FUNCIONAMIENTO SCRIPT INYECCION SQL

Al iniciar el programa, este nos pedirá entre 3 opciones que seleccionemos la que queremos utilizar:

Diagrama

Descripción generada automáticamente con confianza media

En caso de elegir la **primera opción**, únicamente nos dirá el numero de bases de datos que ha encontrado, es bastante sencillo el funcionamiento de esta parte, para ello al igual que en el resto del script, deberemos de introducir el método por el cual queremos obtener la información “GET o POST”.

En caso de elegir el método GET, el programa únicamente nos pedirá la URL de la que queremos obtener la información y el parámetro que queremos atacar, en este caso será el “name”.

Imagen que contiene Texto

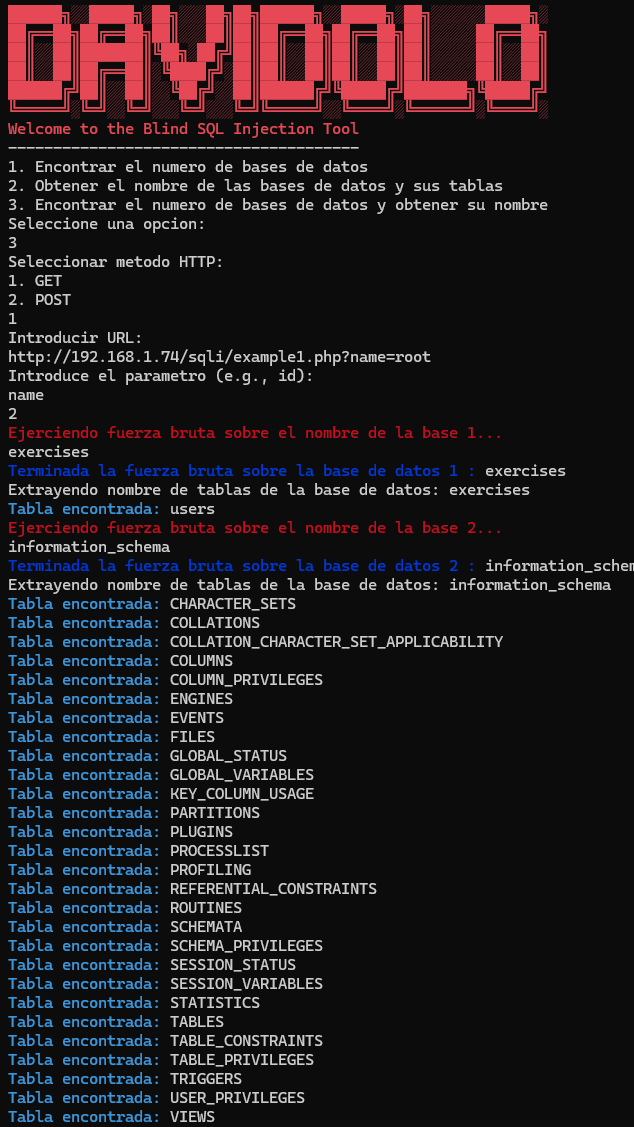
Descripción generada automáticamente

La segunda opción consiste en averiguar tanto el o los nombres de las bases de datos junto con sus respectivas tablas, para ello se deberá de rellenar la misma informacion que en el primer punto, el método por el que se quiere realizar, la URL y el parámetro.

Texto

Descripción generada automáticamente

Por último, la tercera opción hace lo mismo que las dos primeras cosas que ahora mismo no es muy útil ya que la opción 2 te saca directamente todo.



En cuanto el método post el funcionamiento es bastante similar, seleccionar el método, introducir la URL y el parámetro, la única novedad es que puedes introducir las cookies de tu navegador para comprobar la autenticación.

Aquí seleccionamos la primera opción, con el método POST.

Texto

Descripción generada automáticamente

Y a continuación mostraremos el paso 2.

Texto

Descripción generada automáticamente

La razón por la cual en el parámetro utilizamos **uname** sin tenerlo indicado en la url es porque si interceptamos la petición con burpsuite cuando introducimos algún valor en los campos de Username y Password.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Estos campos pasan a llamarse **uname** y **pass**

Texto

Descripción generada automáticamente

FUNCIONAMIENTO DEL SCRIPT

**Menú de opciones y métodos HTTP**: se pregunta al usuario qué acción desea realizar y se le da la opción de buscar el número de bases de datos, obtener el nombre de la base de datos y sus tablas, o ambas. A continuación, seleccione el método HTTP (GET o POST).

**Recopilación de datos de entrada**: el script solicita la URL de destino y los parámetros para probar la inyección SQL. Si se selecciona POST, también solicitará al usuario las cookies necesarias.

**Función send\_request**: esta función utiliza curl para realizar una solicitud al servidor. Si se selecciona POST y se proporcionan cookies, se incluirán en la solicitud. Esta función maneja solicitudes GET y POST y devuelve el tamaño de la respuesta para su posterior análisis.

**Función extract\_length**: intenta determinar cuántas bases de datos existen realizando solicitudes sucesivas con diferentes números hasta que la respuesta cambie, lo que indica que la consulta SQL es verdadera. Devuelva este número para su uso posterior.

**Función extract\_number\_of\_tables**: similar a extract\_length, esta función cuenta cuántas tablas hay en una base de datos específica, probando los números hasta que la respuesta no coincide con el valor de referencia, lo que indica que el número de tablas es correcto.

**Función brute\_force\_table\_names**: intenta adivinar los nombres de las tablas mediante fuerza bruta utilizando caracteres ASCII en cada posición del nombre hasta que no se encuentren más tablas en la base de datos dada.

**Función brute\_force\_db\_names**: utiliza la fuerza bruta para adivinar los nombres de las bases de datos. Realiza solicitudes con diferentes caracteres hasta que la longitud de la respuesta cambia, indicando que la letra es correcta, y luego pasa a la siguiente posición.

**Función brute\_force\_all**: Coordina todo el proceso de adivinar primero el número de bases de datos y luego usar esa información para adivinar los nombres de las bases de datos y las tablas que contienen.

**Ejecutar operación (función list\_items)**: Ejecuta la función correspondiente según la opción seleccionada por el usuario al inicio.