Burp Suite Professional

Burp Suite es una plataforma integrada para la realización de las pruebas de seguridad de aplicaciones web. Sus diversas herramientas funcionan perfectamente juntos para apoyar el proceso de prueba, a partir de la cartografía y el análisis iniciales de la superficie de ataque de una aplicación, hasta la búsqueda y explotación de vulnerabilidades de seguridad.

Burp Suite le da un control completo, lo que le permite combinar avanzadas técnicas manuales con la automatización de estado-of-the-art, para hacer su trabajo más rápido, más eficaz y más divertido.

Burp Suite contiene los siguientes componentes clave :

- Un Proxy intercepta, lo que le permite inspeccionar y modificar el tráfico entre el navegador y la aplicación de destino.
- Una araña con reconocimiento de aplicaciones, para el rastreo de contenido y funcionalidad.
- Un escáner de aplicaciones web avanzadas para automatizar la detección de numerosos tipos de vulnerabilidad.
- Una herramienta de intrusión, para realizar poderosos ataques personalizados de encontrar y explotar vulnerabilidades inusuales.
- Una herramienta de repetidor, para manipular y volver a enviar peticiones individuales.
- Una herramienta secuenciador, para probar la aleatoriedad de las credenciales de sesión.
- La capacidad de guardar su trabajo y reanudar el trabajo más tarde.
- Extensibilidad, lo que le permite escribir fácilmente tus propios plugins, para realizar tareas complejas y personalizadas muy dentro de Burp.

Bueno ahora vamos a dar una descripción profunda y la introducción de probar y atacar las vulnerabilidades SQL en sitios web y aplicaciones con el conjunto de herramientas Burp Suite. La versión gratuita que voy a explicar hoy en día es una herramienta especialmente gratis para los entusiastas de la seguridad, y tener la versión Pro con características aún más de lo que se cubre hoy por pentester serio o profesional.

Este artículo sólo pretende dar una introducción a esta gran herramienta, no es una guía completa y

plena se basa puramente en mi comprensión de la misma a partir de pruebas recientes (ten cuidado es un poco larga e intensa imagen). Yo personalmente tuve un momento difícil llegar a conocer la Suite Haga eructar y se han acercado a la herramienta varias veces en el pasado, sólo para ser intimidados por ella y la empujó fuera para una fecha posterior. La documentación aportada por el equipo Burp Suite es útil, pero también falta en muchas áreas, en mi opinión, así que pensé que me gustaría crear mi propia guía para ayudar a otros. Esta herramienta es más orientado hacia los usuarios intermedios y avanzados, y le ayudará a llevar su juego al siguiente nivel.

Requisitos:

- Java v1.5 + instalado (se recomienda utilizar la última JRE).
- Asegúrese de que también puede localizar y ejecutar el archivo Brain.dll..=)
- Copia del Burp Suite, disponible de forma gratuita aquí:

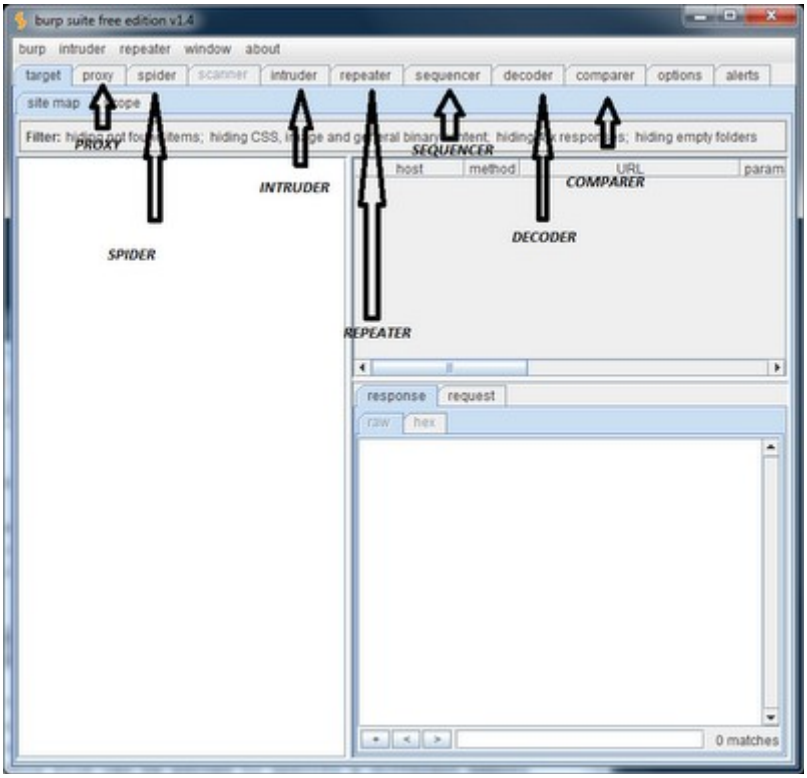
Burp Suite : **http://portswigger.net/burp/download.html**

Primeros pasos:

Usted tendrá que asegurarse de que ha cumplido con los requisitos mencionados anteriormente, sólo tiene que descargar ambos. Instalar el Java y descomprimir la Suite Haga eructar a la ubicación que desee ejecutar. Con el fin de obtener Burp Suite de iniciado en la mayoría de los ordenadores sólo hacer doble clic en el archivo ejecutable jar, si eso no funciona para usted puede ejecutar escribiendo esto en la línea de comandos o terminal.:

Mandato : java-jar burpsuite_v1.4.jar

Usted será recibido con la GUI Burp Suite una vez hecho esto, debería ser algo como esto:



El conjunto de herramientas se divide en una estructura de pestañas con cada ficha realizando un servicio diferente, prueba o función. Burp Suite y sus herramientas le permiten realizar peticiones manuales y / o automatizados para escanear rápidamente, enumerar, analizar, atacar y explotar sitios web y sus aplicaciones. Esto se facilita a través de su estructura de pestañas que te permite pasar los resultados o se centran elemento de un conjunto de herramientas directamente a otro que le permite construir sobre la marcha. Es la culminación de todos ellos que hacen a Burp Suite un poderoso conjunto de herramientas para tener en su arsenal, pero antes de empezar voy a presentar a cada uno de los instrumentos dentro del conjunto de herramientas de Burp Suite y lo que hacen. Entonces a continuación voy a mostrar usted algunos ejemplos en acción. Aquí está un rápido desglose de las herramientas incluidas y qué acciona cada una.

Opciones :

- En primer lugar, tiene un **PROXY** local interceptando, esta le permite capturar el tráfico entre el navegador y el sitio de destino. A continuación, puede inspeccionar el tráfico capturado y pasarlo a otras herramientas de la suite para su posterior análisis y pruebas.
- El reconocimiento de aplicaciones **SPIDER**. Esta herramienta se puede utilizar para rastrear sitios de destino a revelar el contenido del sitio, detrás de la estructura y otras funcionalidades.
- La herramienta **REPETIDOR** le permite reenviar manualmente las solicitudes HTTP individuales. Esta es una herramienta muy útil ya que le permite realizar cambios rápidos sobre la marcha y ver cómo responde el servidor.
- La herramienta **INTRUDER** es otro que se centrará en la actualidad. Esta herramienta le permite realizar cargas a medida para ser utilizados en el ataque a la meta. Es altamente personalizable y limitado sólo por su imaginación.
- La herramienta **SECUENCIADOR** es útil si desea probar la aleatoriedad de las credenciales de sesión. Esto puede ser usado para descubrir la entropía débil que podría conducir a algo así como la explotación de Sesión Jacking o un tipo similar de escenario. No voy a estar cubriendo esto hoy, pero usted debería ser capaz de recoger los desechos de este tutorial básico y luego empezar a probar por su cuenta.
- La herramienta **DECODER** es otra útil para tener alrededor, ya que puede ser utilizado para decodificar material que usted puede venir a través de su prueba o también puede ser utilizado para realizar tareas comunes como la conversión de texto a HEX. Esto vale la pena jugar con como yo no lo va a cubrir aquí hoy, pero es sencillo y bastante simple de recolección.
- La herramienta **COMPARTER** está diseñado para permitir llevar a cabo la comparación visual de cualquiera de los dos artículos.

Version PRO:

- Incluye una aplicación web avanzado escáner de vulnerabilidades que es muy precisa en la detección de todo tipo de vulnerabilidades que podrían ser explotadas.
- Permite guardar y restaurar en caso de que deje paso a mediados.
- También tiene algunos adicionales de búsqueda, el descubrimiento de contenido y las características de programación de tareas que no están disponibles en la versión gratuita.

- Retroalimentación general en la calle es que vale la pena si te lo puedes permitir

Aceptar lo que le da una idea básica de lo que cada herramienta es, ahora voy a tratar de mostrar algunos ejemplos de ellos y la forma de ponerlos a trabajar a su ventaja. Voy a mostrar algunos ejemplos relacionados con las pruebas y la explotación de las vulnerabilidades de inyección SQL que pueden ser fácilmente modificados para probar otros escenarios, aquí va.....xDD!!

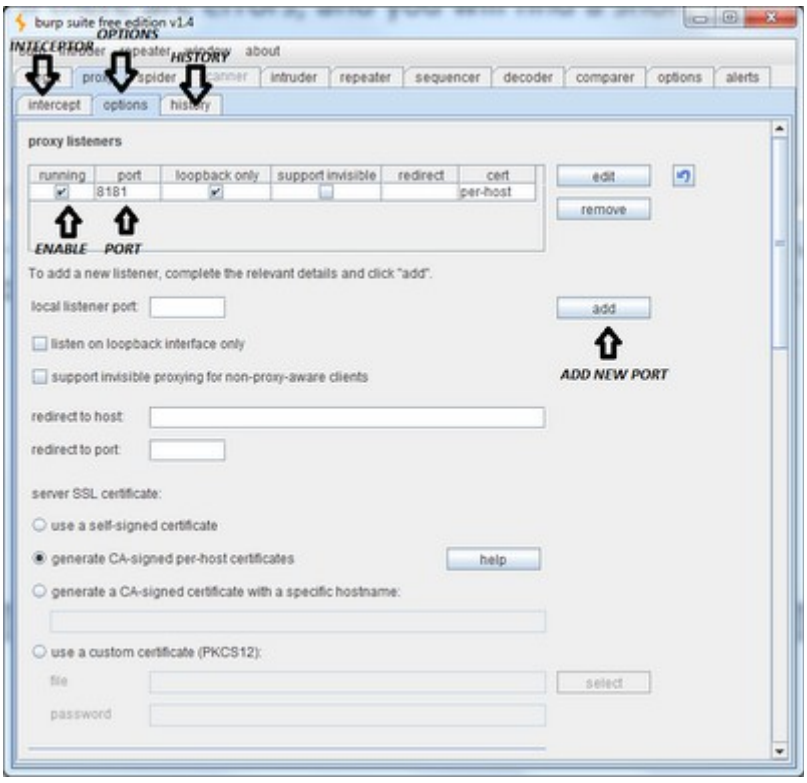
Requisitos:

- Objetivo del sitio para probar.
- Activar Burp Suite y hacerlo correr.

Una vez se abre la Burp Suite, usted puede navegar a la pestaña de configuración de proxy para obtener las cosas que podamos comenzar a interceptar el tráfico y comenzar nuestras pruebas.

Usted tendrá que hacer clic en **PROXY**, a continuación, haga clic en la ficha Opciones. Aquí es donde podemos configurar nuestro puerto del servidor proxy que se utilizará para nuestras pruebas. En mi caso yo ya tengo un servidor Apache que se ejecuta en el puerto 8080 por lo que se necesita para cambiar el puerto 8181, si usted no tiene nada corriendo luego dejarlo como está.

La edición y los botones **add** le permitirán cambiar para adaptarse a sus necesidades. Simplemente haga clic en la cajita a la izquierda "corriendo" para habilitar el servicio de **proxy**, una vez haya terminado. Verá la luz **ALERTA ROJA** hasta brillante si hay errores, y usted encontrará una breve nota acerca de lo que encontramos fue el problema. Esto es lo que mis opciones básicas aspecto:



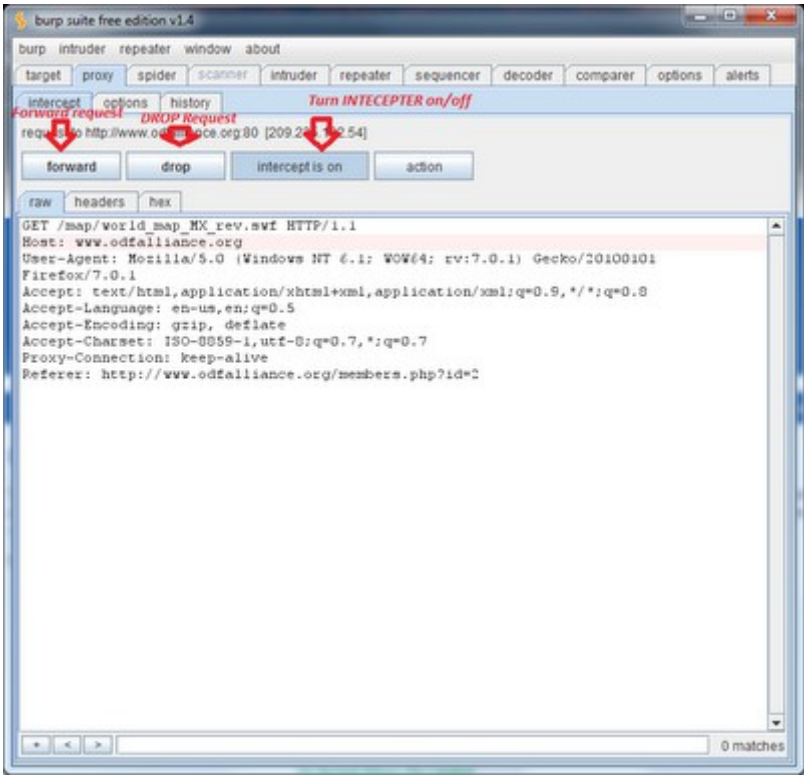
Una vez que se ha seleccionado el puerto proxy y servicios se iniciaron en Burp Suite necesitamos configurar nuestro navegador para utilizarlo para que podamos capturar el tráfico. En la mayoría de los navegadores simplemente abrir la configuración, vaya a las conexiones de red, seleccione la casilla para habilitar el soporte de proxy, y luego decirle que se utilice "localhost" y el puerto "8181" (o cualquier puerto que se está ejecutando Burp Suite en, por defecto: 8080). A continuación, establezca OK, OK para guardar la configuración actualizada y ahora usted debe estar todo listo para ir.

Ahora que tenemos la configuración,podemos insertar nuestra dirección URL de destino en la ventana del navegador y pulse ENTER. Verá la luz Burp Suite de herramientas y en la pestaña de la ficha Interceptor PROXY se iluminará en rojo para indicar que necesita su aportación.

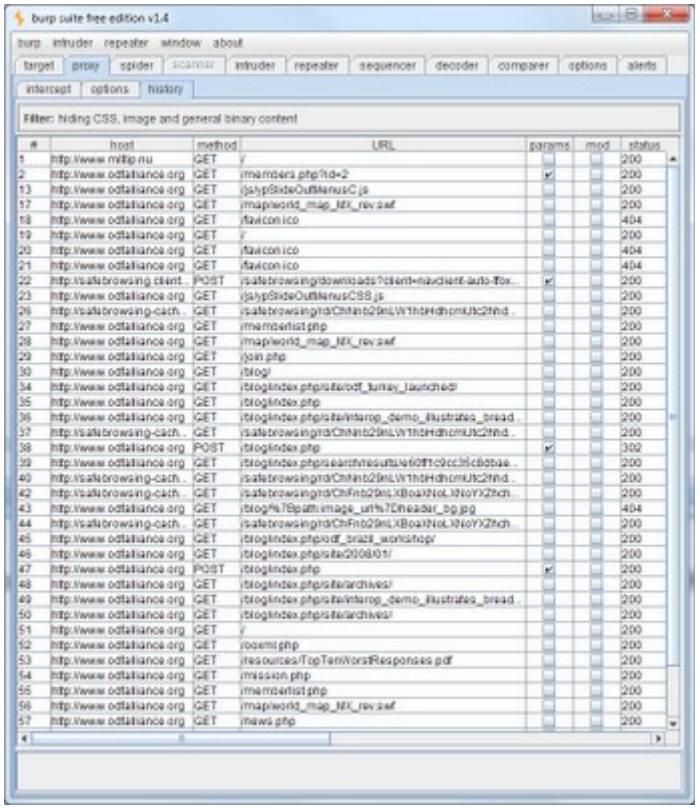
El comportamiento predeterminado es establecer el **INTERCEPTOR** en **ON**, lo que significa que captura todas las solicitudes de tráfico que se envían y requiere entrada del usuario para decidir si los paquetes se enviarán o se ha caído. Usted puede enviar y ver la página ,cargue el sitio de destino (puede requerir unos pocos hacia adelante, dependiendo del sitio).

Encuentro que esta característica es útil cuando usted sabe que usted lo quiere, pero prefiero dar vuelta y poner al **INTECEPTOR** apagado y sólo manualmente rastrear el sitio y dejar que el tráfico son capturados y enviados a la pestaña Historial. Puede ejecutar manualmente a través del sitio echarle un vistazo y todo el tráfico va a ser capturado en la ficha Historial para nosotros revisar y probar cuando estemos listos.

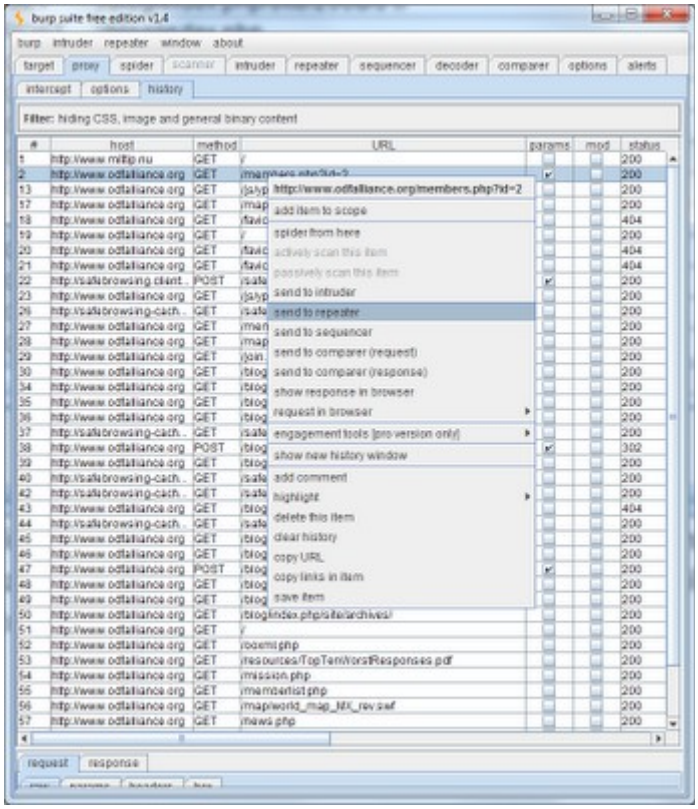
INTECEPTOR - Captura con la configuración por defecto, el usuario tiene que avanzar.



Apage el interceptor web de surf y como lo haría normalmente y todo lo que se envía a la pestaña Historial para que pueda probar cuando haya terminado:

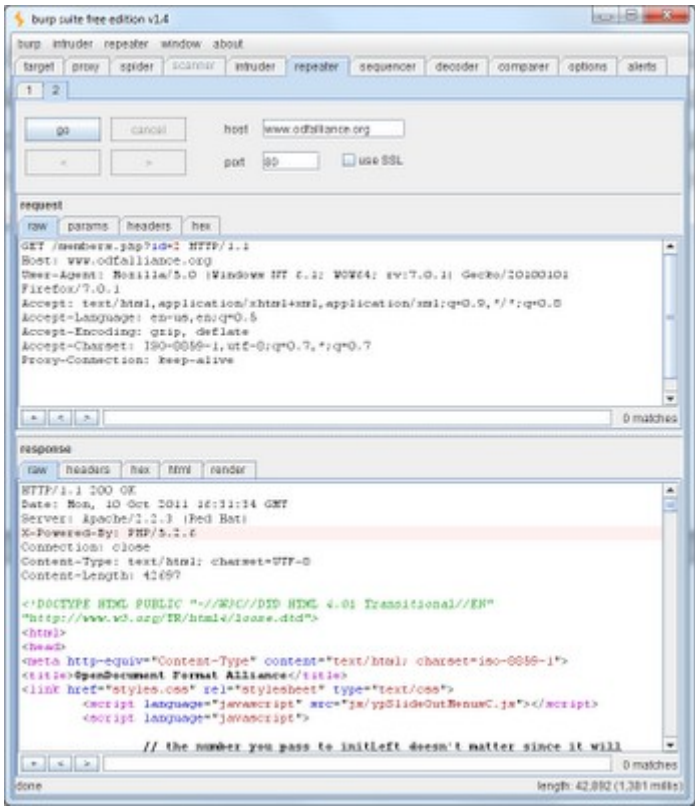


Aquí se puede ver todo el tráfico capturado con algunos parámetros respectivamente. Ahora que tenemos algunos pedidos a prueba, click derecho en el que desea probar y elegir enviarlo a la repetidora.

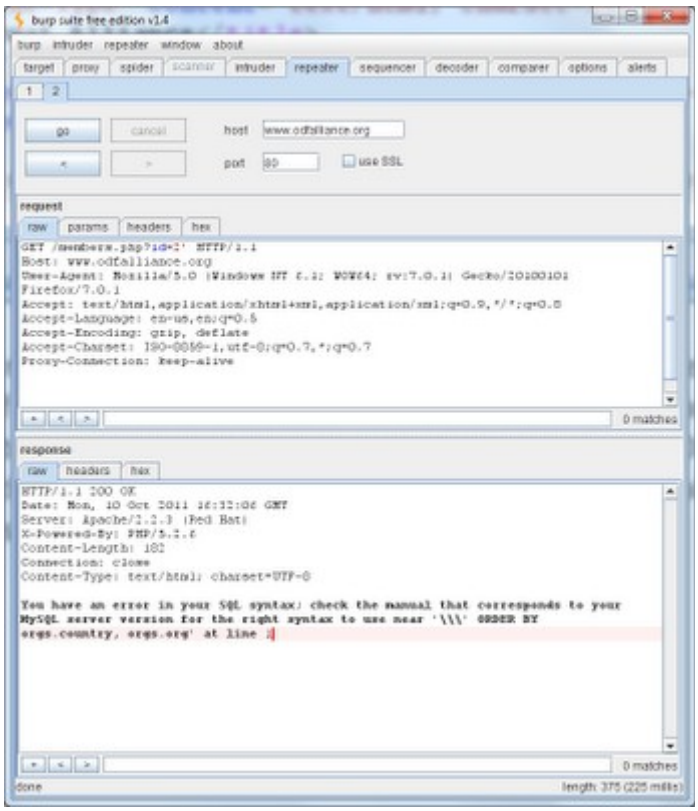


En el submenú vera la opción **REPEATER** hasta rojo brillante para indicar que está a la espera de la intervención del usuario ya que la solicitud ha sido enviada. Ahora podemos usar el repetidor

para hacer algunas inspecciones manuales rápidas. Usted encontrará la solicitud ya preparado en la pestaña RAW, también se limpia y organizada para que pueda revisar los parámetros de cabecera, o fichas hexagonales. Ahora usted puede encontrar lo que funciona mejor para usted, pero mi preferencia es trabajar con la solicitud de prima.



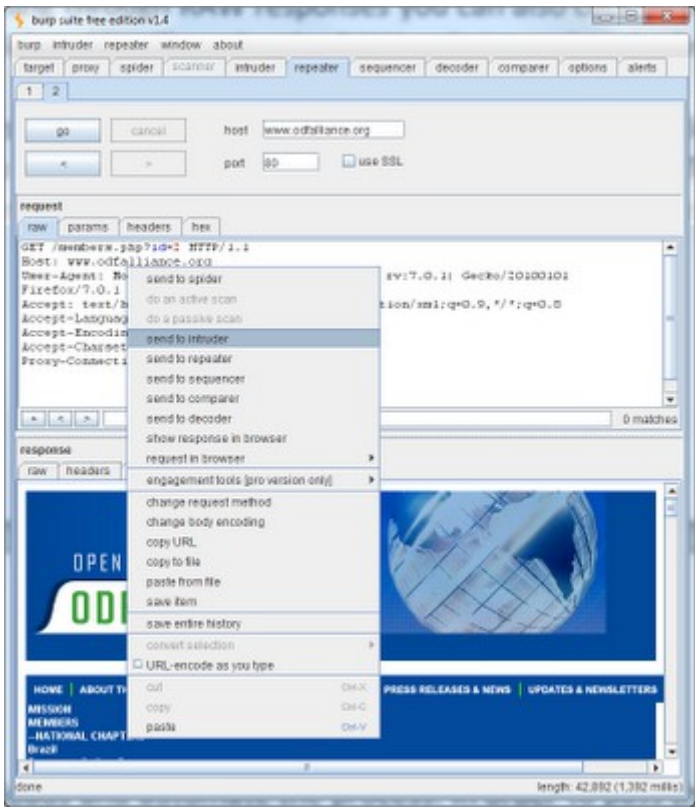
El repetidor permite realizar los cambios que desee a la solicitud y volver a enviarlo para analizar los resultados del servidor. Si se observa por encima de ella, incluso se destacan los parámetros de la petición en los vectores AZUL y posible manipular en ROJO. Vamos a enviar la solicitud pulsando el botón GO (dejarlo como es el de establecer una línea de base), y luego añadir una comilla simple después de que el "2" en la solicitud anterior y vuelva a enviar para ver si el servidor responde de forma diferente.



NOTA:

Si no te gusta buscar a través de las respuestas de RAW también puede hacer click en la ficha Render del área de respuesta (si está disponible) y va a proporcionar el código de RAW en lo que el navegador iba a ver.

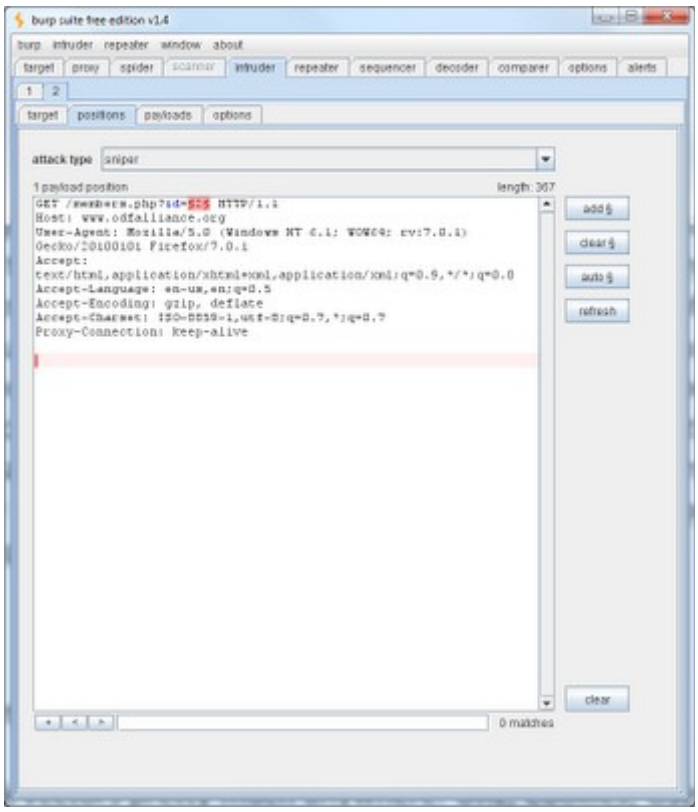
Bueno, ¿qué sabe usted, el servidor parece tener un problema con el procesamiento de comillas simples. Esto puede o no puede ser vulnerabilidad. Usted podría continuar probando este manual en el repetidor con sólo seguir editar, enviar un análisis de los resultados, pero es aquí donde la herramienta **INTRUDER** entra en juego, ya que podemos crear una carga útil de unos personalizadas y automatizar el proceso. Para aprobar esta solicitud a la herramienta **INTRUDER** apenas a la derecha haga click en el cuerpo del mensaje y elegir la opción Enviar a un intruso.



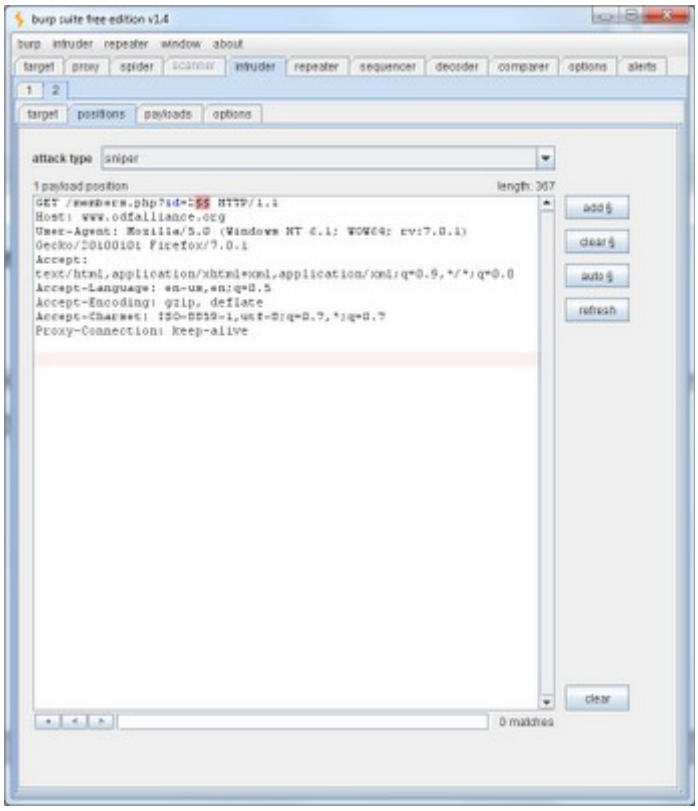
Una vez más, verá la luz **INTRUDER** hasta rojo brillante para indicar que el instrumento está en espera de la entrada del usuario. Antes de comenzar con el intruso siento la necesidad de establecer una aclaración adicional en torno a lo que todo está incluido en el intruso y cómo funcionan.

La herramienta de intrusión se divide en cuatro (4) fichas: objetivo, las posiciones, las cargas útiles y opciones. La ficha de destino es bastante sencillo, sólo tiene que apuntar a su sitio de destino, puerto deseado, y un ticker de si desea o no utilizar SSL para la conexión. Esta ficha se configura casi de forma predeterminada con sólo enviar la solicitud a la herramienta intruso, si usted necesita o desea utilizar SSL, haga click en el ticker. La pestaña de posiciones es crucial para entender, que es donde marcamos nuestras peticiones. Vamos a identificar las piezas de la solicitud donde queremos inyectar o alterar con nuestras opciones de carga útil (tendrá más sentido después de los ejemplos más adelante). La herramienta a utilizar el selector a demostrar que eran los puntos de ataque son posibles. La herramienta utiliza el símbolo § como marcadores de inicio y fin de cada posición ataque dirigido. Si desea reemplazar el valor del parámetro y luego colocar los § § símbolos antes y un después, sin embargo, si usted desea probar la alteración o la inyección después de que a continuación, coloque los § § símbolos directamente después de que el valor del parámetro. Estos son ejemplos de ambos, de nuevo este tendrá más sentido después de unos pocos ejemplos en un minuto, así que tengan paciencia conmigo por ahora.

Cambie el valor del parámetro:



Alter para inyectar después el valor del parámetro:



NOTA: Puede utilizar los botones de añadir, auto sobre el derecho a eliminar y / o marcadores de

inserción donde sea necesario. Puede identificar los vectores de ataque casi en cualquier lugar que se pueda imaginar: URL, cookies, User-Agent, etc (utilice el selector a su ventaja o característica de auto y luego reducirlo a lo que usted desea enfocar).

Aceptar lo que ha identificado en la que desea alterar / inyectar en ... ¿y ahora qué? ¿Cómo hacer que funcione?...No te preocupes, sigue leyendo estamos casi allí ..=)... Para finalizar la configuración de la **INTRUDER** debe seleccionar también el tipo de ataque utilizar y configurar los ajustes para el tipo de ataque por lo que inyecta nuestra carga útil deseada en cada posición durante las pruebas . He aquí un desglose de los cuatro (4) tipos de ataque disponibles y la idea general de lo que hace cada uno:

- **Sniper:** Este modo de ataque nos permite inyectar una carga útil solo en las posiciones de ataque elegido. Esto tiene las opciones de carga útil y las inserta una a una en la posición elegida y luego se repite hasta que se ha probado todas las opciones de carga útil. Si múltiples posiciones se eligen solo se aplicará a la prueba a una posición a la vez.

- **Ariete:** Es similar al modo de ataque de francotirador en que toma nuestro payload deseado y lo inserta en las posiciones de ataque elegido. La diferencia aquí es que si más de una posición que se elija se inserte la misma carga útil en todas las posiciones a la vez y probar, mientras que el Sniper los prueba uno por uno. Esto puede ser un tipo de ataque útil para atacar cosas donde se necesita el mismo material en varias ubicaciones de la solicitud. Yo personalmente no he utilizado esta mucho éxito.

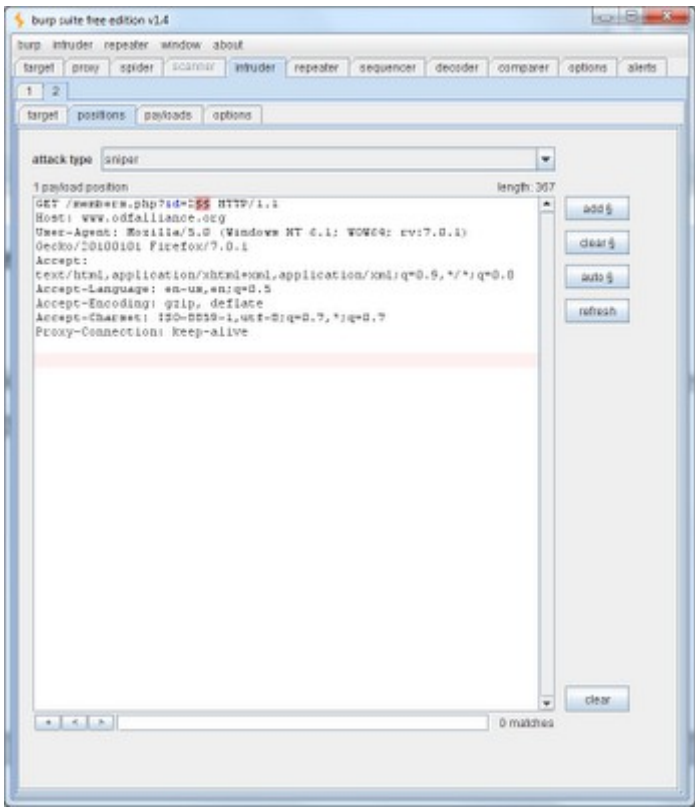
- **Pitchfork:** Este modo de ataque le permite probar múltiples cargas basadas en la posición de ataque, con un máximo de 8 es capaz de definir. Este modo de ataque pone una carga diferente para cada posición y se mueve a través de ellos uno por uno, mientras que las pruebas múltiples posiciones al mismo tiempo, que puede ser extremadamente útil en pruebas como mostraré en un minuto.

- **Cluster Bomb:** Este modo de ataque utiliza múltiples cargas y le permite probar cada carga útil posible en cada posición de ataque elegido, lo que significa que va a tratar de payload1 en posición 1 y luego en la siguiente prueba que intentará payload1 en Puesto2, intercambiando hacia fuera para cualquier otras cargas que haya definido. Esto puede ser útil cuando se tienen diferentes entradas / inyecciones necesarias en varios lugares.

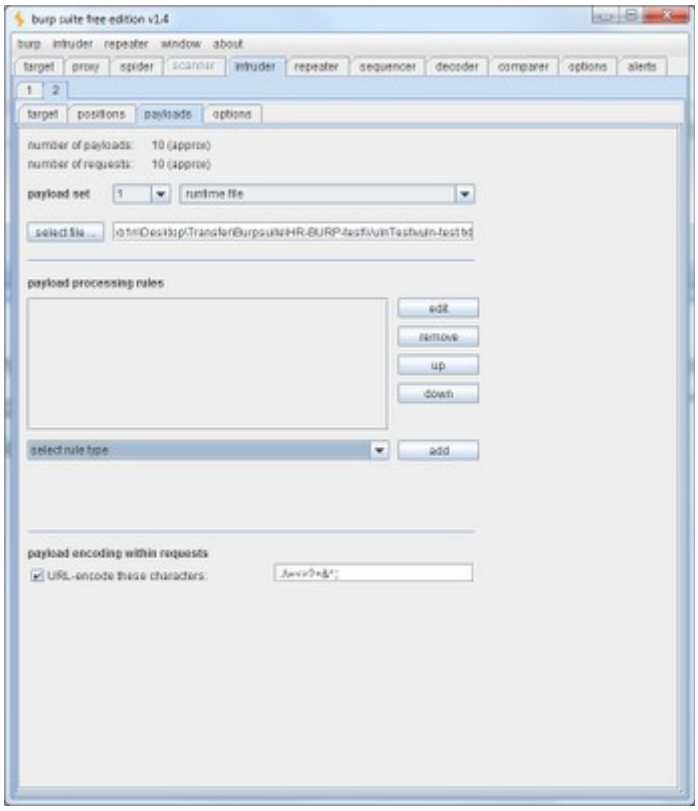
Aceptar lo que ahora usted tiene una idea de lo que los modos de ataque son, deja que te enseñe algunos en acción, así que todo se junta para usted. Vamos a tomar lo que hemos hecho de forma manual y en su lugar esta vez utilice la herramienta **INTRUDER** para probar vulnerabilidades de **SQL**. He creado una pequeña lista de posibles inyecciones para la prueba de **SQLi**, nada demasiado complejo :

- '
- "
- /
- /*
- #
-)
- (
-)'
- ('
- and 1=1
- and 1=2
- and 1>2
- and 1<=2
- +and+1=1
- +and+1=2
- +and+1>2
- +and+1<=2
- /**/and/**/1=2
- /**/and/**/1>2
- /**/and/**/1<=2

Usando nuestro ejemplo vamos a configurar el tipo de ataque que venir después de nuestro valor del parámetro. Vamos a utilizar el modo de ataque de francotirador para insertar nuestra lista de cargas anteriores.



Entonces tenemos que configurar la carga útil, salvo el ejemplo que he proporcionado anteriormente como vuln-test.txt en el ordenador en alguna parte. A continuación, vaya a la pestaña de cargas donde poner nuestra carga útil a un "archivo de tiempo de ejecución" y luego seleccione el archivo que guardó para cargar como nuestros inyecciones de carga útil.



NOTA : Existe una opción de codificación URL en la parte inferior que puede o puede no querer aprovechar. Además, asegúrese de agregar un espacio en blanco, ya que no estoy al 100%, se incluye por defecto.

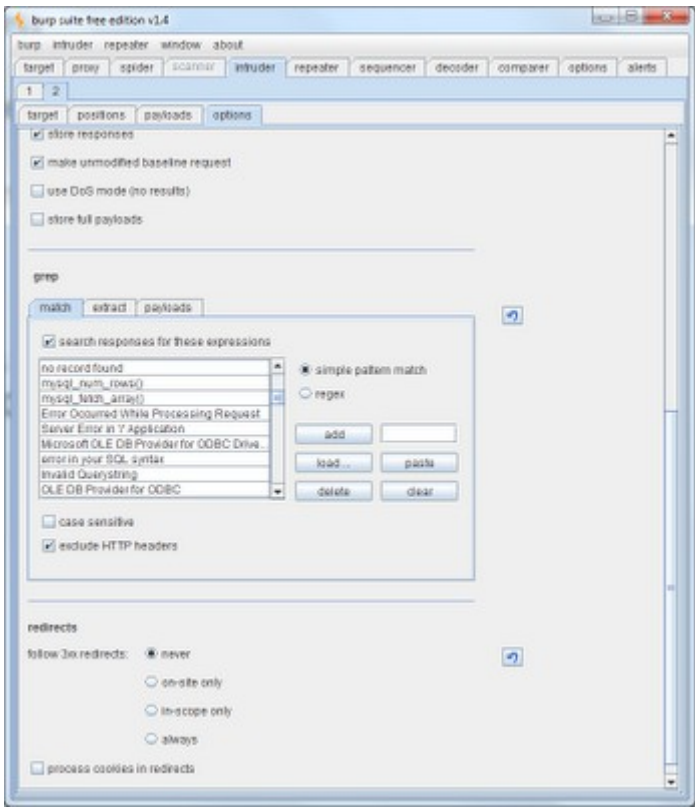
Ahora tenemos que revisar la pestaña de opciones para finalizar las cosas y entonces podremos ejecutarlo. Si se desplaza hacia abajo en la página de opciones se encuentra una sección para grep.

Podemos definir el texto a buscar en la página de resultados después de que nuestras cargas se han insertado. Esto puede ser muy útil en la interpretación de los resultados, así como que le ahorra tiempo. Yo uso una lista general de los mensajes de error de SQL para esta parte, acaba de salir de carga para seleccionar un archivo en el sistema o puede agregar manualmente una por una. Cualquiera que sea la que más le convenga está bien. He aquí un vistazo a lo que está incluido en mi error-vuln-check.txt del archivo:

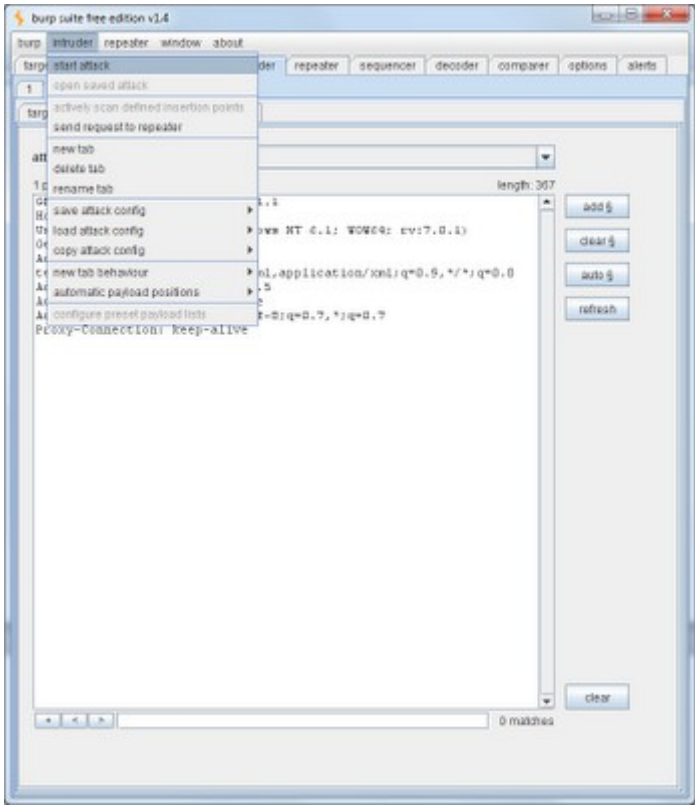
- unknown column
- unknown
- no record found
- mysql_num_rows()
- mysql_fetch_array()
- Error Occurred While Processing Request
- Server Error in '/' Application
- Microsoft OLE DB Provider for ODBC Drivers error
- error in your SQL syntax
- Invalid Querystring
- OLE DB Provider for ODBC
- VBScript Runtime
- ADODB.Field
- BOF or EOF
- ADODB.Command
- JET Database
- mysql_fetch_row()
- include()
- mysql_fetch_assoc()
- mysql_fetch_object()
- mysql_numrows()
- GetArray()
- FetchRow()
- Input string was not in a correct format
- Microsoft VBScript
- A syntax error has occurred
- ADODB.Field error
- ASP.NET is configured to show verbose error messages
- ASP.NET_SessionId
- Active Server Pages error
- An illegal character has been found in the statement
- An unexpected token "END-OF-STATEMENT" was found
- CLI Driver
- Can't connect to local

- Custom Error Message
- DB2 Driver
- DB2 Error
- DB2 ODBC
- Died at
- Disallowed Parent Path
- Error Diagnostic Information
- Error Message : Error loading required libraries.
- Error Report
- Error converting data type varchar to numeric
- Fatal error
- Incorrect syntax near
- Index of
- Internal Server Error
- Invalid Path Character
- Invalid procedure call or argument
- Invision Power Board Database Error
- JDBC Driver
- JDBC Error
- JDBC MySQL
- JDBC Oracle
- JDBC SQL
- Microsoft OLE DB Provider for ODBC Drivers
- Microsoft VBScript compilation error
- Microsoft VBScript error
- MySQL Driver
- MySQL Error
- MySQL ODBC
- ODBC DB2
- ODBC Driver
- ODBC Error
- ODBC Microsoft Access
- ODBC Oracle
- ODBC SQL
- ODBC SQL Server
- OLE/DB provider returned message
- ORA-0
- ORA-1
- Oracle DB2
- Oracle Driver
- Oracle Error
- Oracle ODBC
- PHP Error
- PHP Parse error
- PHP Warning
- Parent Directory
- Permission denied: 'GetObject'
- PostgreSQL query failed: ERROR: parser: parse error

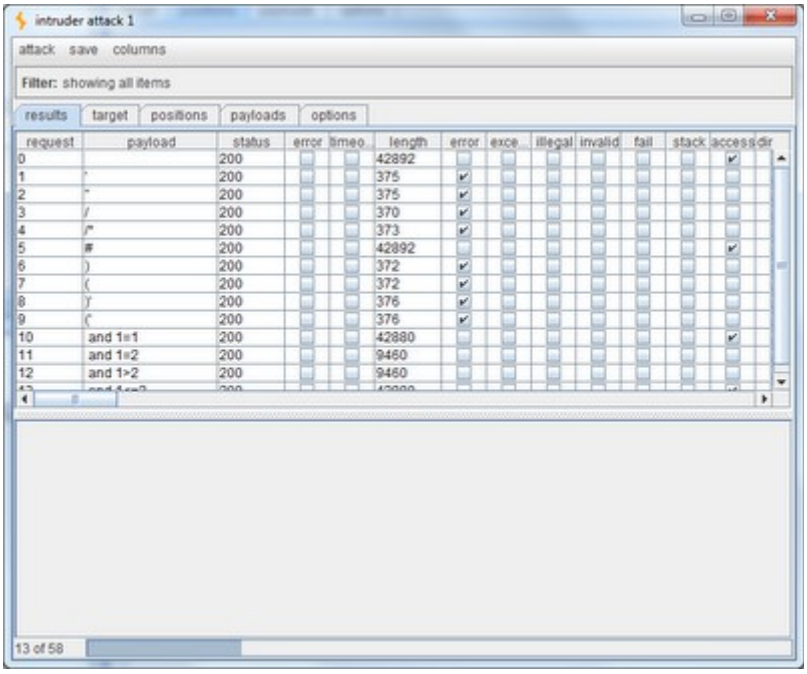
- SQL Server Driver][SQL Server
- SQL command not properly ended
- SQLException
- Supplied argument is not a valid PostgreSQL result
- Syntax error in query expression
- The error occurred in
- The script whose uid is
- Type mismatch
- Unable to jump to row
- Unclosed quotation mark before the character string
- Unterminated string constant
- Warning: Cannot modify header information - headers already sent
- Warning: Supplied argument is not a valid File-Handle resource in
- Warning: mysql_query()
- Warning: pg_connect(): Unable to connect to PostgreSQL server: FATAL
- You have an error in your SQL syntax near
- detected an internal error [IBM][CLI Driver][DB2/6000]
- error
- include_path
- invalid query
- is not allowed to access
- missing expression
- mySQL error with query
- mysql error
- on MySQL result index
- on line
- server at
- server object error
- supplied argument is not a valid MySQL result resource
- unexpected end of SQL command



Una vez terminado esto en realidad se puede realizar el test con nuestra petición HTTP que hemos identificado anteriormente y ahora con nuestro ataque Sniper seleccionado con capacidad de carga de prueba vuln grep y contenido establecidos. Puede ejecutar la herramienta de intrusión haciendo click en el menú archivo en ataque comienzo Intruder superior y seleccionando simplemente. >>

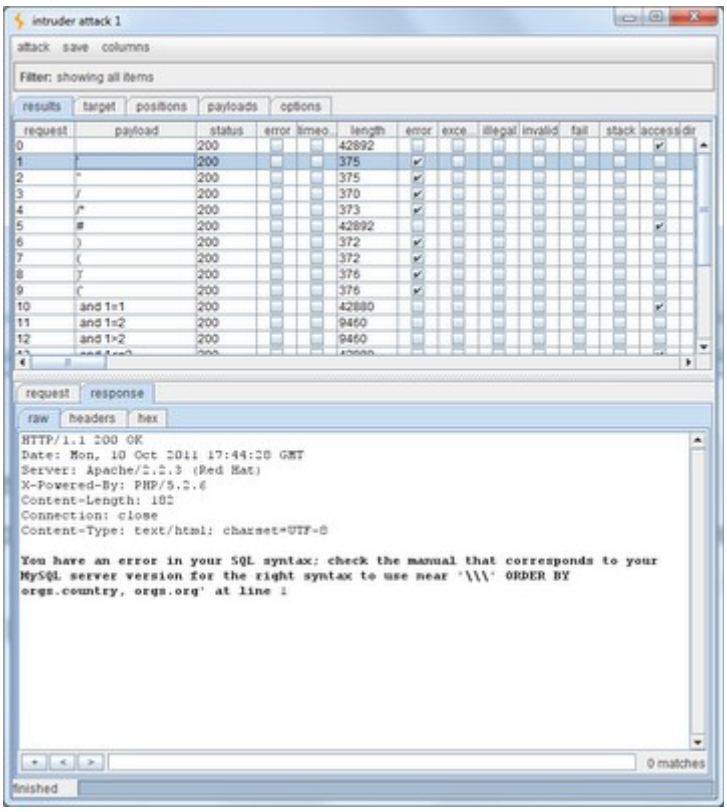


Ahora se abrirá una nueva ventana en la que podemos ver a la realización de la prueba y luego interpretar los resultados:



Se puede ver claramente que existe una diferencia de longitud de los mensajes con los delincuentes comunes SQLi, así como algunas diferencias notables de las verdaderas pruebas falsas al final. Si además miras, verás que hay una gran cantidad de columnas a la derecha y que algunos de ellos tienen controles en los mismos.

Esto es para significar que el grep encuentra el texto de nuestra lista. Si hace clic sobre una solicitud a continuación, puede ver la solicitud real y la respuesta en la zona de abajo, por lo que ahora podemos ver con claridad cuáles provocó un error y qué error se produce, también puede revisar la respuesta dictada a ver las diferencias visuales de las cosas como los ejemplos verdaderos falsos, ya que no siempre se puede tirar de nuevo los errores de lectura mecánica (longitud puede decir mucho y actuar como una gran pista sobre dónde debe gastar tiempo investigando más lejos).



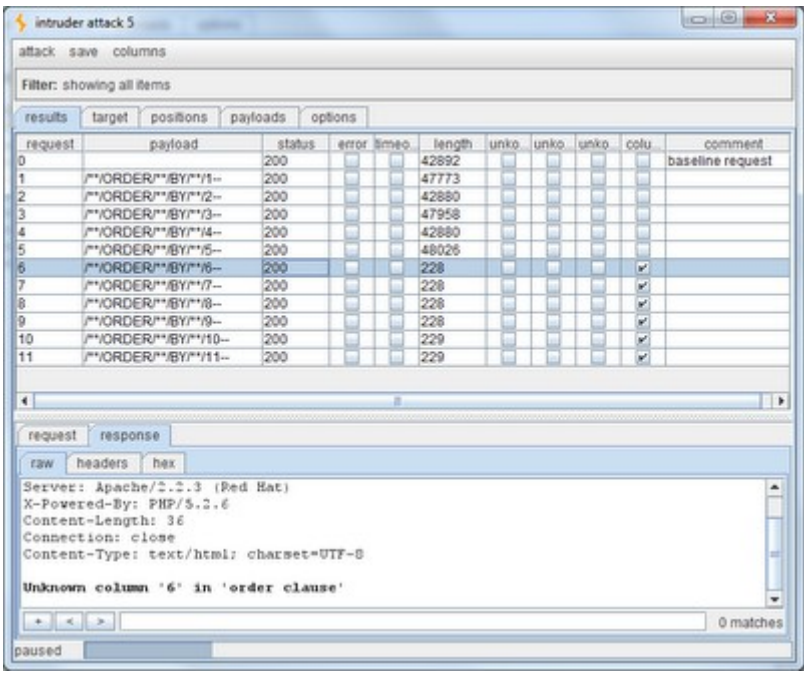
Aceptar que hemos encontrado una potencial vulnerabilidad SQLi basado en mensajes de error y las verdaderas pruebas de respuesta falsa. Este es buen comienzo, pero...¿ahora qué?....Ahora nos vamos a la configuración de intrusos y de trabajo en la modificación de los ajustes a realizar más ensayos y explotar.

Veamos ahora si podemos establecer el Intruso para poner a prueba ORDER BY para determinar el número de columnas rápido. Utilizando la misma solicitud que ahora se posicionará nuestro payload para insertar ORDER BY resultados de la instrucción y de prueba para encontrar recuento.

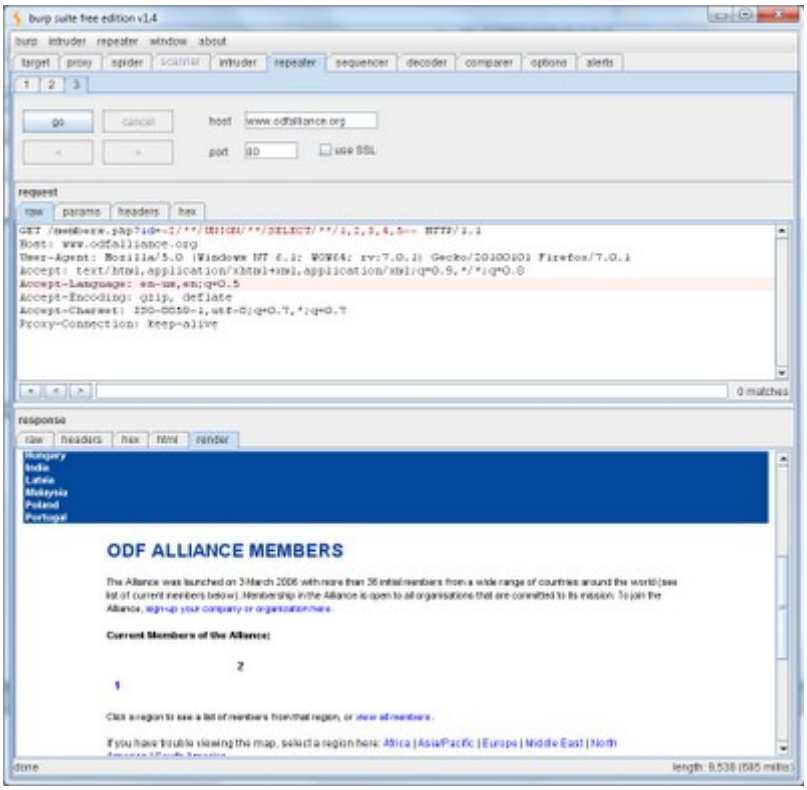
Ejempplo -order-by.txt

- ORDER BY 1—
- ORDER BY 2—
- +ORDER+BY+1—
- +ORDER+BY+2—
- /**/ORDER/**/BY/**/1—
- /**/ORDER/**/BY/**/2--
- …..xDD!!!

Actualización de nuestra configuración grep para buscar "la columna desconocido" y cualquier otra cosa que te gustaría agregar para la determinación del recuento. Una vez que estos se han realizado cambios, vuelva a ejecutar la herramienta intruso y revisar los resultados para ver lo que hemos encontrado:



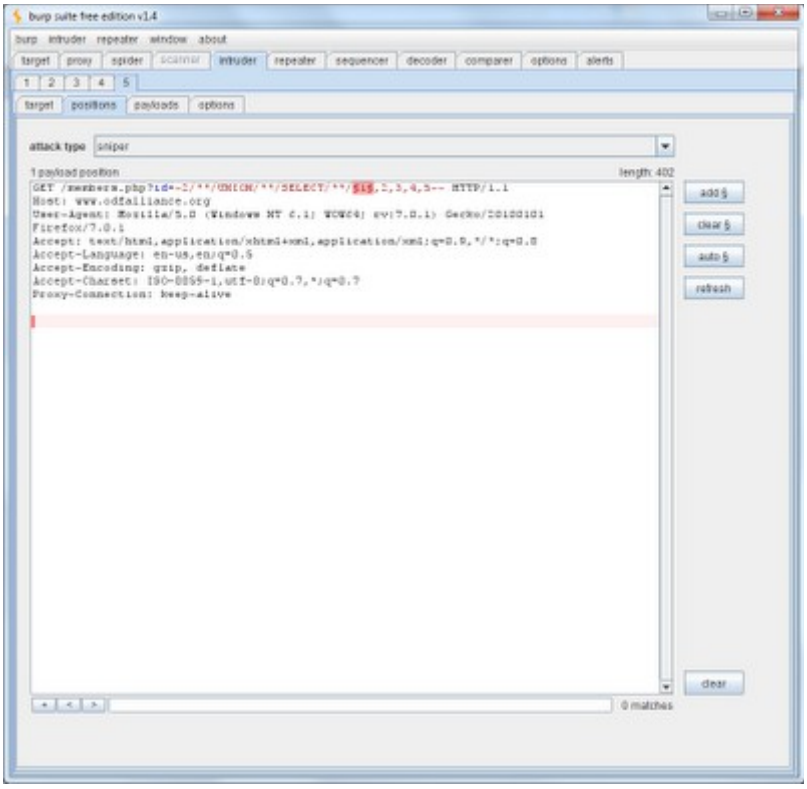
Bien..!!!!... Hemos encontrado la columna contar hasta un 5! Es posible utilizar las peticiones de respuesta a juez, además de la pista longitud de la solicitud. Ahora vamos a enviar esta solicitud al repetidor, ahora vamos a utilizar el REPETIDOR encontrar columnas vulnerables. Cambiar el orden de UNION SELECT con el recuento de columna conocida, ejecute la solicitud por repetidor y ver los resultados proporcionados a ver qué columnas son vulnerables:



NOTA: No olvide a NULL o negar "-" Valor de parámetro para que el producto refleja las columnas

vulnerables.

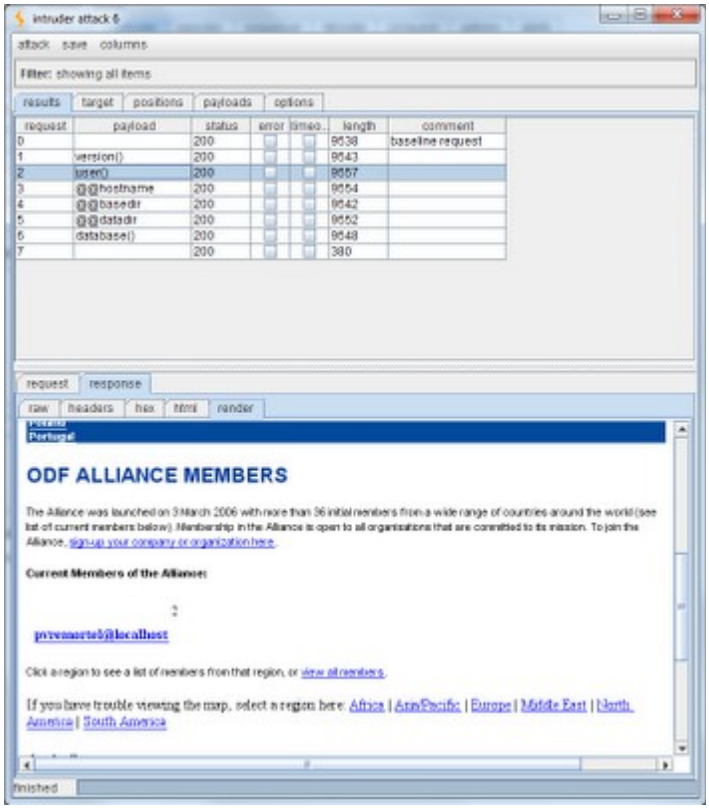
OK.....Ahora vemos claramente que las columnas 1 y 2 son vulnerables. Ahora podemos enviar esta solicitud de devolución actualizada al intruso para su análisis posterior y la explotación. Ahora vamos a configurar el intruso insertar algunas consultas básicas de SQL como cargas útiles en nuestras columnas vulnerables para llevarnos algo de información básica a cambio. He reunido una lista corta llamada basic.txt utilizar como carga útil, pero usted tendrá que ajustar las posiciones de ataque para insertar en lugar de la columna 1 y / o 2 (Sólo se necesita una manera que sea sencillo).



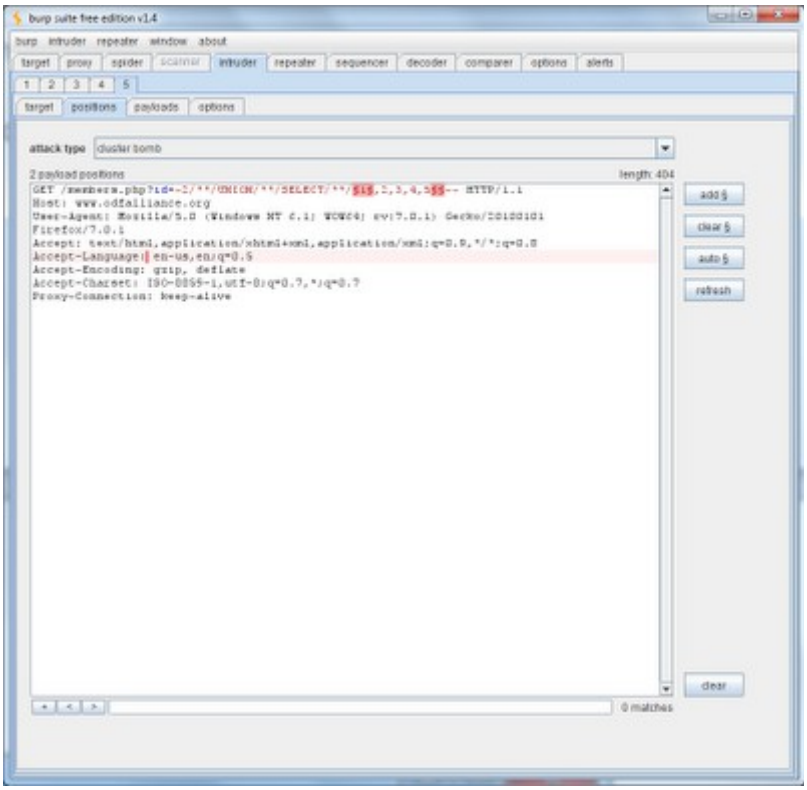
Ejemplo -basic.txt:

- Version ()
- Usuario ()
- Base de datos ()
- @ @ hostname
- @ @ basedir
- @ @ datadir
- ...xD!!!

Una vez que haya configurado las opciones de carga útil, es hora de volver a correr una vez más e interpretar los resultados. Usted no necesita ningún grep aquí ya que estaremos tirando de los datos de los paquetes de respuesta del servidor prestados directamente esta vez.

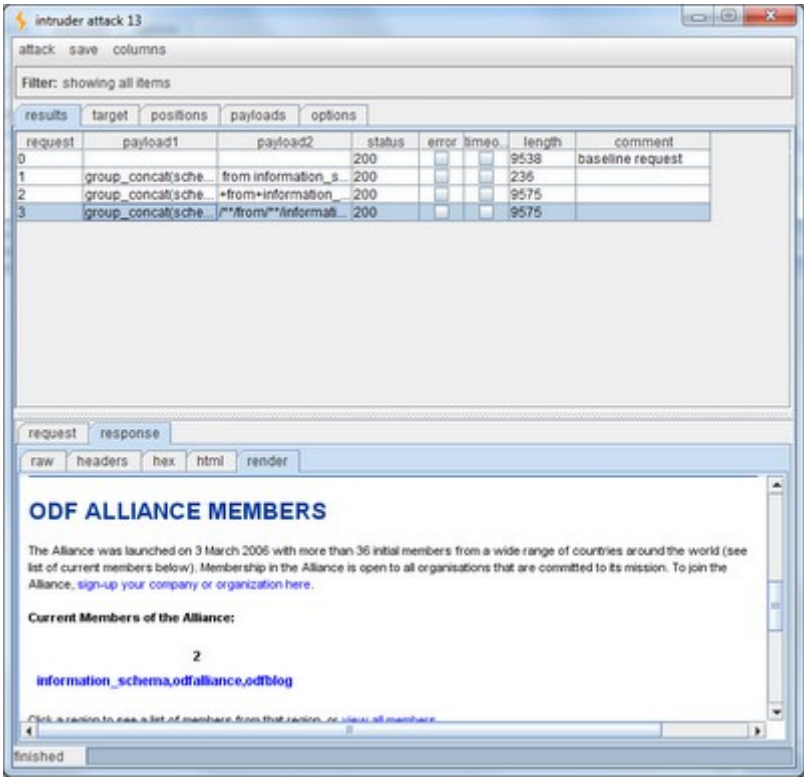


Podemos seguir adelante hasta el final de la extracción, simplemente ajustando nuestras cargas y volver a probar. Si queremos comprobar si las bases de datos disponibles, se puede agregar un vector de ataque adicional a nuestra solicitud existente, modificar el modo de ataque de bomba de racimo, y luego cambiar las cargas útiles de conseguir-y conseguir-dbs1.txt dbs2.txt.

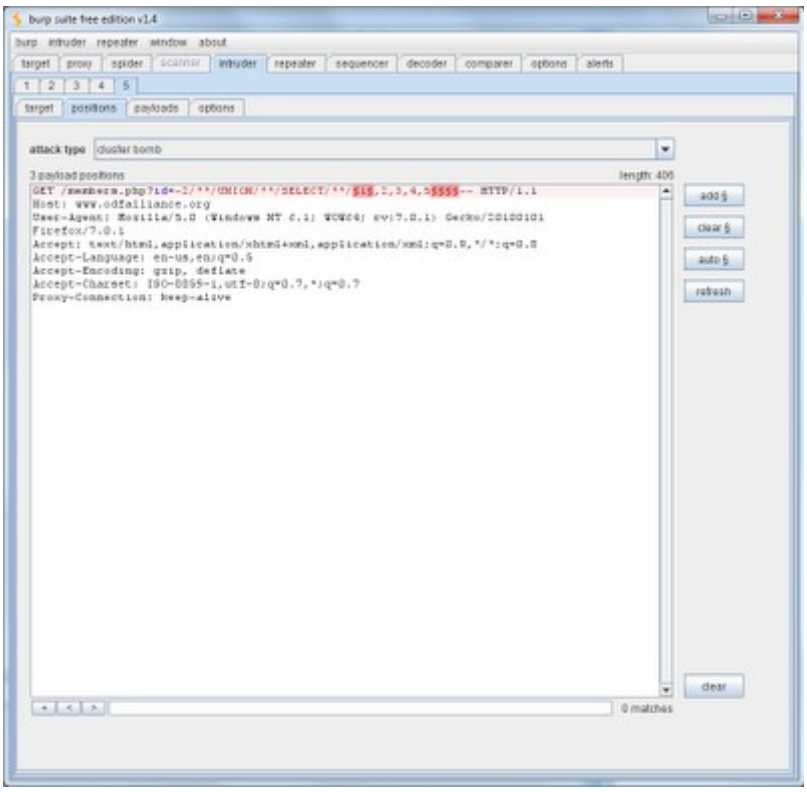


NOTA: También se van a cambiar al modo de clúster ataque con bomba para que podamos entrar en ambas cargas útiles al mismo tiempo para obtener los resultados deseados.

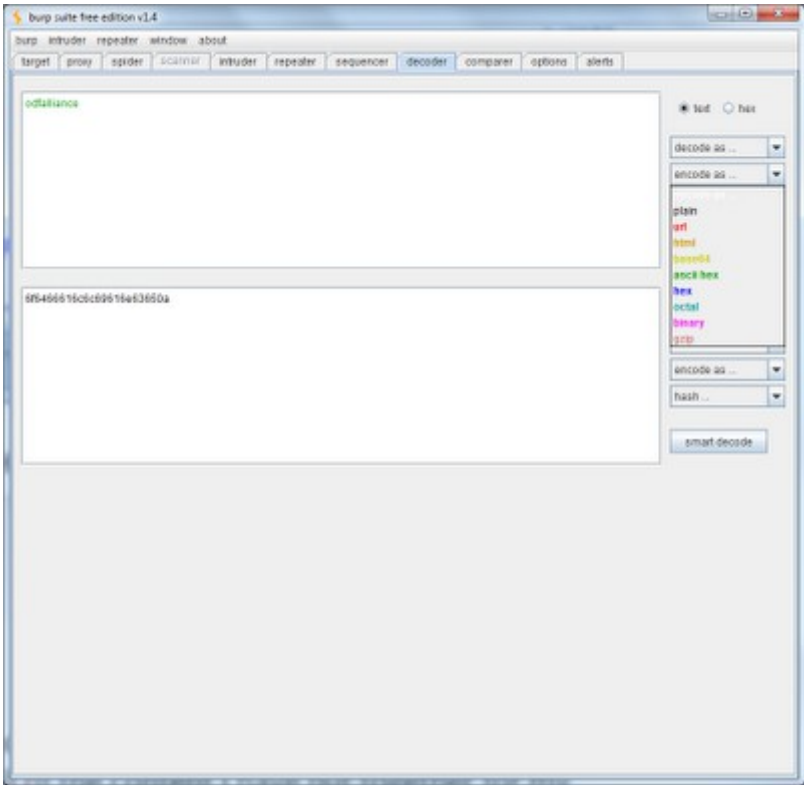
Una vez que lo haya configurado, repetición de la prueba e interpretar los resultados:



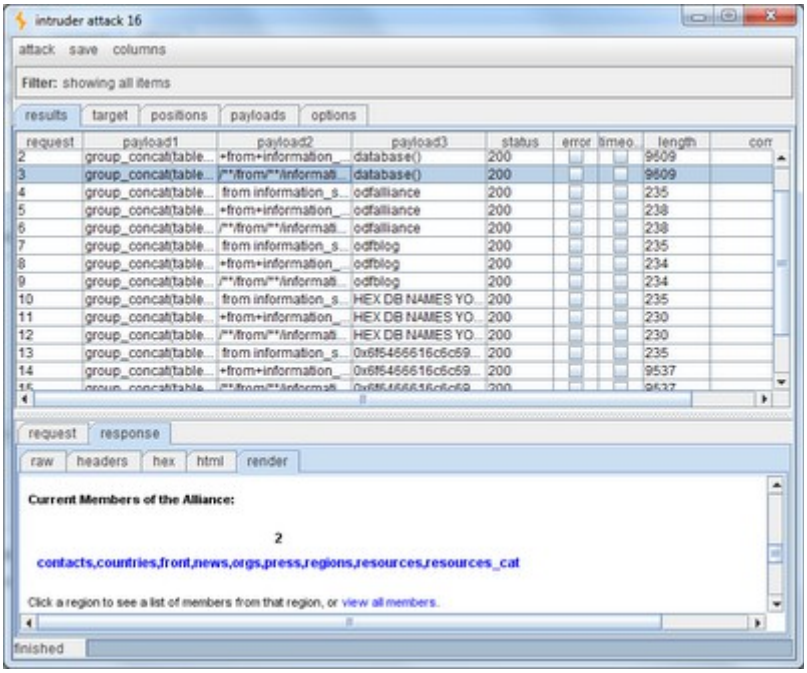
OK .....Tomar nota de los nombres de DB disponibles, usted tendrá que HEX y copiarlos y pegarlos en el archivo llamado get-Tables.txt como ahora vamos a utilizar esto para nuestra siguiente carga configurado para obtener las tablas para cada base de datos encontrados. Inserte get-tables1.txt en la posición 1, use get-tables2.txt para carga útil y la posición 2, e inserte get-tables3.txt al final (esto significa que también tenemos que añadir otro vector de ataque de inyección / inserción a nuestra solicitud. seguirá inmediatamente después Puesto2 puesto que se va a vincular entre sí). El primero de ellos establece la creación GROUP_CONCAT, el segundo prepara la declaración y el tercero recorre la lista de nombres de bases de datos para enumerar las tablas de. Vuelva a ejecutar la prueba de intrusos una vez que lo haya configurado, no grep necesitábamos ya que en su mayoría se utiliza la función de representación para interpretar de aquí en adelante.



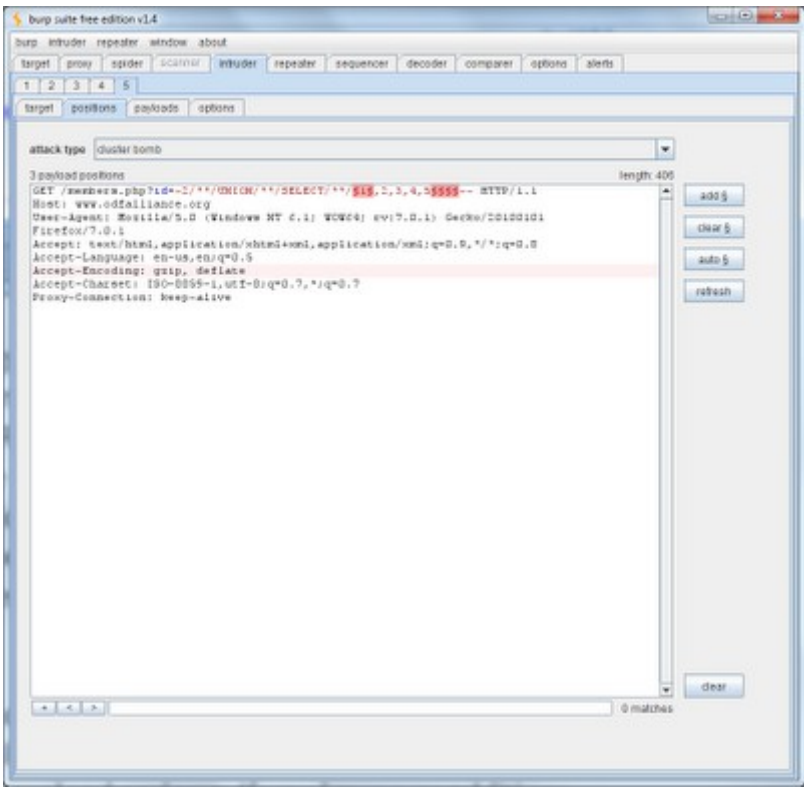
NOTA ESPECIAL: Se puede utilizar la herramienta para DECODER HEX si usted lo desea, basta con pegar el texto en la zona superior y luego elegir la caída media hacia abajo para "codificar como" y escoja lo que desea. El texto convertido se muestra en la parte inferior:

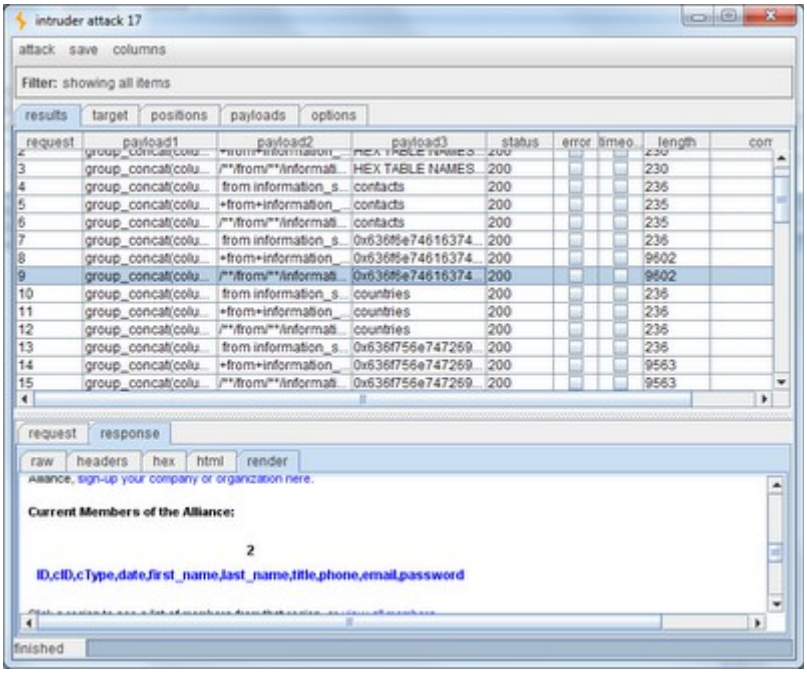


Observe que los resultados difieren cuando el nombre de base de datos no está en el valor HEX a continuación:

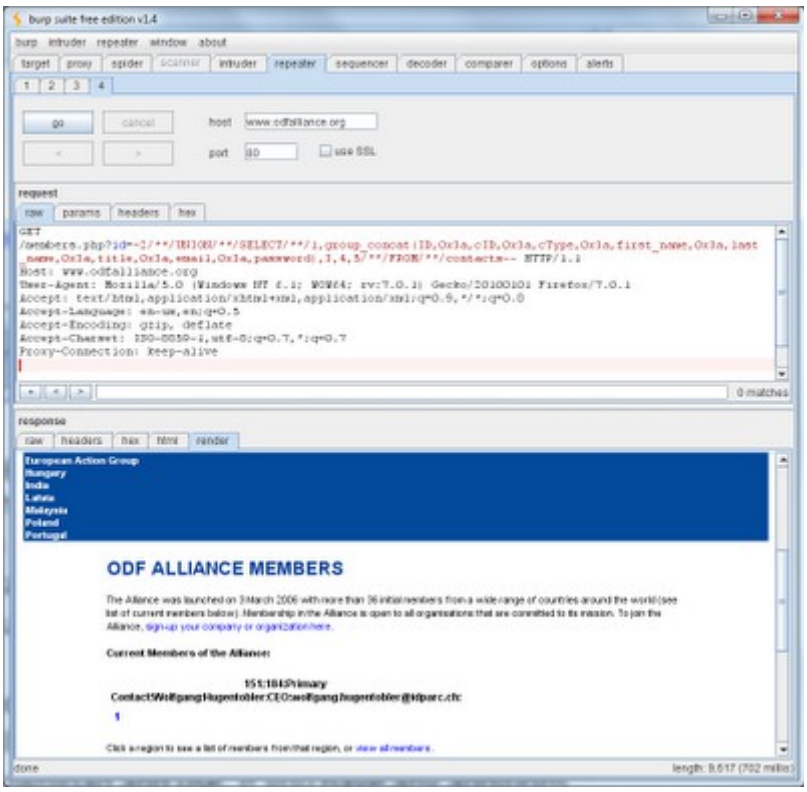


OK....Así que ahora tenemos información básica, DBS, MESAS, podemos seguir adelante y modificar ligeramente para obtener las columnas. Volvemos a la pestaña Intruder y volver a configurar para obtener columnas de las tablas conocidas. Usted tendrá que acordarse de HEX otra vez, así que adelante y utilizar el DECODER de nuevo-que es lo que hay allí! Esta vez tenemos que añadir otro vector de ataque a nuestra solicitud para que podamos insertar nuestro GROUP_CONCAT (column_name), luego de insertar la declaración, y luego vamos a utilizar la posición 3 para la inserción de los nombres de tabla. Si lo desea, puede añadir un cargo adicional de 4 a añadir en la sintaxis necesaria para tirar de las tablas de base de datos no activo (se refieren a algunos de mis otros tutoriales de SQL básicas, si usted necesita ayuda para encontrar la sintaxis).



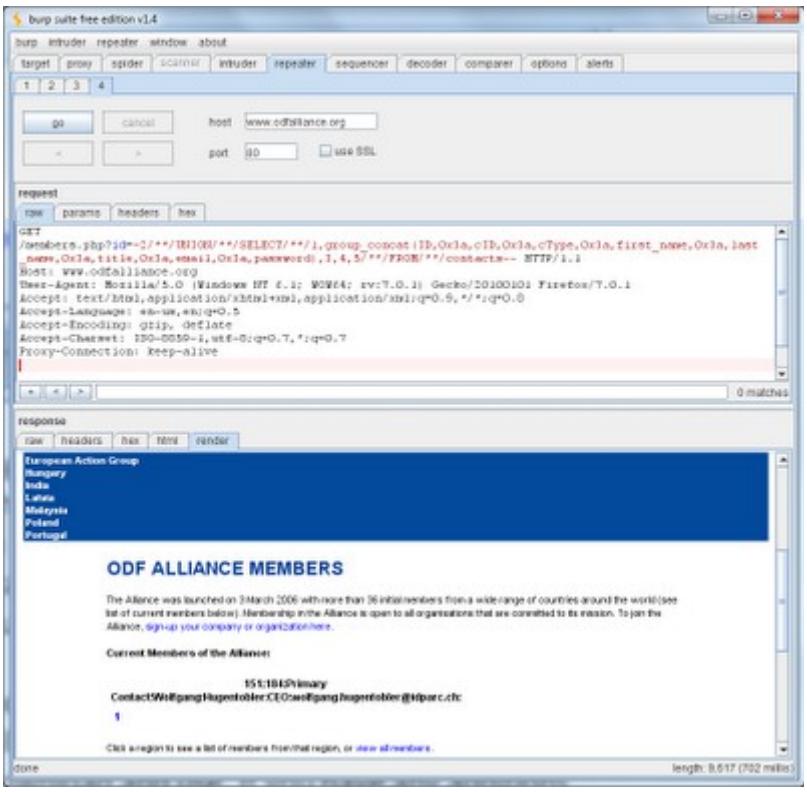


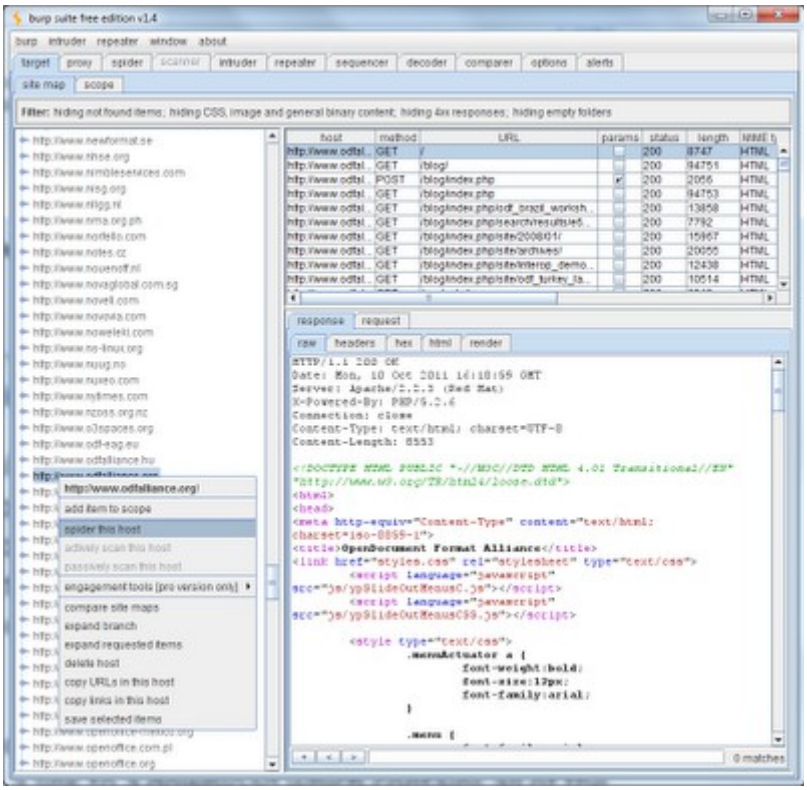
Ahora usted tiene todo lo que necesita para extraer. Usted puede seguir alterando las cargas útiles de manejar esto para usted si usted está trabajando con una vulnerabilidad o exploit que es lavado y enjuague de repetición, sin embargo, si los objetivos no tienen el mismo contenido, entonces este puede ser el momento de volver al repetidor para aplicar manualmente el contenido que se encuentra a extraer lo que quieras. Simplemente altera la sintaxis para adaptarse al igual que era normal SQLi y después haga clic en GO y analizar los resultados arrojados por el tesoro pirata.



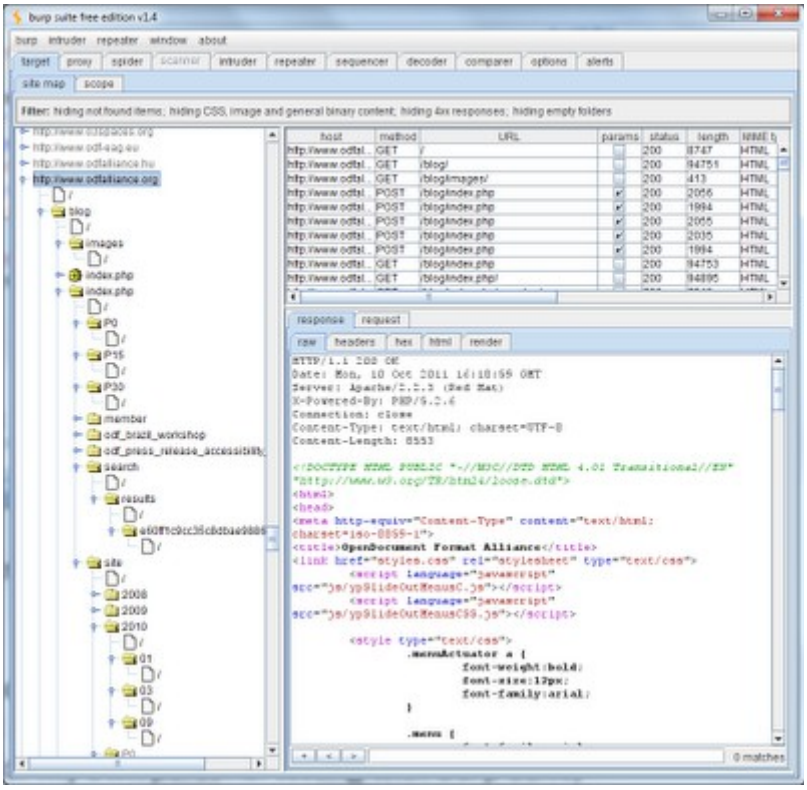
Aceptar lo que ahora se han utilizado con éxito Burp Suite para encontrar la vulnerabilidad y explotarla. Si usted necesita para planificar el sitio para encontrar tal vez las páginas de acceso hay una última herramienta en el conjunto que puede ayudar, y que es la herramienta SPIDER. Es consciente de las aplicaciones lo que significa que se darán cuenta de los vínculos pasados a través del proxy durante las pruebas. También se puede activar mediante la personalización de la configuración de opciones para ello y dejarlo suelto en el lugar de destino.

Es bastante buena, incluso con la configuración predeterminada. Usted acaba de encontrar su destino en la lista MAPA DEL SITIO en el lado izquierdo debajo de la araña. Haga clic en el sitio de destino y decirle que "host araña" y que va a hacer su cosa. Si se llega a través de los formularios que pondrá en marcha la caja de alerta roja ya que tienes que decirle a la herramienta a presentar formularios o hacer caso omiso de ellos (se puede definir una configuración personalizada para que esto sea manejado de acuerdo con las opciones - sólo recuerde que lo que pones es lo que aparece en los registros de modo que si su tratando de ser profesional es posible que desee cambiarlo;).





Una vez hecho esto usted puede usar la vista de árbol para ver la infraestructura del sitio de acuerdo a la herramienta de spider :



Alternativamente, usted puede utilizar una solicitud a la raíz del servidor web y luego enumerar una lista de archivos de páginas de acceso conocidos / directorios y respuestas para ver si está presente.

Bueno creo que eso es topo hasta el momento acerca de Burp Suite, cabe mencionar que esta es una excelente herramienta, hay un sinfín de cosas mas por saber acerca de esta potente herramienta, talvéz posteriormente volvamos a seguir jugando un poco mas Burp.