

```
kali@LAPTOP-GIBQHBQF: ~ x Windows PowerShell x + v  
Disallow: ./env  
  
[(kali㉿LAPTOP-GIBQHBQF)-[~]] $ cat passwords.txt  
# TechCorp Solutions - Password Archive  
# Data: 2024-01-15  
# CONFIDENCIAL - NÃO COMPARTILHAR  
  
SSH Server Credentials:  
- User: techcorp  
- Password: TechCorp2024!  
  
FTP Admin:  
- User: ftpadmin  
- Password: ftp@dm1n123  
  
Database Backup User:  
- User: backup_user  
- Password: B4ckup_S3cr3t_2024  
  
WiFi Office:  
- SSID: TechCorp_Corporate  
- Password: TechC0rp_W1F1_2024  
  
VPN Access:  
- Username: vpn_user  
- Password: VPN_P4ssw0rd!  
  
FLAG{p4ssw0rd_f1l3_d1sc0v3ry}  
# NOTA: Estas senhas devem ser trocadas mensalmente!  
# Última atualização: 15/01/2024  
[(kali㉿LAPTOP-GIBQHBQF)-[~]] $
```



```
File: /Users/josemenezes/Desktop/Relatório Anual 2025 - 2026/Relatório Anual 2025 - 2026.pdf
Last login: Fri Nov 28 20:29:57 on console
josemenezes@Joses-MacBook-Pro [22:34:25] [~]
-> % nmap 98.88.106.35
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-28
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 up
Ping Scan Timing: About 99.99% done; ETC: 22:34 (0:00)
Note: Host seems down. If it is really up, but blocking
Nmap done: 1 IP address (0 hosts up) scanned in 3.06
josemenezes@Joses-MacBook-Pro [22:34:37] [~]
-> %

josemenezes@Joses-MacBook-Pro [22:34:37] [~]
-> %
```

```
kali@LAPTOP-GIBQHBQF: ~ + 
</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 TI</h3>
            <p>Expertise técnica para seu negócio</p>
        </div>
    </div>
</section>

<footer>
    <div class="container">
        <p>&copy; 2024 TechCorp Solutions. Todos os direitos reservados.</p>
        <!-- FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n} -->
        <p>Desenvolvido por nossa equipe interna</p>
    </div>
</footer>
</body>
</html>
-(kali@LAPTOP-GIBQHBQF)-[~]
```

This is an experimental AI feature and won't always get it right.

```
kali@LAPTOP-GIBQHBQF: ~      Windows PowerShell  
=====  
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}  
[(kali㉿LAPTOP-GIBQHBQF)-[~]]$ cat usuarios.txt  
admin  
root  
user  
ctf  
guest  
[(kali㉿LAPTOP-GIBQHBQF)-[~]]$ cat users.conf  
# vsftpd user configuration  
# FLAG{c0nf1g_f113_r34d}  
  
anonymous:password123  
ftpadmin:ftp@dm1n123  
techcorp:TechCorp2024!  
guest:guest123  
[(kali㉿LAPTOP-GIBQHBQF)-[~]]$ |  
6
```

```
kali@LAPTOP-GIBQHBFQF:~ x + ~
rw-r--r-- 1 kali kali 0 Nov 11 11:25 http_requests.txt
drwxr-xr-x 3 kali kali 4096 Nov 5 17:37 .java
drwxr-xr-x 2 kali kali 4096 Nov 19 01:21 lab_ctf01
drwxr-xr-x 4 kali kali 4096 Nov 7 18:41 .local
-rw-r--r-- 1 kali kali 5758976 Dec 1 16:11 log_pentest_98.95.207.28_20251201_1557.log
-rw-r--r-- 1 kali kali 28672 Dec 1 16:14 log_pentest_98.95.207.28_20251201_1610.log
-rw-r--r-- 1 kali kali 5758976 Dec 1 16:11 log_pentest_98.95.207.28_.log
drwxr-xr-x 1 kali kali 0 Nov 19 01:19 logs_evidencias.txt
drwxr-xr-x 2 kali kali 4096 Nov 7 13:17 nmap
-rw-r--r-- 1 kali kali 0 Nov 10 22:16 page.html
drwxr-xr-x 3 kali kali 542 Nov 17 11:28 passwords.txt
drwxr-xr-x 2 kali kali 4096 Nov 6 22:39 pentest
drwxr-xr-x 3 kali kali 4096 Nov 7 18:44 pentest_54.91.129.121_5000
drwxr-xr-x 1 kali kali 4096 Nov 10 22:24 pentest_evidence
-rw-r--r-- 1 kali kali 0 Nov 11 11:27 post_data.txt
-rw-r--r-- 1 kali kali 807 Nov 5 17:37 .profile
-rw-r--r-- 1 kali kali 208 Nov 17 11:28 readme.txt
-rw-r--r-- 1 kali kali 30 Nov 11 10:45 robots.txt
-rw-r--r-- 1 tcpdump tcpdump 31909 Nov 13 04:01 scan_capture.pcap
-rw-r--r-- 1 kali kali 150 Nov 11 10:45 sitemap.xml
drwx----- 2 kali kali 4096 Nov 17 23:26 .ssh
-rw-r--r-- 1 kali kali 0 Nov 5 17:56 .sudo_as_admin_successful
-rw-r--r-- 1 kali kali 135 Nov 17 11:28 users.conf
-rw-r--r-- 1 kali kali 26 Nov 19 14:57 usuarios.txt
-rw-r--r-- 1 kali kali 329 Nov 17 11:28 welcome.txt
-rw-r--r-- 1 kali kali 336 Nov 5 17:37 .zprofile
-rw-r--r-- 1 kali kali 10855 Nov 5 17:37 .zshrc

(kali㉿LAPTOP-GIBQHBFQF)~[~]
$ |
```

Não seguro 06/05/2021 20:00:00 /index.php/routes/table/change/crop_techcorp_db/editable-users

pMyAdmin

Servidor: db:3306 » Banco de dados: techcorp_db » Tabela: users

Favoritos

Visualizar Estrutura SQL Procurar Inserir Exportar Importar Operações Ação Adm

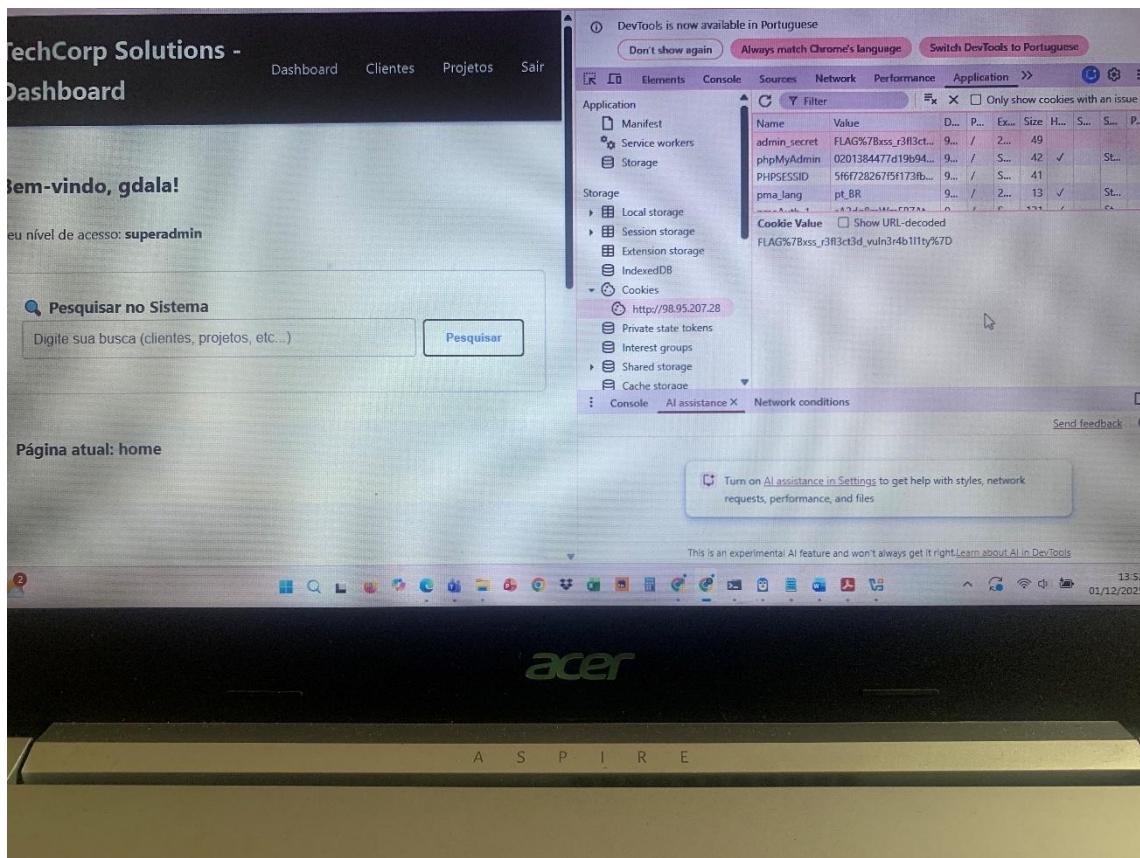
Coluna	Tipo	Função	Nulo	Valor
id	int			20
username	varchar(20)			gdala
password	varchar(255)			gd414sup3r4dmin
role	varchar(20)			superadmin
created_at	timestamp			2025-12-01 13:07:42

Executar

Ignorar

Coluna	Tipo	Função	Nulo	Valor
Console	int			

acer



```
kali㉿LAPTOP-GIBQHBFQ: ~ x Windows PowerShell x + ~
└─# ftp 98.95.207.28
Connected to 98.95.207.28.
220 (vsFTPd 3.0.5)
Name (98.95.207.28:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||21104|)
150 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   1118 Nov 17 14:28 Dockerfile
drwxr-xr-x  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> cd confidential
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||21104|)
150 Here comes the directory listing.
drwxr-xr-x  2 1000      1000   4096 Nov 17 14:28 .
drwxr-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> cat passwords.txt
?Invalid command.
ftp> echo passwords.txt
?Invalid command.
```

13:54 01/12/2025

```
kali@LAPTOP-GIBQHBFQ: ~ x Windows PowerShell x + 
ftp> get passwords.txt
Not connected.
ftp> exit
└─(kali㉿LAPTOP-GIBQHBFQ)-[~]
$ cat passwords.txt
# TechCorp Solutions - Password Archive
# Data: 2024-01-15
# CONFIDENCIAL - NÃO COMPARTELHAR

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

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

Database Backup User:
- User: backup_user
- Password: B4ckup_S3cr3t_2024

WiFi Office:
- SSID: TechCorp_Corporate
- Password: TechCorp_WiFi_2024

VPN Access:
- Username: vpn_user
- Password: VPN_P4ssw0rd!

FLAG{p4ssw0rd_f1ll3_d1sc0v3ry}

# NOTA: Estas senhas devem ser trocadas mensalmente!
# Última atualização: 15/01/2024

12:53 01/12/2024
```

```
kali@LAPTOP-GIBQHBFQ: ~ x + 
└─(kali㉿LAPTOP-GIBQHBFQ)-[~]
$ curl -s http://98.95.207.28/config.php
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.54 (Debian) Server at 98.95.207.28 Port 80</address>
</body></html>

└─(kali㉿LAPTOP-GIBQHBFQ)-[~]
$ curl -s http://98.95.207.28/config/database.php.txt
<?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}
?>
```

kali@LAPTOP-GIBQHBF: ~ x Windows PowerShell x + v

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 25.82 seconds

```
(kali㉿LAPTOP-GIBQHBF)-[~]
└─$ nmap -p 98.95.207.28 21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 18:40 -03
Error #487: Your port specifications are illegal. Example of proper form: "-180,200-1024,T:3000-4000,U:60000--"
QUITTING!
```

```
(kali㉿LAPTOP-GIBQHBF)-[~]
└─$ nmap -p 21 --scriptftp-anon 98.95.207.28
/usr/lib/nmap/nmap: unrecognized option '--scriptftp-anon'
See the output of nmap -h for a summary of options.
```

```
(kali㉿LAPTOP-GIBQHBF)-[~]
└─$ nmap -p 21 --script ftp-anon 98.95.207.28
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 18:45 -03
Nmap scan report for ec2-98-95-207-28.compute-1.amazonaws.com (98.95.207.28)
Host is up (0.16s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_.Can't get directory listing: PASV IP 172.20.0.20 is not the same as 98.95.207.28

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
```

```
(kali㉿LAPTOP-GIBQHBF)-[~]
└─$ ftp 98.95.207.28
Connected to 98.95.207.28.
220 (vsFTPD 3.0.5)
Name (98.95.207.28:kali): admin
ftp: lostpeer due to signal 13
```



The image shows a laptop screen displaying a terminal session on Kali Linux. The terminal window is titled 'Windows PowerShell' and contains several commands and their outputs related to a network scan and an FTP session. The background of the screen shows the Windows desktop environment with various icons and the Acer logo at the bottom.

kali1 [Executando] - Oracle VirtualBox

Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

Sessão Ações Editar Exibir Ajuda

```
<footer>
    <div class="container">
        <p>&copy; 2024 TechCorp Solutions. Todos os direitos reservados.
    </div>
</footer>
</body>
</html>
```

(gdala@kali1)-[~]

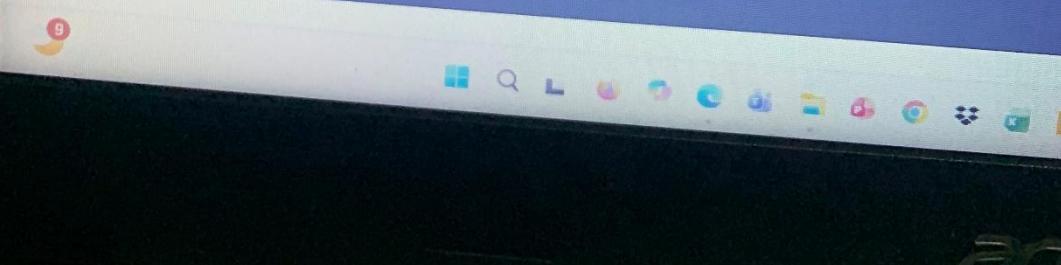
```
$ curl http://98.95.207.28/.ht_wsr.txt
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.54 (Debian) Server at 98.95.207.28 Port 80</address>
```

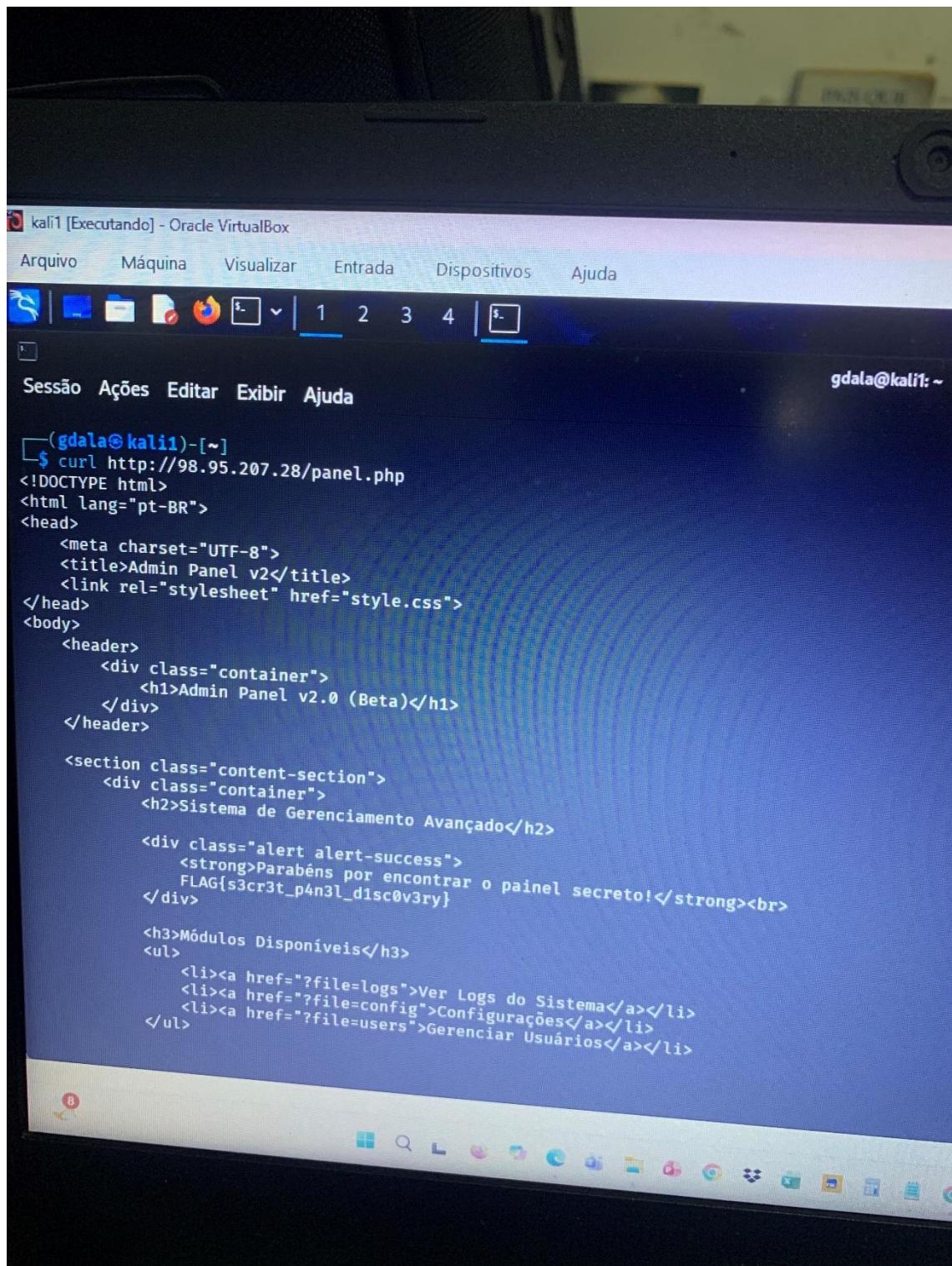
(gdala@kali1)-[~]

```
$ curl http://98.95.207.28/.git-credentials
https://admin:gh_p4t_S3cr3tT0k3n_2024_TechCorp@github.com
# FLAG{git_cr3d3nt14ls_l34k}
```

(gdala@kali1)-[~]

```
$
```

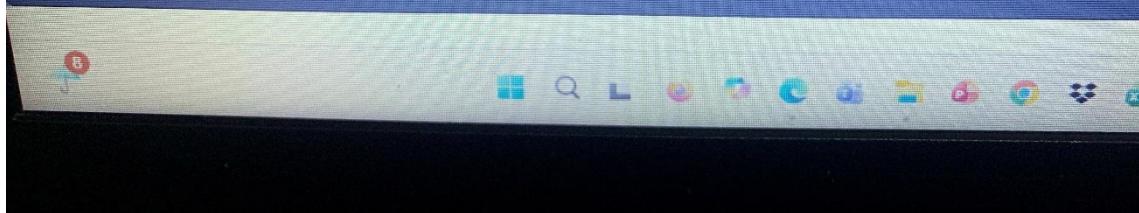




```
</div>
<div class="feature-box">
    <h3>Consultoria TI</h3>
    <p>Expertise técnica para seu negócio</p>
</div>
</div>
</section>

<footer>
    <div class="container">
        <p>&copy; 2024 TechCorp Solutions. Todos os direitos reservados.<br/>
        <!-- FLAG{b4sic_s0urc3_c0d3_insp3ct10n} -->
        <p>Desenvolvido por nossa equipe interna</p>
    </div>
</footer>
</body>
</html>

(gdala㉿kali1)-[~]
```



kali1 [Executando] - Oracle VirtualBox

Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

Sessão Ações Editar Exibir Ajuda

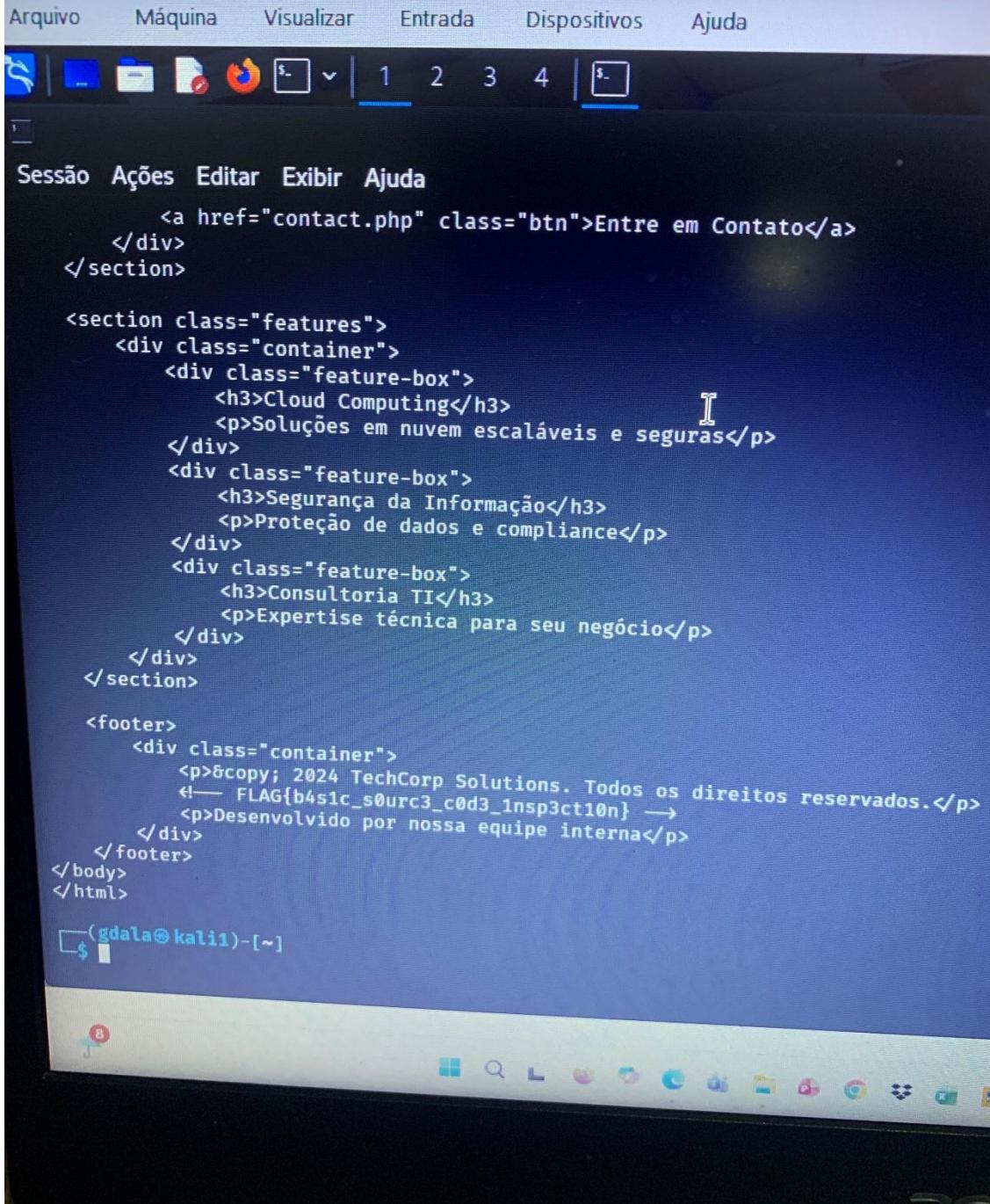
```
<a href="contact.php" class="btn">Entre em Contato</a>
</div>
</section>

<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 TI</h3>
<p>Expertise técnica para seu negócio</p>
</div>
</div>
</section>

<footer>
<div class="container">
<p>&copy; 2024 TechCorp Solutions. Todos os direitos reservados.</p>

<p>Desenvolvido por nossa equipe interna</p>
</div>
</footer>
</body>
</html>
```

\$



The screenshot shows a terminal window running on a Kali Linux system within an Oracle VirtualBox environment. The terminal displays a portion of an HTML file with several sections and a footer. A cursor is positioned over the word 'seguras' in the first feature box. The terminal prompt '\$' is visible at the bottom. The window title is 'kali1 [Executando] - Oracle VirtualBox'. The menu bar includes 'Arquivo', 'Máquina', 'Visualizar', 'Entrada', 'Dispositivos', and 'Ajuda'. The toolbar contains icons for file operations like cut, copy, paste, and search, along with tabs for multiple windows.

```
221 Goodbye.  
  
[kali㉿LAPTOP-GIBQHBQF:~]$ cat 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}  
[kali㉿LAPTOP-GIBQHBQF:~]$
```

```
der>  
<div class="container">  
    <h1>Admin Panel v2.0 (Beta)</h1>  
</div>  
ader>  
  
tion class="content-section">  
<div class="container">  
    <h2>Sistema de Gerenciamento Avançado</h2>  
  
    <div class="alert alert-success">  
        <strong>Parabéns por encontrar o painel secreto!</strong><br>  
        FLAG{s3cr3t_p4n3l_d1sc0v3ry}<br>  
    </div>  
  
    <h3>Módulos Disponíveis</h3>  
    <ul>  
        <li><a href="?file=logs">Ver Logs do Sistema</a></li>  
        <li><a href="?file=config">Configurações</a></li>  
        <li><a href="?file=users">Gerenciar Usuários</a></li>  
    </ul>
```

kali1 [Executando] - Oracle VirtualBox

Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

gdala@kali1: ~

Sessão Ações Editar Exibir Ajuda

[20:35:28] Starting:

```
[20:35:34] 200 - 87B - ./git-credentials
[20:35:35] 403 - 277B - ./ht_wsr.txt
[20:35:35] 403 - 277B - ./htaccess.bak1
[20:35:35] 403 - 277B - ./htaccess_extra
[20:35:35] 403 - 277B - ./htaccess.orig
[20:35:35] 403 - 277B - ./htaccess_orig
[20:35:35] 403 - 277B - ./htaccess.sample
[20:35:35] 403 - 277B - ./htaccess_sc
[20:35:35] 403 - 277B - ./htaccess.save
[20:35:35] 403 - 277B - ./htaccessBAK
[20:35:35] 403 - 277B - ./htaccessOLD
[20:35:35] 403 - 277B - ./htaccessOLD2
[20:35:35] 403 - 277B - ./htm
[20:35:35] 403 - 277B - ./html
[20:35:35] 403 - 277B - ./htpasswd_test
[20:35:35] 403 - 277B - ./htpasswd
[20:35:35] 403 - 277B - ./httr-oauth
[20:35:44] 200 - 690B - /about.php
[20:35:48] 302 - 0B - /admin.php -> login.php
[20:36:05] 301 - 313B - /config -> http://98.95.207.28/config/
[20:36:06] 200 - 485B - /config/
[20:36:07] 200 - 815B - /contact.php
[20:36:09] 302 - 0B - /dashboard.php -> login.php
[20:36:28] 200 - 657B - /login.php
[20:36:29] 302 - 0B - /logout.php -> index.php
[20:36:38] 200 - 616B - /panel.php
[20:36:48] 200 - 140B - /robots.txt
[20:36:50] 403 - 277B - /server-status/
[20:36:50] 403 - 277B - /server-status/
```

Right Control

```
221 Goodbye.

[kali㉿LAPTOP-GIBQHBQF) - [~]
$ cat 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}

[kali㉿LAPTOP-GIBQHBQF) - [~]

# CONFIDENCIAL - NÃO COMPARTILHAR

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

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

Database Backup User:
- User: backup_user
- Password: B4ckup_S3cr3t_2024

WiFi Office:
- SSID: TechCorp_Corporate
- Password: TechC0rp_W1F1_2024

VPN Access:
- Username: vpn_user
- Password: VPN_P4ssw0rd!

FLAG{p4ssw0rd_f1l3_d1sc0v3ry}

# NOTA: Estas senhas devem ser trocadas mensalmente!
# Última atualização: 15/01/2024
```

```
drwxr-xr-x 2 1000 1000 4096 Nov 17 14:28 confider
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-rxr-xr-x 1 1000 1000 135 Nov 17 14:28 users.conf
-rw-rxr-xr-x 1 1000 1000 329 Nov 17 14:28 welcome.txt
226 Directory send OK.
ftp> cat confidential
?Invalid command.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||21110|)
550 Failed to open file.
ftp> |
```

The image shows a laptop screen with three windows:

- Top Terminal:** An FTP session with the server at 98.95.207.28. It lists files in the current directory and attempts to download a file named "flag.txt".
- Middle Terminal:** A curl command is run against port 3000 to fetch a JSON package file.
- Bottom Terminal:** A curl command is run against port 80 to fetch the robots.txt file.
- Browser Window:** A browser tab is open to the URL 98.95.207.28/index.php. The page displays a 404 Not Found error message, indicating the requested URL was not found on the server. The page also includes standard Apache server information.

```
[kali㉿LAPTOP-GIBQHBF: ~]  Windows PowerShell
tp> get passwords.txt
ot connected.
tp> exit
--(kali㉿LAPTOP-GIBQHBF: ~]
-$ cat passwords.txt
TechCorp Solutions - Password Archive
Data: 2024-01-15
CONFIDENCIAL - NÃO COMPARTILHAR

SH Server Credentials:
User: techcorp
Password: TechCorp2024!

TP Admin:
User: ftpadmin
Password: ftp@dmin123

atabase Backup User:
User: backup_user
Password: B4ckup_S3cr3t_2024

iFi Office:
SSID: TechCorp_Corporate
Password: TechC0rp_WiFl_2024

PN Access:
Username: vpn_user
Password: VPN_P4ssw0rd!

LAG{p4ssw0rd_f1l3_d1sc0v3ry}

NOTA: Estas senhas devem ser trocadas mensalmente!
Última atualização: 15/01/2024
--(kali㉿LAPTOP-GIBQHBF: ~]
-$ ftp 98.95.207.28
Connected to 98.95.207.28.
220 (vsFTPd 3.0.5)
Name (98.95.207.28:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||21104|)
50 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 ..
rwxr-xr-x  1 1000      1000      1110 Nov 17 14:28 Dockerfile
rwxr-xr-x  2 1000      1000      4096 Nov 17 14:28 confidential
rwxr-xr-x  4 0          0          4096 Nov 17 17:55 ftp
rwxr-xr-x  2 1000      1000      4096 Nov 17 14:28 public
rwxr-xr-x  1 1000      1000      135 Nov 17 14:28 users.conf
rwxr-xr-x  1 1000      1000      329 Nov 17 14:28 welcome.txt
226 Directory send OK.
ftp> cd confidential
500 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||21100|)
50 Here comes the directory listing.
drwxr-xr-x  2 1000      1000      4096 Nov 17 14:28 .
drwxr-xr-x  5 1000      1000      4096 Nov 17 17:55 ..
rwxr-xr-x  1 1000      1000      542 Nov 17 14:28 passwords.txt
226 Directory send OK.
ftp> cat passwords.txt
Invalid command.
ftp> echo passwords.txt
Invalid command.
```

```

└─(kali㉿LAPTOP-GIBQHBQF)-[~]
$ ftp 98.95.207.28
Connected to 98.95.207.28.
20 (vsFTPd 3.0.5)
Name (98.95.207.28:kali): anonymous
31 Please specify the password.
password:
30 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
tp> ls -la
29 Entering Extended Passive Mode (|||21104|)
50 Here comes the directory listing.
rwxr-xr-x 5 1000 1000 4096 Nov 17 17:55 .
rwxr-xr-x 5 1000 1000 4096 Nov 17 17:55 ..
rwxr-xr-x 1 1000 1000 1110 Nov 17 14:28 Dockerfile
rwxr-xr-x 2 1000 1000 4096 Nov 17 14:28 confidential
rwxr-xr-x 4 0 0 4096 Nov 17 17:55 ftp
rwxr-xr-x 2 1000 1000 4096 Nov 17 14:28 public
rwxr-xr-x 1 1000 1000 135 Nov 17 14:28 users.conf
rwxr-xr-x 1 1000 1000 329 Nov 17 14:28 welcome.txt
26 Directory send OK.
tp> cd confidential
50 Directory successfully changed.
tp> ls -la
29 Entering Extended Passive Mode (|||21100|)
50 Here comes the directory listing.
rwxr-xr-x 2 1000 1000 4096 Nov 17 14:28 .
rwxr-xr-x 5 1000 1000 4096 Nov 17 17:55 ..
rwxr-xr-x 1 1000 1000 542 Nov 17 14:28 passwords.txt
26 Directory send OK.
tp> cat passwords.txt
Invalid command.
tp> echo passwords.txt
Invalid command.

└─(kali㉿LAPTOP-GIBQHBQF)-[~]
$ nmap -p 98.95.207.28 21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 18:40 -03
Error #487: Your port specifications are illegal. Example of proper form: "-100,200-1024,T:3000-4000,U:60000--"
QUITTING!
└─(kali㉿LAPTOP-GIBQHBQF)-[~]
$ nmap -p 21 --scriptftp-anon 98.95.207.28
/usr/lib/nmap/nmap: unrecognized option '--scriptftp-anon'
See the output of nmap -h for a summary of options.

└─(kali㉿LAPTOP-GIBQHBQF)-[~]
$ nmap -p 21 --script ftp-anon 98.95.207.28
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 18:45 -03
Nmap scan report for ec2-98-95-207-28.compute-1.amazonaws.com (98.95.207.28)
Host is up (0.16s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_.Can't get directory listing: PASV IP 172.20.0.20 is not the same as 98.95.207.28

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds

└─(kali㉿LAPTOP-GIBQHBQF)-[~]
$ ftp 98.95.207.28
Connected to 98.95.207.28.
220 (vsFTPd 3.0.5)
Name (98.95.207.28:kali): admin
ftp: lostpeer due to signal 13

```

Não seguro 98.95.207.28:8080/index.php?route=/sql&db=techcorp_db&tabela=secret_data&pos=0

Ação necessária

phpMyAdmin

Servidor: db.3306 » Banco de dados: techcorp_db » Tabela: secret_data

Visualizar Estrutura SQL Procurar Inserir Exportar Importar Operações Acionadores

Recente Favoritos

information_schema

Views

performance_schema

techcorp_db

Tabelas

Nova clients contacts secret_data users Views

Mostrando registros 0 - 3 (4 no total, Consulta levou 0.0000 segundos.)

SELECT * FROM `secret_data`

Perfil [Editar em linha] [Editar] [Demonstrar SQL] [Criar código PHP] [Atualizar]

Mostrar tudo Número de linhas: 25 Filtrar linhas: Procurar nesta tabela Ordenar pela chave: Nenhum

Opções extras

	id	secret_key	secret_value	created_at
<input type="checkbox"/>	1	database_flag	FLAG{sql_1nj3ct10n_m4st3t}	2025-11-17 14:30:36
<input type="checkbox"/>	2	admin_token	FLAG{h1dd3n_d4t4_1n_d4t4b4s3}	2025-11-17 14:30:36
<input type="checkbox"/>	3	api_secret	sk_prod_A7x9mP2qR5tY0wZ3vC6nB4jK1IM0hG	2025-11-17 14:30:36
<input type="checkbox"/>	4	backup_path	/var/backups/techcorp/backup_20240115.tar.gz	2025-11-17 14:30:36

↑ Marcar todos Com marcados: Editar Copiar Remover Exportar

Mostrar tudo Número de linhas: 25 Filtrar linhas: Procurar nesta tabela Ordenar pela chave: Nenhum

Operações resultantes das consultas

Imprimir Copiar para a área de transferência Exportar Exibir gráfico Criar view

Não seguro 98.95.207.28/dashboard.php

Ação necessária

TechCorp Solutions - Dashboard

Bem-vindo, gdala!

Seu nível de acesso: superadmin

Pesquisar no Sistema

Digite sua busca (clientes, projetos, etc...)

Pesquisar

Página atual: home

```
kali㉿LAPTOP-GIBQHBQF: ~ + 
└$ gobuster dir -u http://98.95.207.28/ -w /usr/share/dirb/wordlists/common.txt
=====
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://98.95.207.28/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.8
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta           (Status: 403) [Size: 277]
/.htaccess      (Status: 403) [Size: 277]
/.htpasswd      (Status: 403) [Size: 277]
/admin.php      (Status: 302) [Size: 0] [--> login.php]
/config         (Status: 301) [Size: 313] [--> http://98.95.207.28/config/]
/index.php      (Status: 200) [Size: 2081]
/robots.txt     (Status: 200) [Size: 169]
/server-status  (Status: 403) [Size: 277]
Progress: 4613 / 4613 (100.00%)
=====
Finished
```

```
[kali㉿LAPTOP-GIBQHBQF]:~]$ nmap -sV -p 3306 --script=mysql-info 98.95.207.28
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 10:35 -03
Nmap scan report for ec2-98-95-207-28.compute-1.amazonaws.com (98.95.207.28)
Host is up (0.14s latency).

PORT      STATE SERVICE VERSION
3306/tcp   open  mysql  MySQL 8.0.44
| mysql-info:
|_ Protocol: 10
| Version: 8.0.44
| Thread ID: 133816
| Capabilities flags: 65535
| Some Capabilities: SupportsLoadDataLocal, IgnoreSigpipes, Speaks41ProtocolNew, ConnectWithDatabase, InteractiveClient, SwitchToSSLAfterHandshake
| LongColumnFlag, LongPassword, SupportsTransactions, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolOld, Support41Auth, ODBCClient, SupportsCompression, DontAllowDatabaseTableColumn, FoundRows, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
| Status: Autocommit
| Salt: P-\x05zdBdNjqDlc\x1A\x1C<LS\x1E'B
|_ Auth Plugin Name: caching_sha2_password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.89 seconds

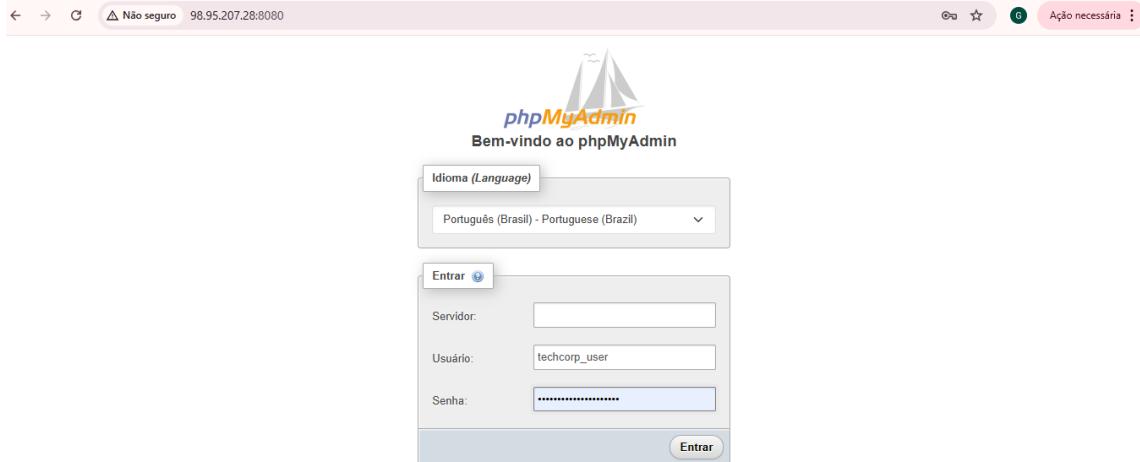
[kali㉿LAPTOP-GIBQHBQF]:~]$ nmap -Pn -sV 98.95.207.28
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 10:40 -03
Nmap scan report for ec2-98-95-207-28.compute-1.amazonaws.com (98.95.207.28)
Host is up (0.15s latency).

Not shown: 994 filtered tcp ports (no-response)

PORT      STATE SERVICE VERSION
20/tcp    closed  ftp-data
21/tcp    open   ftp    vsftpd 3.0.5
80/tcp    open   http   Apache httpd 2.4.54 ((Debian))
2222/tcp  open   ssh    OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
3306/tcp  open   mysql  MySQL 8.0.44
8080/tcp  open   http   Apache httpd 2.4.65 ((Debian))

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.75 seconds
```



This screenshot displays the configuration interface of phpMyAdmin. The top navigation bar includes links for 'Servidor: db 3306', 'Bancos de dados', 'SQL', 'Status', 'Exportar', 'Importar', 'Configurações', 'Variáveis', 'Charsets', 'Motores', and 'Plugins'. On the left, a sidebar lists databases: 'information_schema', 'performance_schema', and 'techcorp_db'. The main content area is divided into several sections: 'Configurações gerais' (General Configuration) showing 'Alterar a senha' (Change password) and 'Collation de conexão do servidor MySQL:' set to 'utf8mb4_unicode_ci'; 'Configurações do Tema' (Theme Configuration) showing 'Idioma (Language)' set to 'Português (Brasil) - Portuguese (Brazil)', 'Tema' set to 'pmahomme', and a 'Ver todos' (View all) button; 'Servidor de banco de dados' (Database Server) listing server details like 'Servidor: db via TCP/IP', 'Tipo de servidor: MySQL', and 'Conexão do servidor: O SSL não está sendo usado' (SSL is not being used); 'Servidor web' (Web Server) listing web server details like 'Apache/2.4.65 (Debian)'; and a summary section 'phpMyAdmin' with links for 'Informações da versão: 5.2.3 (atualizado(a))' and 'Documentação'.