Ketchup

En el login se inspecciona la página y se obtiene la siguiente pista:

webmaster@teamketchup.info.unlp.edu.ar
Haciendo click en materias aparece filtro buscador; pequeña inyección sql devuelve el error de que el navegador debe de ser uno correspondiente al año 2002.
Con burpsuite se realiza el cambio del user-agent a uno correspondiente: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Con eso me devuelve lo siguiente:
RWluYXIgbm8gdGUgb2x2aWRlcyBxdWUgbGEgcGFzcyBlcyAxMTc5MjcyZTFkNjU0ZmFjOWYxNzMwMDBjODk1OGE4MyA=

Herramienta para decodificar obtengo lo siguiente:
Einar no te olvides que la pass es 1179272e1d654fac9f173000c8958a83

herramienta para encontrar que se trata de md5:
Clave: thesimpsons

Con el mail y contraseña se logra acceder (tener en cuenta que a veces modifica el protocolo a uno no seguro - http, devolviendo error):
FLAG{con_ketchup}

Ctrl + Panic

en ruta /perfil/id se utiliza burpsuite para realizar un sniper attack, similar a casos anteriores, donde se utiliza como parámetro iterable el id en la ruta perfil, buscando alguna coincidencia con la palabra “admin”. Guiado además por el código 200 de respuesta, se obtiene lo siguiente:

Request	Payload	Status co...	Respons...	Error	Timeout	Length	admin
126	126	200	142			2247	
42	42	200	348			2270	1
30	30	200	217			2162	
29	29	200	474			2162	
28	28	200	316			2162	
27	27	200	396			2155	
26	26	200	162			2160	

Se busca el perfil con id: 42

Se encuentra primera parte:

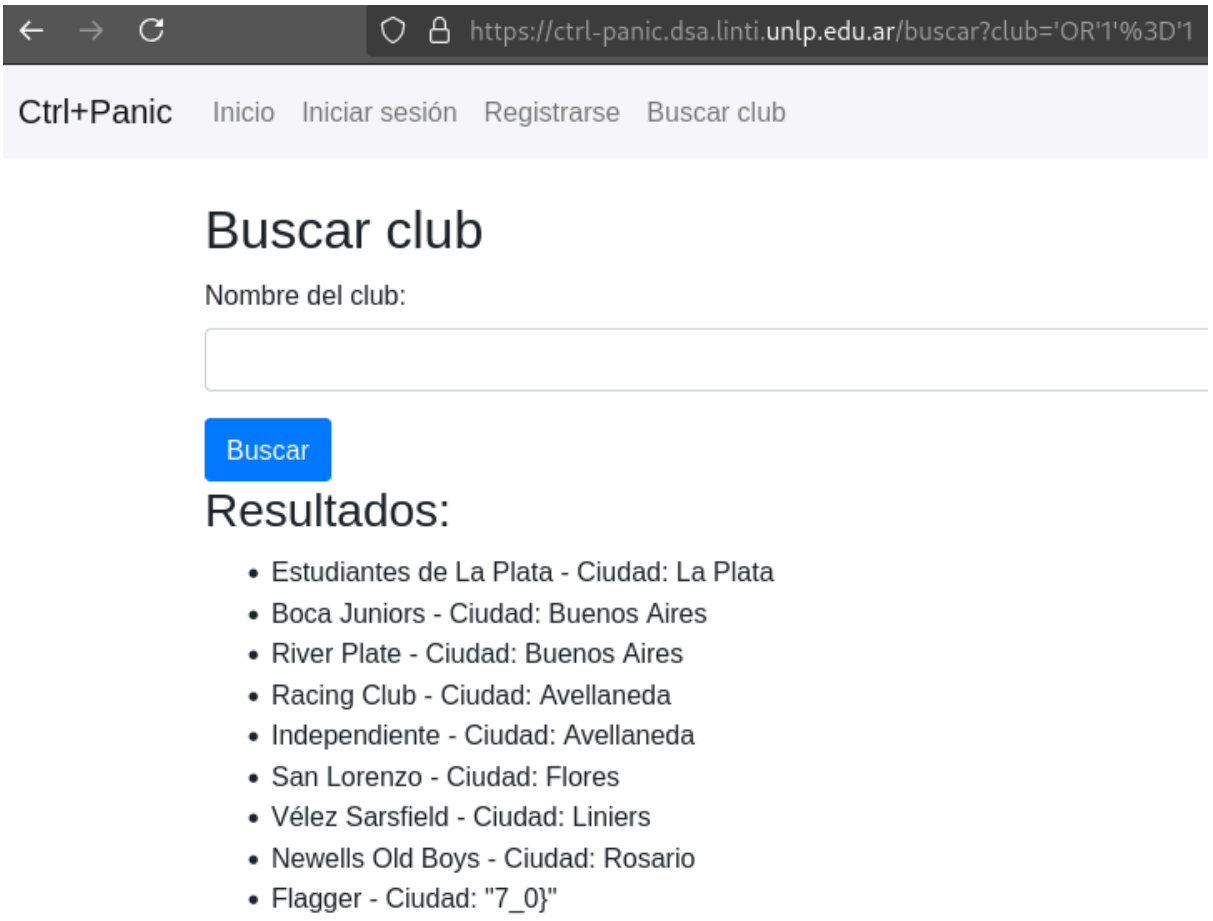
flag{memoria_Ctrl+P

Además, nos da una pista con respecto al usuario DSA. Se realiza ataque de fuerza bruta con un diccionario sobre el mismo, con la ayuda de la herramienta de hydra, obteniendo lo siguiente:

Contraseña: **123456789**
Una vez logueado, el servidor redirige al perfil 126 obteniendo lo siguiente:

Se encuentra la 2da parte de la flag:
anic_Rules_

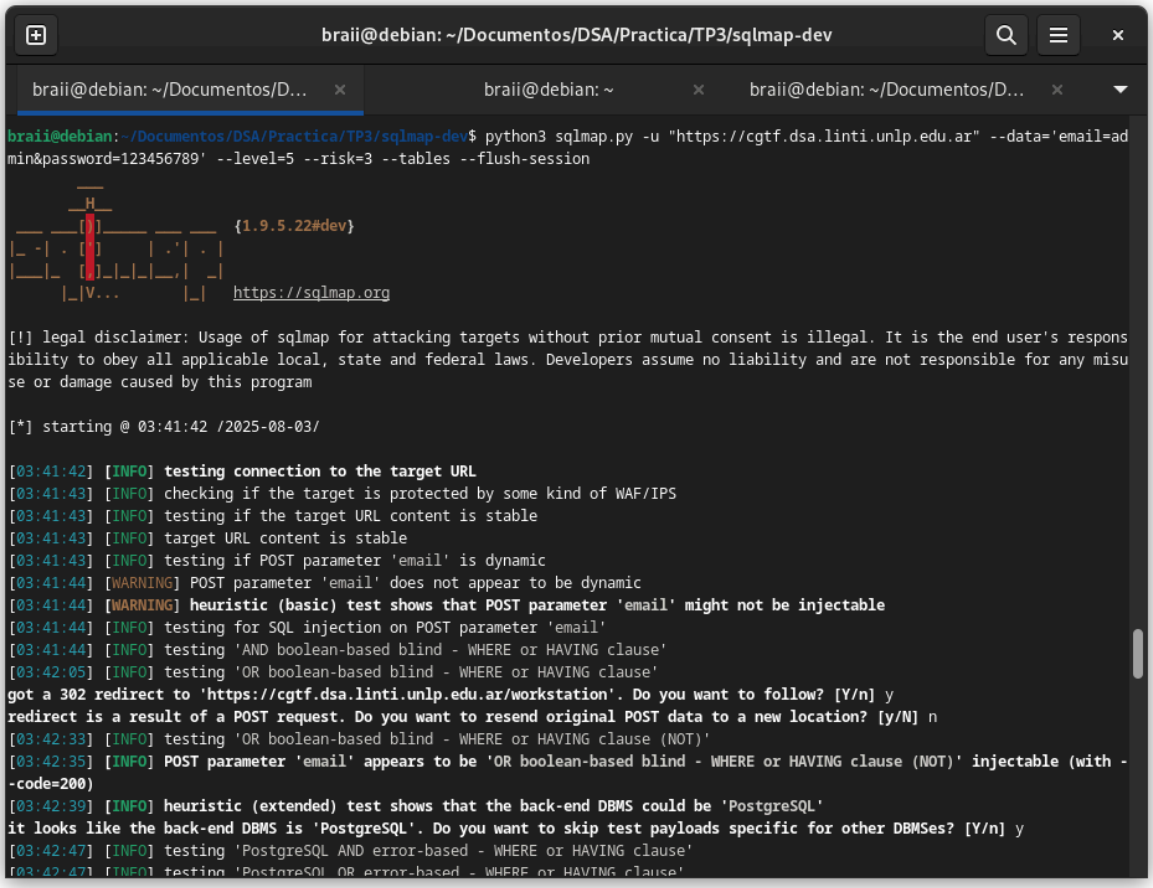
En el buscador se realiza inyección sql:

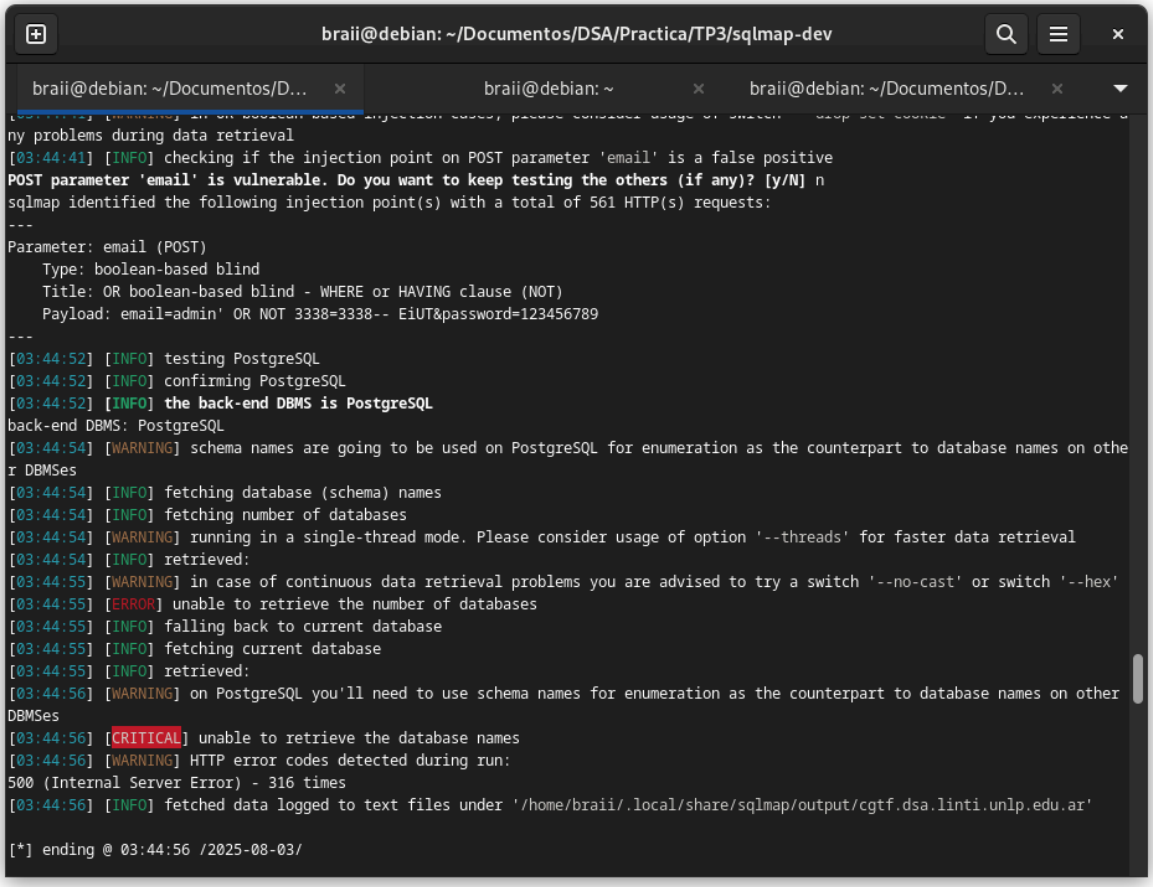


Flagger - Ciudad: "7_0}"

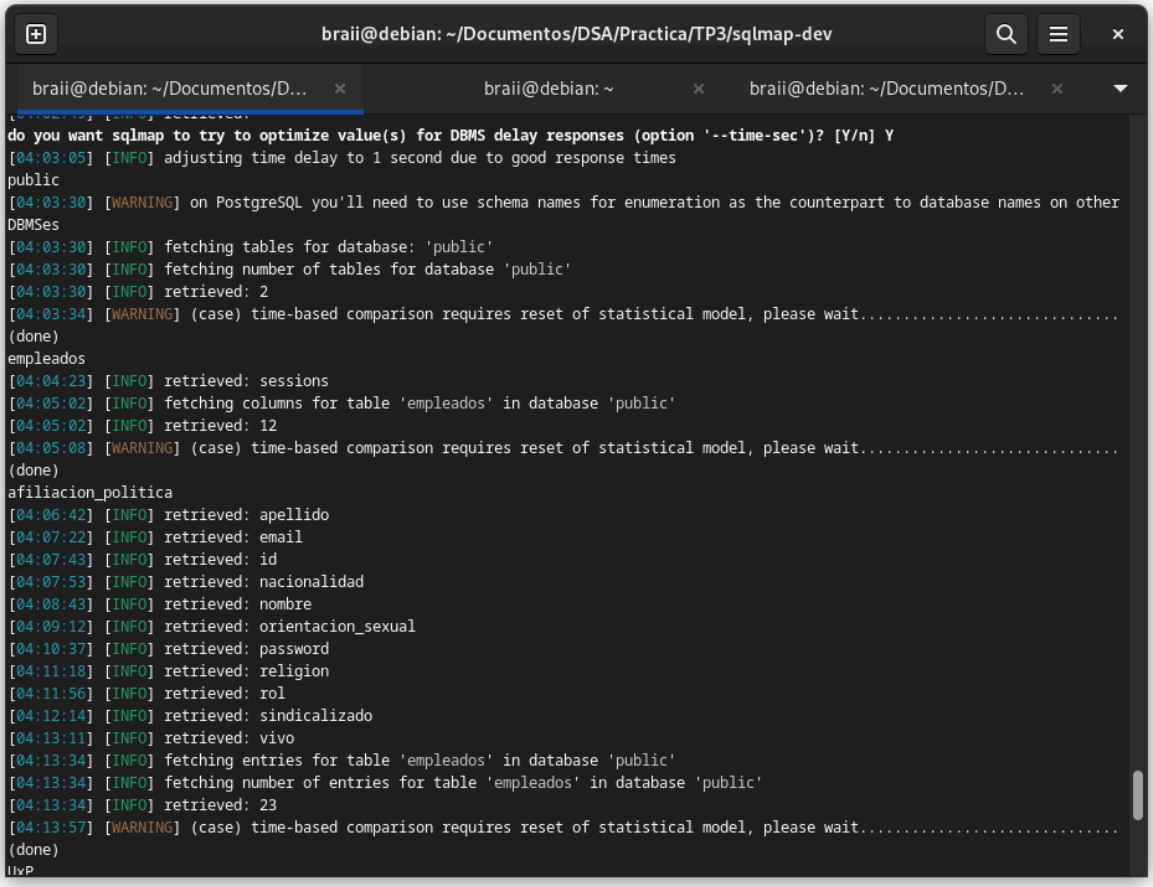
Luego de un intento fallido, se resuelve que la flag es:
flag{memoria_Ctrl+Panic_Rules_”7_0}

CGTF
Se realizaron varias pruebas





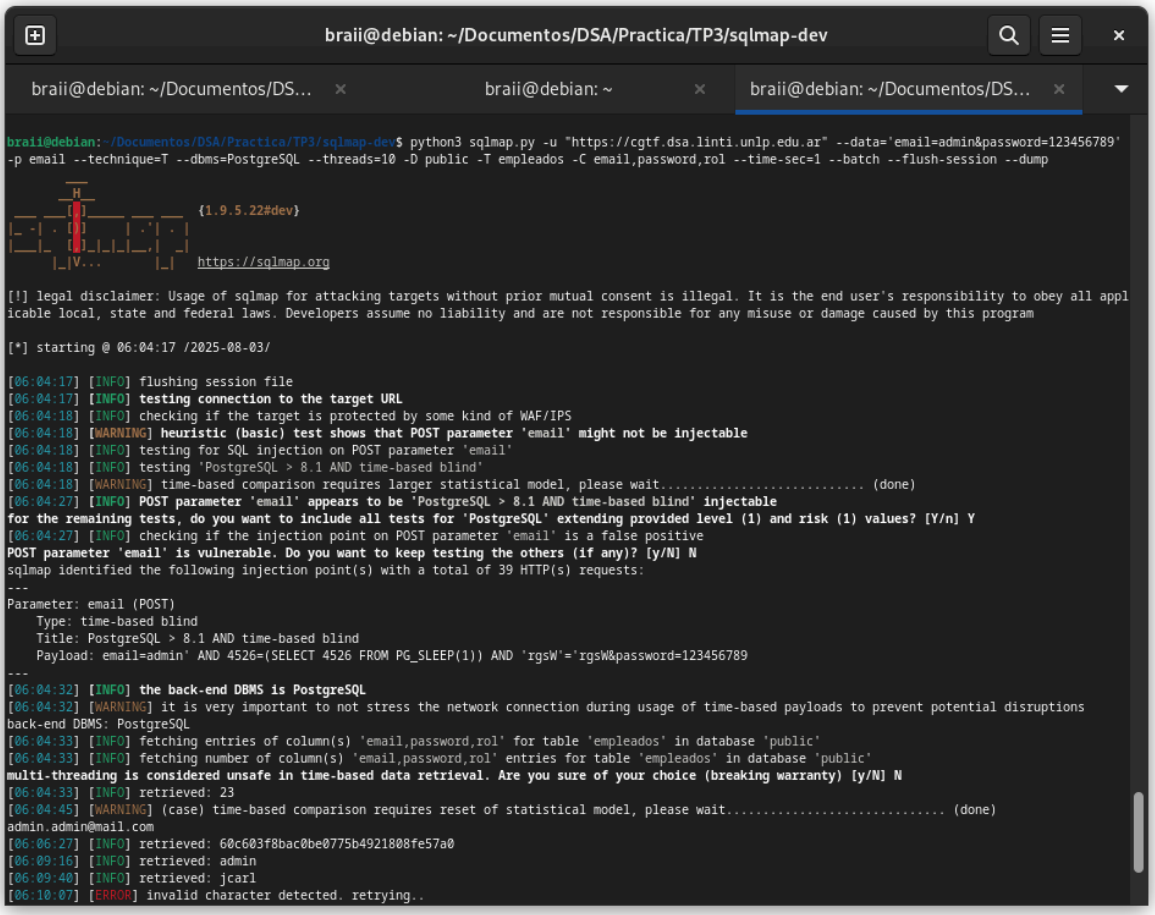
Luego de varias, se concluye que la dbms es PostgreSQL y se debe realizar una inyección sql del tipo basado en error:



Al ser time-based, las respuestas tardan al menos 1 segundo en obtener cada caracter de la tabla, por lo que una vez que se obtuvo el nombre de la tabla y las columnas necesarias se concluye y ejecuta el siguiente comando:

```
python3 sqlmap.py -u "https://cgtf.dsa.linti.unlp.edu.ar"
--data='email=admin&password=123456789' -p email --technique=T
--dbms=PostgreSQL --threads=10 -D public -T empleados -C
email,password,rol --time-sec=1 --batch --flush-session --dump
```

Obteniendo lo siguiente:



Para el usuario admin.admin@mail.com de rol admin, se obtiene la siguiente clave:
60c603f8bac0be0775b4921808fe57a0
Que utilizando la herramienta para reconocer a qué codificación pertenece se concluye que es md5, obteniendo la siguiente clave:
sodastereo
De ese modo, se procede a loguearse dentro de la página, obteniendo junto a los usuarios del sistema la flag:
FLAG{CGTF_es_la_FLAG_COMPLETA}