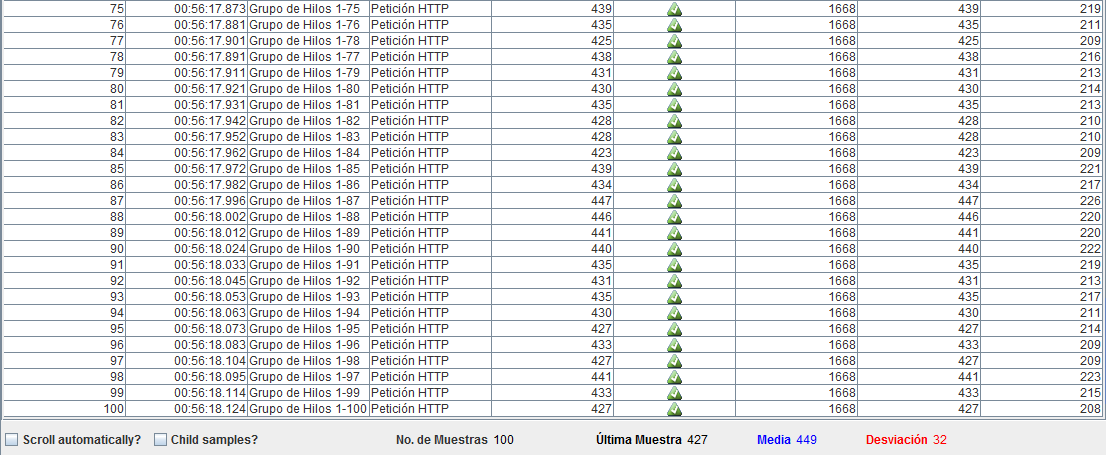
# FASE DE PRUEBAS

# Pruebas

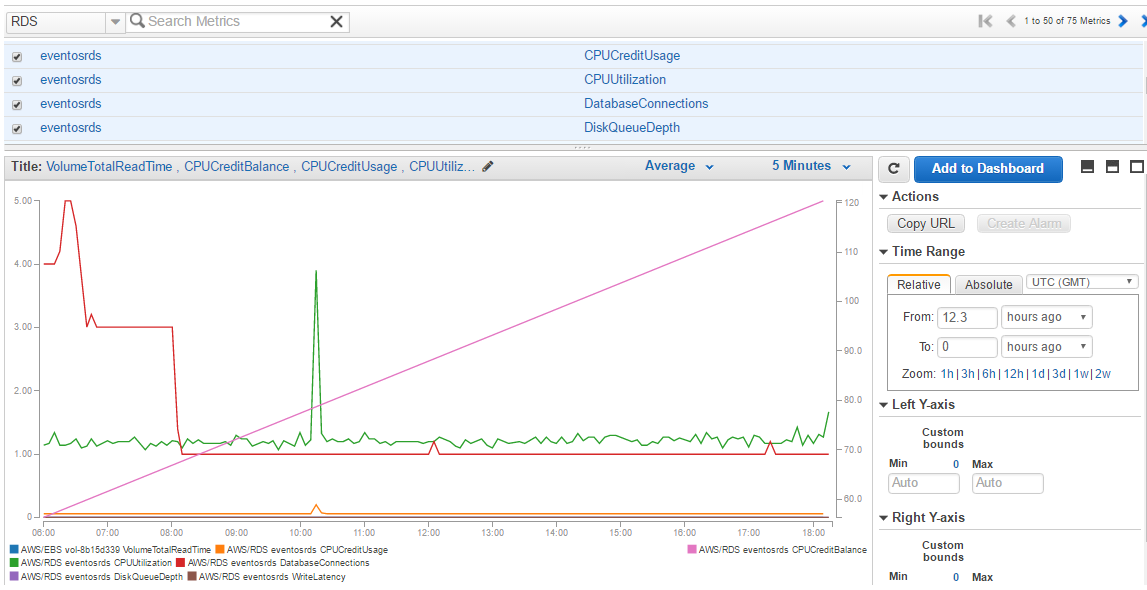
## Pruebas de rendimiento con JMeter

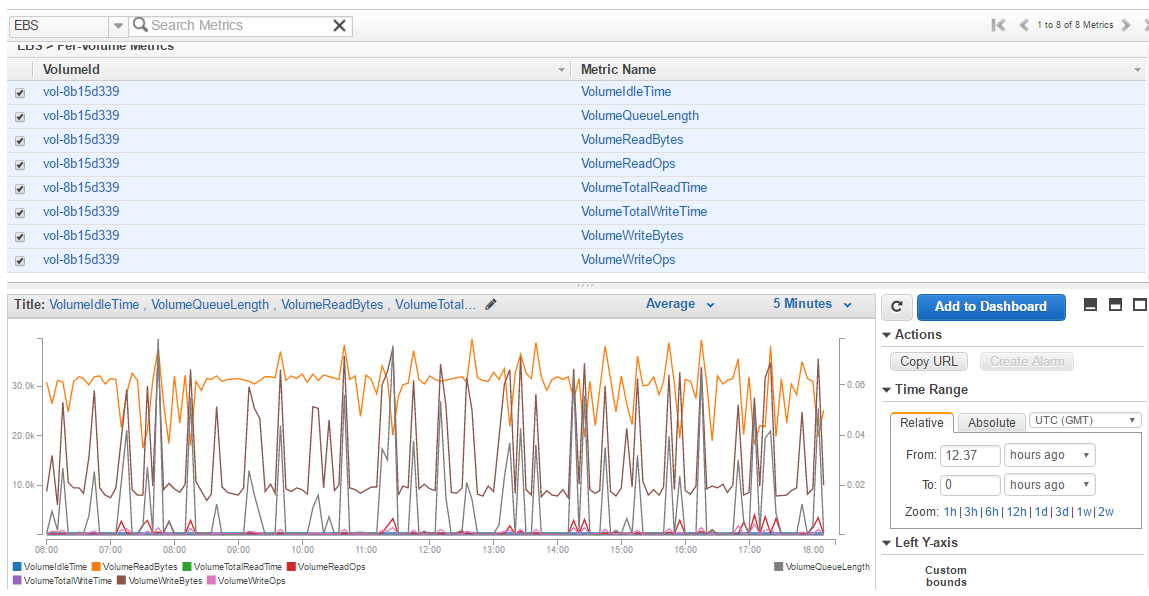


Muestreo hecho sobre 100 peticiones http

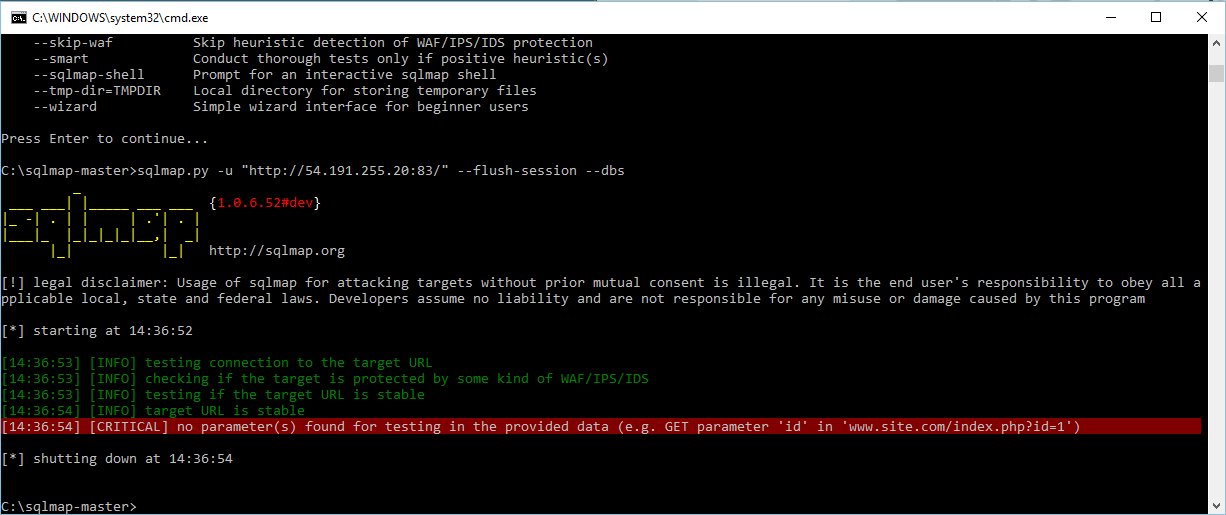


## Pruebas de eficiencia con Amazon CloudWath



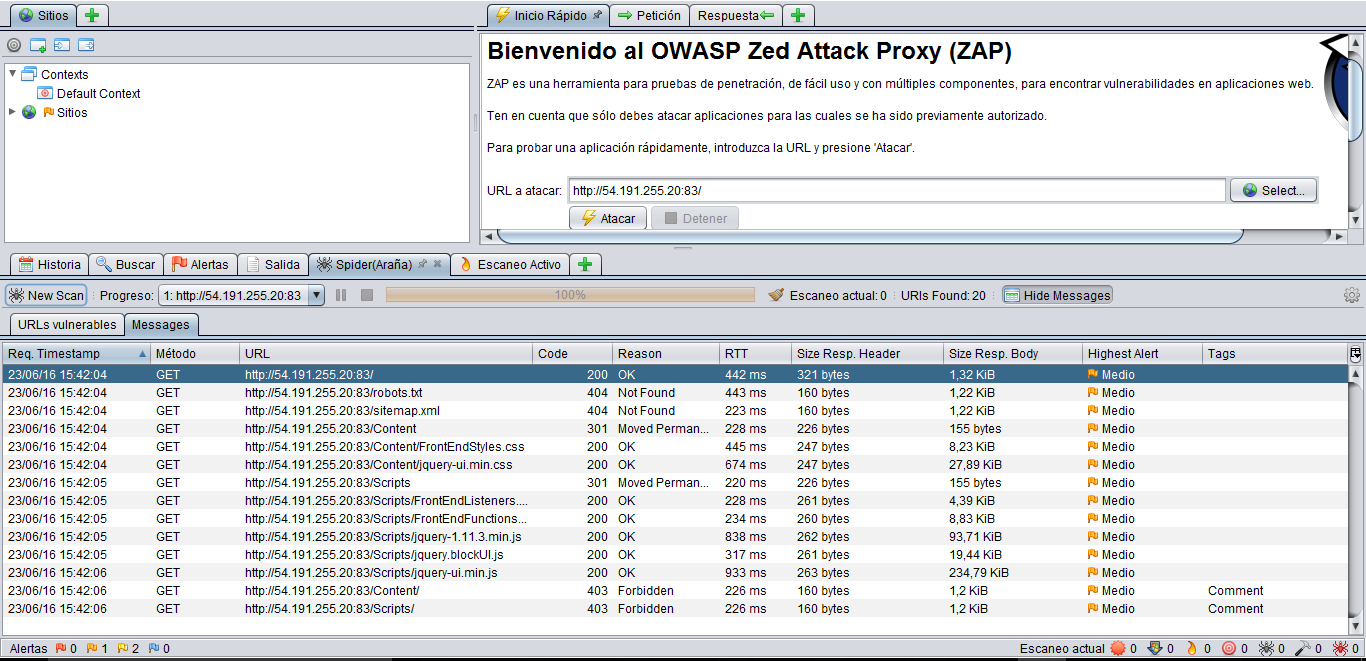


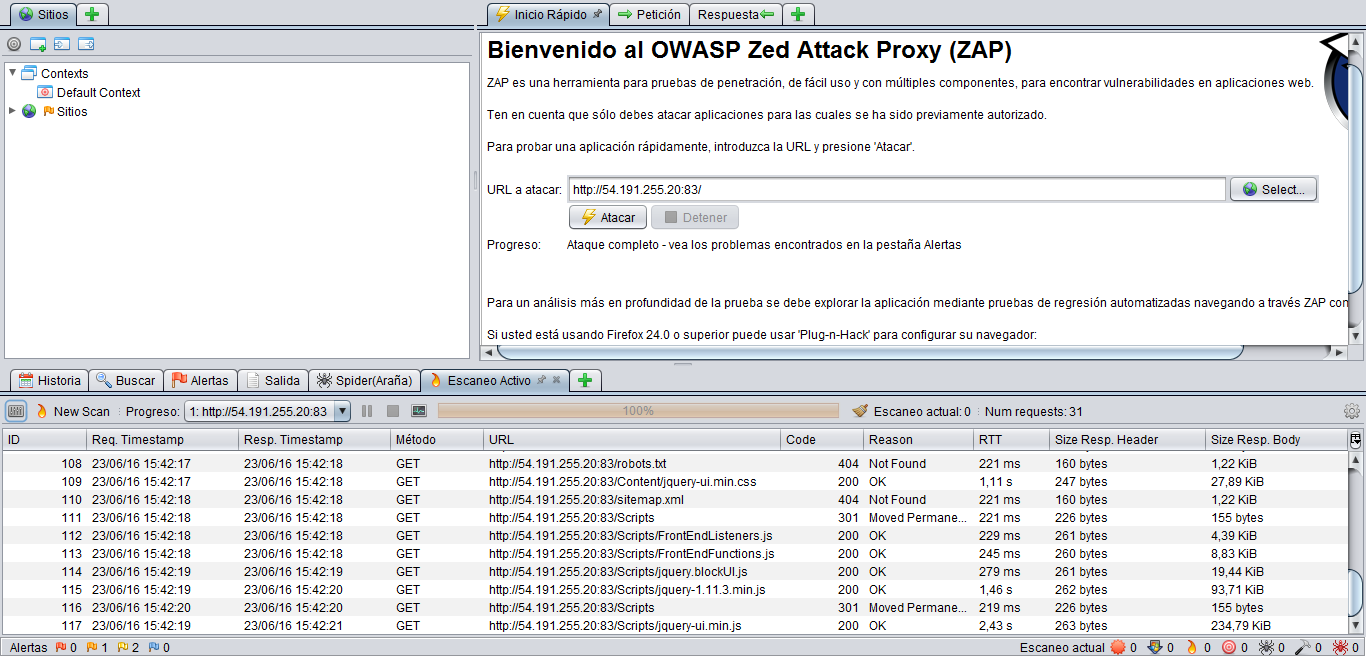
## Pruebas de seguridad

Utilizando SQLmap para realizar ataques SQL Inyection

Se puede observar que por la protección a nivel WAF, la aplicación es segura a ataques SQL inyection

## Prueba de seguridad utilizando ZAP, para ataques contra bots, scripts, querys



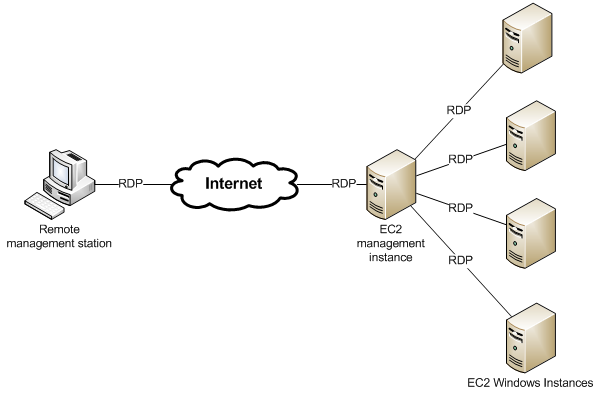


# HERRAMIENTAS

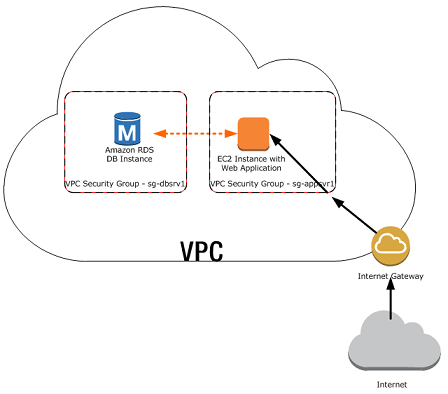
## Amazon EC2 (Elastic Compute Cloud)

Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona capacidad de cómputo con tamaño modificable en la cloud. Está diseñado para facilitar a los desarrolladores el [cloud computing](https://aws.amazon.com/es/what-is-cloud-computing/) escalable basado en web.

La sencilla interfaz de servicios web de Amazon EC2 permite obtener y configurar la capacidad con una fricción mínima. Proporciona un control completo sobre los recursos informáticos y puede ejecutarse en el entorno informático acreditado de Amazon. Amazon EC2 reduce el tiempo necesario para obtener y arrancar nuevas instancias de servidor en cuestión de minutos, lo que permite escalar rápidamente la capacidad, ya sea aumentándola o reduciéndola, según cambien sus necesidades. Amazon EC2 cambia el modelo económico de la informática, ya que solo tendrá que pagar por la capacidad que realmente utilice. Amazon EC2 proporciona a los desarrolladores las herramientas necesarias para crear aplicaciones resistentes a errores y para aislarse de los casos de error más comunes.



## Amazon RDS (Relational Database Service)

Con Amazon Relational Database Service (Amazon RDS), es sencillo configurar, utilizar y escalar una base de datos relacional en la cloud. Proporciona capacidad rentable y de tamaño modificable y, al mismo tiempo, administra las tediosas tareas de administración de la base de datos, lo que le permite centrarse en sus aplicaciones y en su negocio. Amazon RDS le permite elegir entre seis motores de bases de datos conocidos: Amazon Aurora, Oracle, Microsoft SQL Server, PostgreSQL, MySQL y MariaDB.

## Amazon WAF (WEB APPLICATION FIREWALL)

AWS WAF es un firewall web que ayuda a proteger sus aplicaciones web de ataques web habituales que podrían afectar a la disponibilidad de la aplicación, comprometer la seguridad o consumir excesivos recursos. AWS WAF permite controlar el tráfico que desea habilitar o bloquear en su aplicación web mediante la definición de reglas de seguridad web personalizables. Puede usar AWS WAF para crear reglas personalizadas que bloquean patrones de ataque comunes, como la inyección de código SQL y los scripts de sitios, así como reglas diseñadas para su aplicación específica. Las nuevas reglas se pueden implementar en cuestión de minutos, con lo que puede responder rápidamente ante cambios en los patrones de tráfico. Además, AWS WAF incluye una completa API que puede utilizar para automatizar la creación, la implementación y el mantenimiento de reglas de seguridad en la web.

**Mayor protección ante ataques en la web**

AWS WAF protege las aplicaciones web de ataques al filtrar el tráfico en función de las reglas que cree. Por ejemplo, puede filtrar las solicitudes web por direcciones IP, encabezados HTTP o cadenas URI, lo que permite bloquear patrones de ataque comunes, como la inyección de código SQL y los scripts entre sitios.

**Seguridad que se integra con el modo en que desarrolla sus aplicaciones**

Todas las características de AWS WAF se pueden configurar usando la API de AWS WAF o la consola de administración de AWS. Esto permite definir reglas específicas a la aplicación que incrementan la seguridad web a medida que desarrolla su aplicación. De este modo, puede incorporar la seguridad web en numerosos puntos de la cadena de desarrollo, desde el desarrollador que escribe el código en primera instancia al ingeniero de operaciones de desarrollo que implementa el software y los expertos en seguridad que realizan una auditoría.

**Facilidad de implementación y mantenimiento**

AWS WAF es sencillo de implementar, protege cualquier aplicación implementada en el servicio de entrega de contenido de Amazon CloudFront y no requiere implementar ningún software adicional. Puede definir las reglas a nivel central y reutilizarlas para todas las aplicaciones web que deba proteger.

**Visibilidad del tráfico web mejorada**

Puede configurar AWS WAF para que monitorice solamente las solicitudes que coincidan con sus criterios de filtros. AWS WAF ofrece visibilidad del tráfico web en tiempo casi real, que puede utilizar para crear reglas o alertas nuevas en Amazon CloudWatch.

**Protección rentable para aplicaciones web**

Con AWS WAF, paga únicamente por lo que utiliza. AWS WAF constituye una oferta de autoservicio personalizable cuyo precio depende de la cantidad de reglas que implemente y las solicitudes web que reciba su aplicación web. No se requieren pagos mínimos ni compromisos iniciales.

## Amazon CloudWatch

Amazon CloudWatch es un servicio de monitorización de los recursos de la nube de AWS y de las aplicaciones que se ejecutan en AWS. Puede utilizar Amazon CloudWatch para recopilar y realizar el seguimiento de métricas y logs, establecer alarmas y reaccionar automáticamente a los cambios en sus recursos AWS. Amazon CloudWatch puede monitorizar recursos de AWS como, por ejemplo, instancias de Amazon EC2, tablas de Amazon DynamoDB e instancias de base de datos de Amazon RDS, así como métricas personalizadas generadas por las aplicaciones y los servicios, y los logs generados por las aplicaciones. Puede utilizar Amazon CloudWatch para obtener visibilidad para todo el sistema sobre la utilización de recursos, el desempeño de las aplicaciones y el estado de funcionamiento. Puede usar esta información para iniciar y mantener la ejecución de la aplicación sin problemas.

**Monitorización de Amazon EC2**

Consulte métricas del uso de CPU, transferencia de datos y actividad de uso del disco desde las instancias de Amazon EC2 (monitorización básica) sin gastos adicionales. Por un cargo adicional, CloudWatch proporciona monitorización detallada de las instancias EC2 con mayor resolución y agregación de métricas. No es necesario instalar software adicional.

**Benefit\_Simple\_Orange**

Monitorización de otros recursos de AWS

Monitorice las métricas de las tablas de Amazon DynamoDB, los volúmenes de Amazon EBS, las instancias de base de datos de Amazon RDS, los flujos de trabajo de Amazon Elastic MapReduce, Elastic Load Balancers, las colas de Amazon SQS, los temas de Amazon SNS y mucho más sin gastos adicionales. No es necesario instalar software adicional.

**Monitorización de métricas personalizadas**

Envíe métricas personalizadas generadas por las aplicaciones propias a través de una sencilla solicitud de API y deje que Amazon CloudWatch se encargue de monitorizarlas. Puede enviar y almacenar métricas importantes para el desempeño operativo de la aplicación con el fin de ayudarle a solucionar problemas y detectar tendencias.

**Monitorización y almacenamiento de logs**

Puede utilizar CloudWatch Logs para monitorizar sistemas y aplicaciones y solucionar problemas relacionados, para lo que debe usar los archivos de∙log personalizados, archivos de la aplicación y archivos del sistema existentes. Puede enviar los archivos de log personalizados, de la aplicación y del sistema existentes a CloudWatch Logs para monitorizarlos prácticamente en tiempo real. Esto le puede ayudar a comprender y operar mejor los sistemas y las aplicaciones, y puede almacenar los logs mediante un almacenamiento de alta durabilidad y bajo costo para su posterior acceso.

**Definición de alarmas**

Establezca alarmas en cualquiera de las métricas para enviarle notificaciones o adoptar otras acciones automáticas. Por ejemplo, cuando una métrica específica de Amazon EC2 cruza el umbral de alarma, puede utilizar Auto Scaling para añadir o eliminar instancias EC2 de forma dinámica o para enviarle una notificación.

**Visualización de gráficos y estadísticas**

Los paneles de Amazon CloudWatch le permiten crear gráficos reutilizables de recursos de AWS y métricas personalizadas, de modo que pueda monitorizar el estado operativo e identificar problemas de un vistazo. Los datos de las métricas se guardan durante dos semanas, lo que le permite consultar datos muy actuales y también datos del historial. Amazon CloudWatch puede cargar todas las métricas en la cuenta a efectos de búsquedas y gráficos con la consola de administración de AWS. Esto incluye logs, métricas de recursos de AWS y las métricas de las aplicaciones que proporcione.

**Monitorización y reacción ante cambios en los recursos**

CloudWatch Events proporciona un flujo de eventos que describe los cambios en sus recursos de AWS. Es fácil crear flujos de trabajo que realicen acciones automáticamente, como invocar una función de AWS Lambda, cuando se produzca un evento de interés.

## JMETER

**JMeter** es un proyecto de [Apache](https://es.wikipedia.org/wiki/Apache_Software_Foundation) que puede ser utilizado como una herramienta de prueba de carga para analizar y medir el desempeño de una variedad de servicios, con énfasis en [aplicaciones web](https://es.wikipedia.org/wiki/Aplicaci%C3%B3n_web).

JMeter puede ser usado como una herramienta de pruebas unitarias para [conexiones de bases de datos con JDBC](http://jmeter.apache.org/usermanual/build-db-test-plan.html), [FTP](http://jmeter.apache.org/usermanual/build-ftp-test-plan.html), [LDAP](http://jmeter.apache.org/usermanual/build-ldap-test-plan.html), [Servicios web](http://jmeter.apache.org/usermanual/build-ws-test-plan.html),[JMS](http://jmeter.apache.org/usermanual/build-jms-topic-test-plan.html), [HTTP](http://jmeter.apache.org/usermanual/build-web-test-plan.html) y conexiones TCP genéricas. JMeter puede también ser configurado como un [monitor](http://jmeter.apache.org/usermanual/build-monitor-test-plan.html), aunque es comúnmente considerado una solución ad-hoc respecto de soluciones avanzadas de monitoreo.

Mientras que JMeter es clasificado como una herramienta de "generación de carga", no es una descripción completa de la herramienta. JMeter soporta aserciones para asegurarse que los datos recibidos son correctos, por cookies de hilos, configuración de variables y una variedad de reportes.

## Spawner

Es una herramienta que permite poblar bases de datos con el fin de realizar pruebas de Rendimiento, capacidad de almacenamiento y otros tipos de testing para bases de datos. Esta herramienta posee la capacidad de generar scripts sql, mysql entre miles y miles de datos con un diccionario y métricas personalizables para los usuarios

## GitHub

GitHub es una (plataforma de desarrollo colaborativo) para alojar proyectos utilizando el sistema de control de versiones Git. Utiliza el framework Ruby on Rails por GitHub, Inc. (anteriormente conocida como Logical Awesome). Desde enero de 2010, GitHub opera bajo el nombre de GitHub, Inc.

## SourceTree

Sourcetree, como ya comentamos, es probablemente uno de los mejores clientes para gestionar repositorios Git o Mercurial (hasta ahora sólo en Mac). Ideal para los principiantes teniendo a mano los comandos más comunes: create, clone, commit, push, pull o merge. Todos disponibles en un par de clicks y guiados por un entorno gráfico que siempre ayuda. Podemos conectarnos a repositorios locales de Git o Mercurial y remotos como Github o Bitbucket.

Pero no deja de ser una herramienta para usuarios avanzados de Git para revisar todos los cambios de los repositorios, manejar de forma sencilla los distintos branch de desarrollo o visualizar claramente cada modificación en los gráficos de cada rama. Sin olvidar muchos comandos como rebase, stash, shelve,.. Por supuesto, los harduser de git pueden lanzar su línea de comandos y tenerlo como apoyo gráfico.

SourceTree es una herramienta bastante eficaz para manejarse por repositorios del trabajo en los que varios desarrolladores trabajan de forma simultanea y poder aplicar de la forma eficiente el modelo de desarrollo propuesto por Git-flow o Hg-flow.

## SQLMap

sqlmap es una herramienta de pruebas de penetración de código abierto que automatiza el proceso de detectar y explotar los errores de inyección SQL y toma de carga de los servidores de bases de datos. Viene con un potente motor de detección, muchas características de nicho para el probador de penetración máxima y una amplia gama de interruptores que duran de toma de huellas dactilares de base de datos, ir a buscar a través de datos de la base de datos, para acceder al sistema de archivos subyacente y ejecutar comandos en el sistema operativo a través de fuera conexiones de banda.

Características:

Soporte completo para MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB y HSQLDB sistemas de gestión de base de datos.

Soporte completo para seis técnicas de inyección SQL: ciegos basado en booleano, ciegos basado en el tiempo, basado en el error, apilados, consultas basadas en consulta UNION y fuera de banda .

Apoyo a conectar directamente a la base de datos sin pasar a través de una inyección SQL, proporcionando credenciales del DBMS, dirección IP, el puerto y el nombre de la base de datos.

Soporte para enumerar los usuarios, los hashes de contraseñas, privilegios, roles, bases de datos, tablas y columnas .

El reconocimiento automático de formatos de hash de la contraseña y el apoyo para la formación de grietas usando un ataque basado en diccionario .

Apoyar a volcar tablas de bases en su totalidad, una serie de entradas o columnas específicas como por la elección del usuario. El usuario también puede elegir para volcar sólo un rango de caracteres de entrada de cada columna.

Apoyar a buscar nombres de bases de datos específicas, tablas específicas a través de todas las bases de datos o columnas específicas a través de las tablas de las bases de datos ' . Esto es útil, por ejemplo, para identificar las tablas que contienen las credenciales de aplicación personalizados donde los nombres de las columnas relevantes 'contienen cadena como nombre y pase.

Apoyo a descargar y cargar cualquier archivo desde el servidor de base de datos del sistema de archivos subyacente cuando el software de base de datos es MySQL, PostgreSQL o Microsoft SQL Server.

Apoyo a ejecutar comandos arbitrarios y recuperar su salida estándar en el servidor de base de datos de sistema operativo cuando el software de base de datos es MySQL, PostgreSQL o Microsoft SQL Server subyacente.

Apoyo a establecer una conexión TCP con estado fuera de la banda entre la máquina atacante y el servidor de base de datos del sistema operativo subyacente. Este canal puede ser un símbolo del sistema interactivo, una sesión Meterpreter o una sesión de interfaz gráfica de usuario (VNC) a elección del usuario.

El apoyo a una escalada de privilegios de usuario proceso de base de datos ' a través de Meterpreter de Metasploit getSystem comando.

## ZAP (Zed Attack Proxy)

La OWASP Zed Attack Proxy (ZAP) es una de las herramientas de seguridad gratuita más populares del mundo y se mantiene activa por cientos de voluntarios internacionales Puede ayudar a encontrar automáticamente las vulnerabilidades de seguridad en sus aplicaciones web mientras está desarrollando y probando sus aplicaciones. También es una gran herramienta para pentesters experimentados a utilizar para las pruebas de seguridad manual.

las pruebas de seguridad de software es el proceso de evaluación y ensayo de un sistema para descubrir los riesgos de seguridad y vulnerabilidades del sistema y sus datos. No hay una terminología universal, pero para nuestros propósitos, definimos las evaluaciones como el análisis y descubrimiento de vulnerabilidades sin tratar de realidad explotar esas vulnerabilidades. Definimos las pruebas como el descubrimiento y explotación de intento vulnerabilidades. Las pruebas de seguridad se rompe a menudo fuera, algo arbitrariamente, según sea el tipo de la vulnerabilidad que se investiga o el tipo de prueba se está realizando. Una ruptura común es:

• Evaluación de la vulnerabilidad - El sistema se escanean y se analizaron para la seguridad cuestiones.

• Pruebas de Penetración - El sistema se somete a análisis y atacar desde simulado atacantes maliciosos.

• Prueba de tiempo de ejecución - El sistema se somete a análisis y pruebas de seguridad de un usuario final.

• Revisión de código - El código del sistema se somete a una revisión y un análisis detallado mirando Específicamente para las vulnerabilidades de seguridad.Tenga en cuenta que la evaluación de riesgos, que comúnmente se enumeran como parte de las pruebas de seguridad, no es incluido en esta lista. Esto se debe a una evaluación del riesgo no es en realidad una prueba sino más bien El análisis de la percepción de la gravedad de los diferentes riesgos (seguridad de software, la seguridad personal, de seguridad de hardware, etc.) y las medidas de mitigación de esos riesgos.Más sobre las pruebas de penetración

Pruebas de Penetración (pentesting) se lleva a cabo como si el probador era un malévolo externo atacante con el objetivo de entrar en el sistema y, o bien el robo de datos o la realización de algún tipo de ataque de denegación de servicio. Pentesting tiene la ventaja de ser más preciso, ya que tiene un menor número de falsos positivos (Resultados que informan de una vulnerabilidad que no está realmente presente), pero puede ser mucho tiempo para correr.

Pentesting también se utiliza para probar los mecanismos de defensa, verificar los planes de respuesta, y confirmar la adhesión política de seguridad. pentesting automatizado es una parte importante de la validación de integración continua. Ayuda a descubrir nuevas vulnerabilidades, así como las regresiones de vulnerabilidades anteriores en una entorno que cambia rápidamente, y para los que el desarrollo puede ser altamente colaborativa y distribuida.

El Proceso de Pentesting

Tanto pentesting manual y automatizado se utilizan, a menudo en combinación, para probar todo lo desde los servidores, a las redes, a los dispositivos, a los puntos finales. Este documento se centra en la Web pentesting aplicación o sitio web.

Pentesting por lo general sigue estas etapas:

• Explorar - El probador intenta aprender sobre el sistema que se está probando. Esto incluye Tratando de determinar qué software está en uso, lo que los puntos finales de existir, lo que son parches Instalado, etc. También incluye buscar el sitio para el contenido oculto, conocida

Vulnerabilidades y otros indicios de debilidad.

• Ataque - El probador intenta explotar las vulnerabilidades se sabe o sospecha demuestran que existen.

• Informe - Los informes probador copia de los resultados de sus pruebas, incluyendo el vulnerabilidades, la forma en que los explotaron y la dificultad de la explotación eran, y la gravedad de la explotación.

Objetivos pentesting

El objetivo final de pentesting es la búsqueda de vulnerabilidades de modo que estas vulnerabilidades pueden ser abordados. También puede verificar que un sistema no es vulnerable a una clase conocida o defecto específico; o, en el caso de las vulnerabilidades que han sido reportados como fijos, verificar que el sistema ya no es vulnerable a ese defecto.

La introducción de ZAP Ataque Zed Proxy (ZAP) es una herramienta de código abierto libre de pruebas de penetración se mantiene en el marco del Proyecto de Seguridad de aplicaciones web abierta (OWASP). ZAP está diseñado específicamente para el ensayo de aplicaciones web y es a la vez flexible y extensible. En su esencia, ZAP es lo que se conoce como un "proxy de la interceptación." Se encuentra entre el probador de navegador y la aplicación web para que pueda interceptar e inspeccionar los mensajes enviados entre navegador y aplicaciones web, modificar el contenido si es necesario, y luego reenviar los paquetes en el destino. En esencia, ZAP se puede utilizar como un "hombre en el medio", pero también puede ser utilizado como una aplicación independiente y como un proceso demonio. Si hay otro proxy de red que ya están en uso, como en muchos entornos corporativos, ZAP puede ser configurado para conectarse a dicho proxy. ZAP proporciona la funcionalidad para una amplia gama de niveles de habilidad - de los desarrolladores, a los probadores a nuevos las pruebas de seguridad, a los especialistas de pruebas de seguridad. ZAP tiene versiones para cada sistema operativo principal y Cargador de muelle, por lo que no están atados a un solo sistema operativo. La funcionalidad adicional está disponible gratuitamente a partir de una variedad de complementos en el mercado ZAP, accesibles desde el cliente de ZAP.