EJERCICIOS INYECCIÓN SQL

Prerrequisitos

Kali Linux

OWASP BWA

Ejercicio 1 - SQLMap

Realizar el ejercicio de inyección SQL en la aplicación web Mutillidae II:

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

Intentar conseguir la siguiente información:

Base de datos que se está utilizando.

Tablas de la base de datos.

Columnas de la base de datos.

Esquema completo.

Volcado completo de tabla de usuarios con contraseñas.









Ejercicio 2 - SQLMap

Realizar el ejercicio de inyección SQL en la aplicación web Mutillidae II:

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

Intentar conseguir la siguiente información:

Base de datos que se está utilizando.

Tablas de la base de datos.

Columnas de la base de datos.

Esquema completo.

Volcado completo de tabla de usuarios con contraseñas.









Ejercicio 3 - SQLMap

Realizar el ejercicio de inyección SQL en la aplicación web Mutillidae II:

OWASP 2013 > A1 - Injection (SQL) > SQLMap Practice > View Someones Blog

Intentar conseguir la siguiente información:

Base de datos que se está utilizando.

Tablas de la base de datos.

Columnas de la base de datos.

Esquema completo.

Volcado completo de tabla de usuarios con contraseñas.









Ejercicio 4

Interpretar los resultados obtenidos: ¿Las tres aplicaciones web usan la misma base de datos? En caso de ser la misma, justifica tu respuesta. En caso de no ser la misma, justifica tu respuesta.

SI, UTILIZAN LA MISMA: MYSQL