

VAI NA WEB
CURSO DE CIBERSEGURANÇA

RELATÓRIO PENTEST
TechCorp Solutions

Karyne Guinyver Dias da Silva

Brasília
23/11/2025

IMPORTANTE

Este documento contém informações confidenciais e privilegiadas, sendo seu sigilo protegido por lei.

Se você não for o destinatário autorizado, não deve utilizar, copiar ou divulgar qualquer conteúdo aqui presente.

Caso tenha recebido este documento por engano, notifique o remetente imediatamente e apague-o em seguida.

O presente relatório não deve ser enviado por e-mail, fax ou qualquer outro meio eletrônico sem aprovação prévia, conforme as políticas de segurança da contratante.

SUMÁRIO

IMPORTANTE.....	2
SUMÁRIO.....	3
1. ESCOPO.....	4
2. OBJETIVO DA PESQUISA.....	5
3. CONTATO.....	5
4. DECLARAÇÃO DE LIMITE DE RESPONSABILIDADE.....	6
5. DATA DOS TESTES.....	6
6. METODOLOGIA UTILIZADA.....	6
7. EVIDÊNCIAS E VULNERABILIDADES ENCONTRADAS.....	6
7.1 ACESSO INICIAL AO SITE.....	6
7.2 EXPOSIÇÃO DE INFORMAÇÃO NO CÓDIGO-FONTE.....	7
7.3 CREDENCIAIS EXPOSTAS NA TELA DE LOGIN.....	8
7.4 NAVEGAÇÃO INTERNA EXPONDO DADOS SENSÍVEIS.....	9
7.5 VARREDURA COM NMAP.....	10
7.6 FLAG E DIRETÓRIOS EXPOSTOS NO ARQUIVO ROBOTS.TXT.....	11
7.7 FTP SEM AUTENTICAÇÃO (ANONYMOUS LOGIN).....	12
7.8 ENUMERAÇÃO DE DIRETÓRIOS COM GOBUSTER.....	13
7.9 ACESSO AO DIRETÓRIO /CONFIG/.....	14
7.10 ACESSO AO DIRETÓRIO /CONFIG/DATABASE.PHP.TXT.....	15
8. CONCLUSÃO DO RELATÓRIO.....	17

1. ESCOPO

A equipe foi designada para conduzir um Penetration Test no ambiente CTF educacional disponibilizado em:

URL alvo: <http://98.95.207.28/>

Objetivos principais:

- Mapear a superfície de ataque
- Identificar e explorar vulnerabilidades web
- Avaliar configurações inseguras
- Coletar as flags distribuídas
- Demonstrar riscos reais decorrentes das falhas encontradas

Escopo técnico incluído:

- Avaliação da camada web
- Enumeração de diretórios e arquivos

- Varredura de portas e serviços
 - Exploração de credenciais expostas
 - Leitura de arquivos sensíveis
 - Coleta e documentação de flags
-

2. OBJETIVO DA PESQUISA

A pesquisa teve como finalidade:

- Identificar vulnerabilidades críticas acessíveis via HTTP
- Verificar falhas de autenticação, controle de sessão e exposição de informações
- Avaliar a robustez da configuração do servidor
- Demonstrar impactos reais de falhas encontradas
- Registrar todas as flags do ambiente

Este relatório documenta o processo completo, incluindo comandos utilizados e evidências técnicas.

3. CONTATO

Empresa alvo: TechCorp Solutions

Responsável técnico: José Carlos Menezes

Finalidade: Exercício acadêmico – Formação em Cibersegurança

4. DECLARAÇÃO DE LIMITE DE RESPONSABILIDADE

Todos os testes foram conduzidos exclusivamente no ambiente autorizado.

Nenhum teste foi realizado fora do escopo definido.

Não houve qualquer intenção de causar indisponibilidade, danos ou prejuízos.

5. DATA DOS TESTES

23 a 28 de Novembro de 2025

6. METODOLOGIA UTILIZADA

A metodologia aplicada seguiu padrões OWASP e PTES:

- Reconhecimento (recon)
- Enumeração
- Varredura
- Exploração
- Extração de evidências e flags
- Documentação técnica

7. EVIDÊNCIAS E VULNERABILIDADES ENCONTRADAS

7.1 ACESSO INICIAL AO SITE

A navegação inicial revelou exposição indevida de informações e ausência de controles de segurança fundamentais.

Vulnerabilidade identificada:

- Conteúdo sensível disponível sem autenticação
- Falta de segregação entre conteúdo público e interno



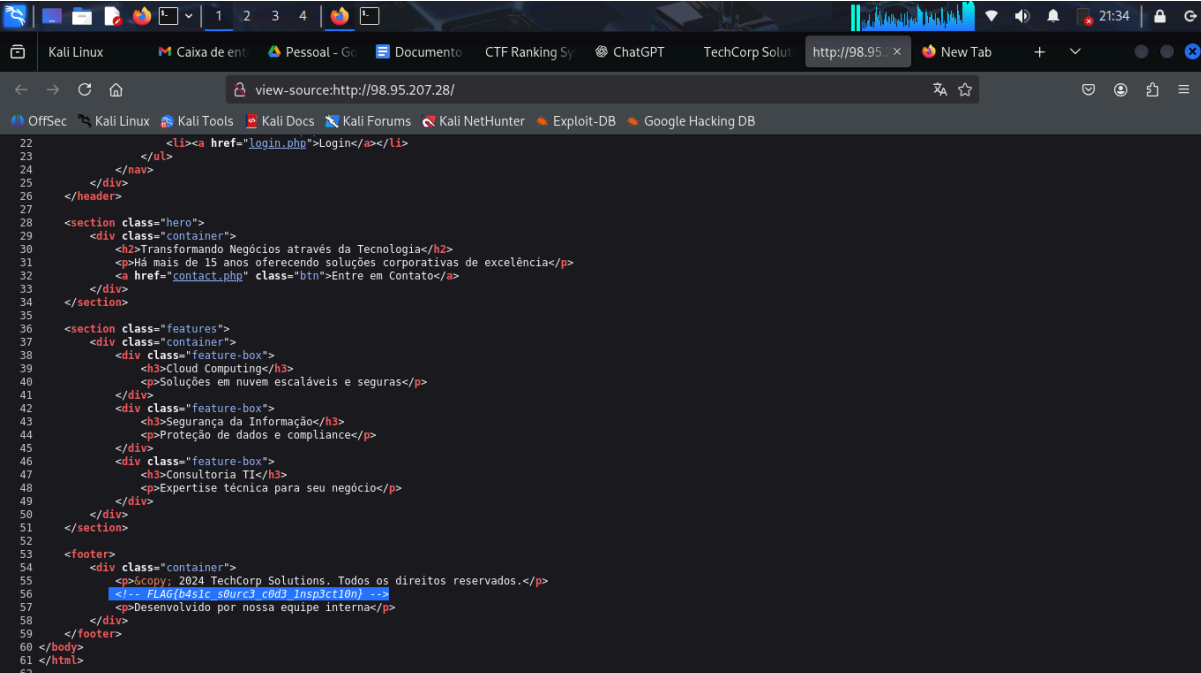
7.2 EXPOSIÇÃO DE INFORMAÇÃO NO CÓDIGO-FONTE

Ao exibir o código-fonte da página (CTRL + U), foi encontrada uma flag diretamente no HTML.

Impacto técnico:

- Vazamento decorrente de má validação
- Falha de controle do conteúdo entregue ao cliente
- Exposição de informações internas
- Facilidade de exploração para qualquer visitante

Classificação: OWASP A01 – Broken Access Control



```
22 <li><a href="login.php">Login</a></li>
23 </ul>
24 </div>
25 </div>
26 </div>
27 </div>
28 <section class="hero">
29 <div class="container">
30 <h2>Transformando Negócios através da Tecnologia</h2>
31 <p>Há mais de 15 anos oferecendo soluções corporativas de excelência</p>
32 <a href="contact.php" class="btn">Entre em Contato</a>
33 </div>
34 </section>
35
36 <section class="features">
37 <div class="container">
38 <div class="feature-box">
39 <h3>Cloud Computing</h3>
40 <p>Soluções em nuvem escaláveis e seguras</p>
41 </div>
42 <div class="feature-box">
43 <h3>Segurança da Informação</h3>
44 <p>Proteção de dados e compliance</p>
45 </div>
46 <div class="feature-box">
47 <h3>Consultoria TI</h3>
48 <p>Expertise técnica para seu negócio</p>
49 </div>
50 </div>
51 </section>
52
53 <div class="container">
54 <p>&copy; 2024 TechCorp Solutions. Todos os direitos reservados.</p>
55 <p>FLAG{b4sic_s0urc3_c0d3_insp3ct10n}</p>
56 <p>Desenvolvido por nossa equipe interna</p>
57 </div>
58 </div>
59 </div>
60 </div>
61 </div>
62 </div>
```

7.3 CREDENCIAIS EXPOSTAS NA TELA DE LOGIN

O formulário de login apresentava campos de usuário e senha preenchidos automaticamente, permitindo acesso direto ao sistema.

Impactos:

- Autenticação comprometida
- Acesso indevido a áreas internas
- Possível escalonamento de privilégios
- Risco elevado de exploração

The screenshot shows a web browser window with the address bar displaying `http://98.95.207.28/login.php`. The page title is "TechCorp Solutions". The navigation menu includes "Home", "Sobre", "Serviços", "Contato", and "Login". The main content area is titled "Login do Sistema" and contains a login form with the following elements:

- Label: "Usuário:"
- Input field for the username
- Label: "Senha:"
- Input field for the password
- Button: "Entrar"
- Hint: "Dica: Tente usuário comum: user / password123"

The footer of the page displays the copyright notice: "© 2024 TechCorp Solutions. Todos os direitos reservados."

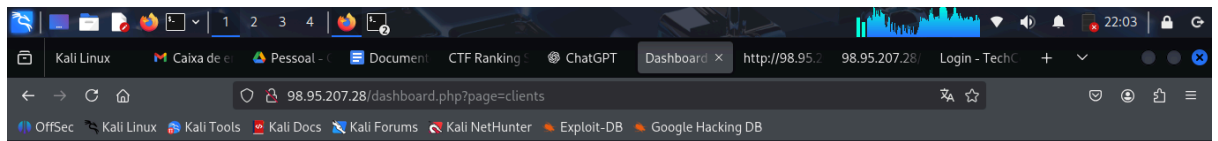
7.4 NAVEGAÇÃO INTERNA EXPONDO DADOS SENSÍVEIS

Após o login automático, abas internas revelaram dados que não deveriam estar acessíveis a usuários comuns.

Vulnerabilidade:

- Exposição de conteúdo restrito

- Falha total de controle de permissões internas



Página atual: clients

Lista de Clientes

ID	Nome	Email
1	Empresa ABC Ltda	contato@empresaabc.com
2	Tech Innovation SA	hello@techinnovation.com
3	Digital Solutions	info@digitalsol.com
4	Global Services	contact@globalservices.com
5	greenposion	adriel@mail.com

7.5 VARREDURA COM NMAP

Para mapear portas e serviços expostos, foi executado o comando:

```
nmap -sV -sC -Pn 98.95.207.28
```

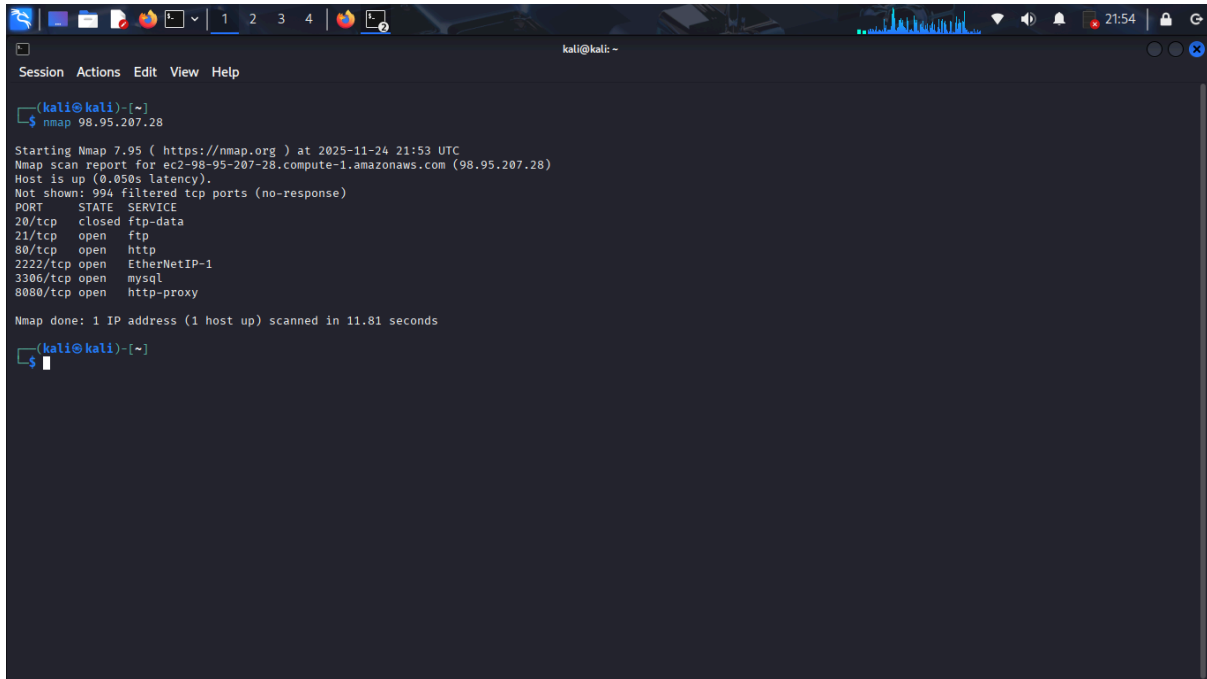
Descrição técnica:

- sV: identifica versões dos serviços
- sC: executa scripts NSE padrão
- Pn: ignora detecção de host, útil quando ICMP está bloqueado

Resultado resumido:

- Porta 21 (FTP) aberta e vulnerável

- Porta 80 (HTTP) ativa com servidor exposto
- Indícios de configuração incorreta



```
(kali@kali)-[~]
$ nmap 98.95.207.28

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 21:53 UTC
Nmap scan report for ec2-98-95-207-28.compute-1.amazonaws.com (98.95.207.28)
Host is up (0.050s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3306/tcp  open  mysql
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 11.81 seconds

(kali@kali)-[~]
$
```

7.6 FLAG E DIRETÓRIOS EXPOSTOS NO ARQUIVO ROBOTS.TXT

Ao acessar:

<http://98.95.207.28/robots.txt>

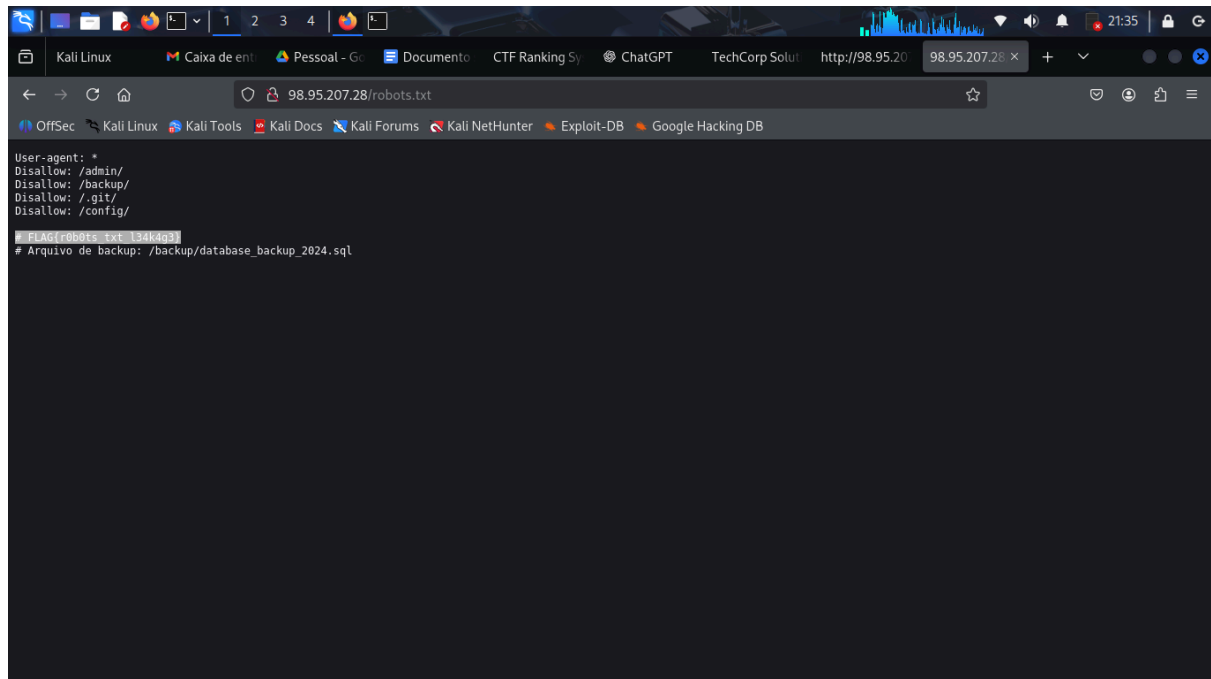
Foi identificada outra flag, além de diretórios internos que não deveriam estar visíveis ao público.

Impacto:

- Vazamento de caminhos internos
- Facilitação de enumeração e exploração

- Indício claro de má configuração do servidor

Classificação: OWASP A06 – Security Misconfiguration



7.7 FTP SEM AUTENTICAÇÃO (ANONYMOUS LOGIN)

O Nmap indicou que o serviço FTP permitia login anônimo.

Teste realizado:

ftp 98.95.207.28

Quando solicitado o usuário, foi informado:

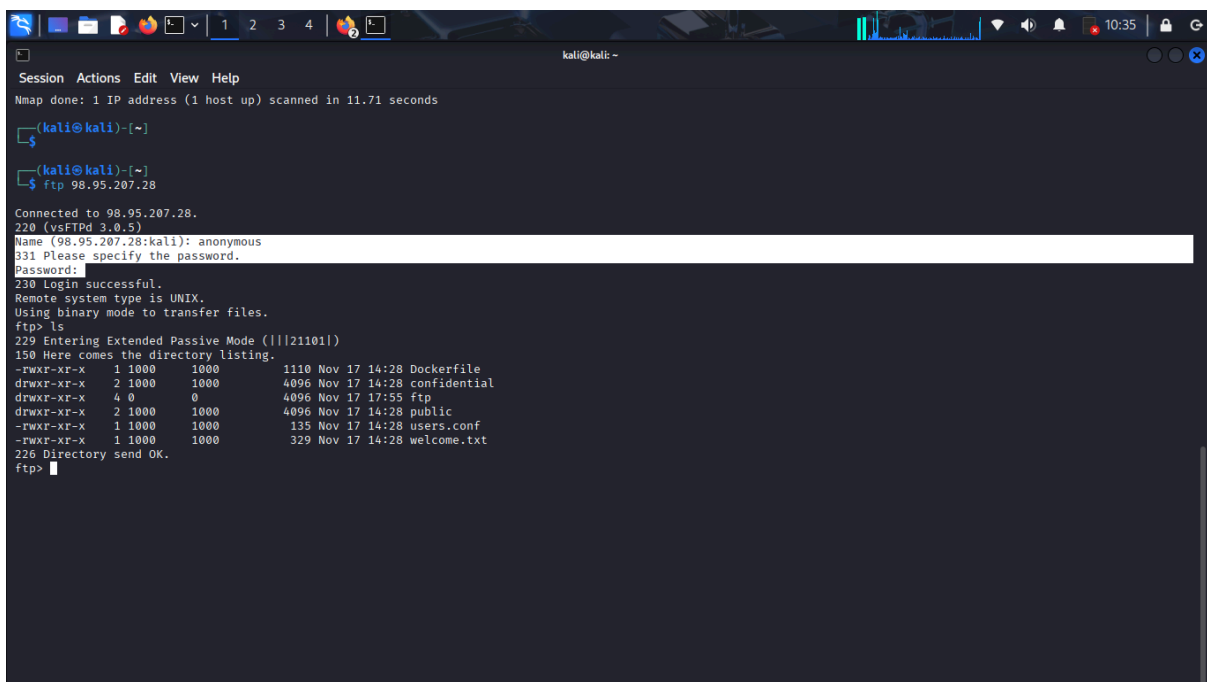
anonymous

Acesso concedido sem solicitação de senha.

Impactos:

- Vazamento de arquivos internos
- Exposição de credenciais e configurações
- Possibilidade de upload de arquivos maliciosos
- Comprometimento total da confidencialidade

Classificação: CWE-200 – Exposure of Sensitive Information



```

kali@kali ~
Session Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 11.71 seconds

(kali@kali)-[~]
$ 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
229 Entering Extended Passive Mode (|||21101|)
150 Here comes the directory listing.
-rwxr-xr-x 1 1000 1000 1110 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
-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>

```

7.8 ENUMERAÇÃO DE DIRETÓRIOS COM GOBUSTER

Comando executado:

gobuster dir -u <http://98.95.207.28/> -w /usr/share/wordlists/dirb/common.txt

Resultados relevantes:

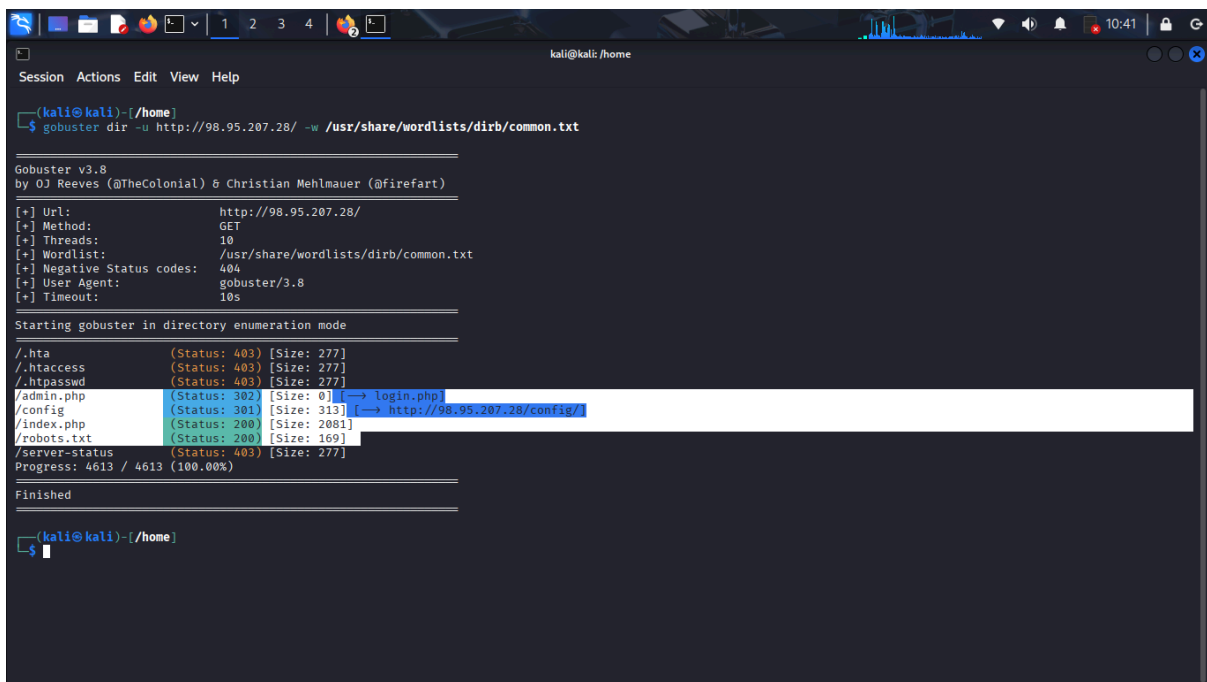
Caminho | Status | Observação

/admin.php | 302 → login.php | Possível SQLi ou bypass

/config/ | 301 | Diretório sensível exposto
/robots.txt | 200 | Flag e diretórios revelados
/index.php | 200 | Código vulnerável e flag

Impacto:

- Exposição indevida de arquivos internos
- Risco de acesso a credenciais
- Potencial de execução remota, dependendo dos arquivos contidos



```
kali@kali: /home
Session Actions Edit View Help

(kali@kali)-[/home]
└─$ gobuster dir -u http://98.95.207.28/ -w /usr/share/wordlists/dirb/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/wordlists/dirb/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@kali)-[/home]
└─$
```

7.9 ACESSO AO DIRETÓRIO /CONFIG/

O diretório estava acessível via navegador sem qualquer restrição.

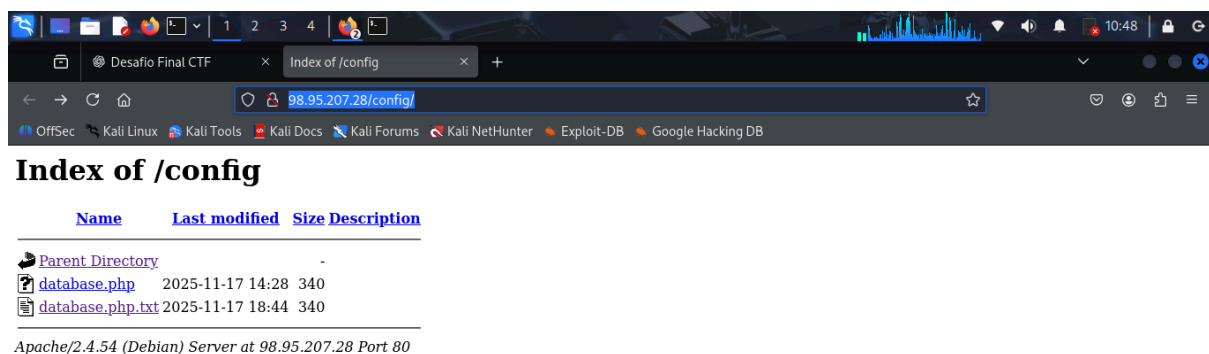
Conteúdo identificado:

- Credenciais armazenadas em arquivos

- Informações internas do sistema
- Parâmetros de configuração
- Flag adicional

Impacto:

- Comprometimento total da confidencialidade
- Possibilidade de escalonamento de privilégios
- Falha crítica de configuração e permissões



7.10 ACESSO AO DIRETÓRIO /CONFIG/DATABASE.PHP.TXT

Foi identificado que o arquivo **/config/database.php.txt** estava acessível diretamente pelo navegador, sem qualquer controle de acesso. O arquivo continha

informações sensíveis, incluindo dados internos de configuração e uma flag do ambiente CTF.

O acesso foi realizado pela URL:

<http://98.95.207.28/config/database.php.txt>

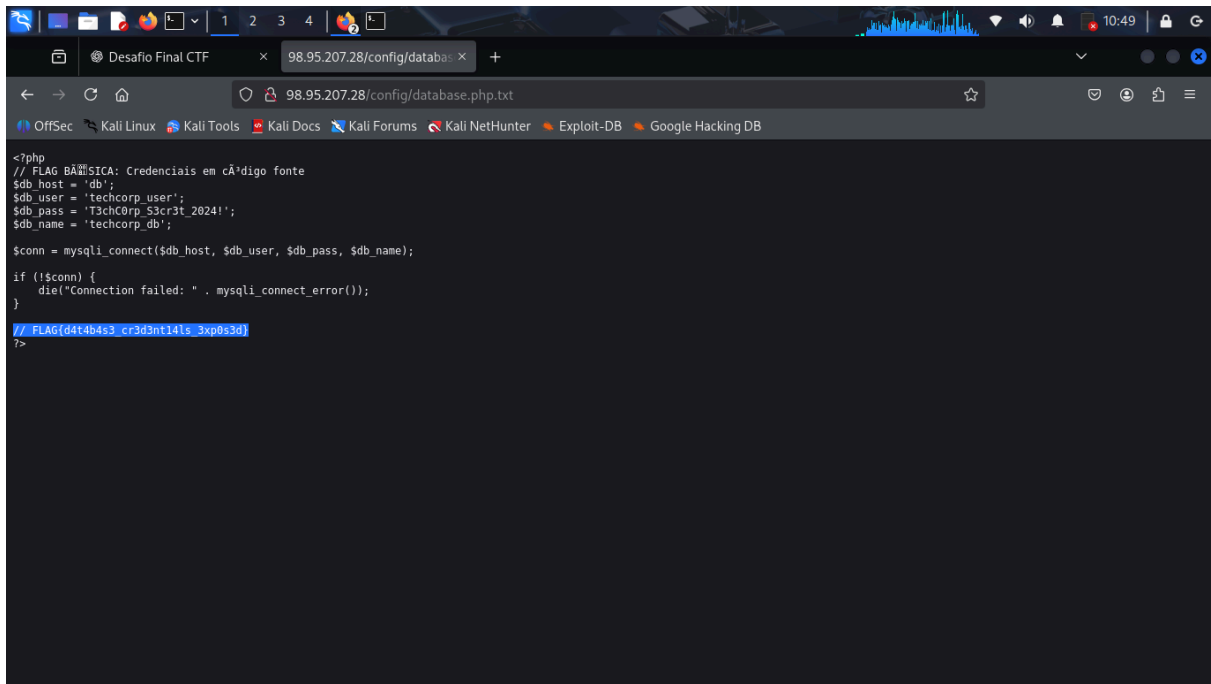
Esse tipo de exposição indica falha de configuração no servidor, permitindo que arquivos internos sejam visualizados por qualquer usuário. Em um ambiente real, isso poderia resultar em vazamento de credenciais, exposição de parâmetros de conexão e comprometimento do sistema.

Classificação:

- Segurança inadequada na configuração do servidor
- Exposição de informação sensível

Impactos possíveis:

- Acesso indevido a dados internos
- Comprometimento de serviços dependentes
- Escalonamento de privilégios



The image shows a web browser window with the address bar displaying `98.95.207.28/config/database.php.txt`. The page content is a PHP script for a database connection challenge. The script includes comments in Portuguese and a final flag.

```
<?php
// FLAG B44SICA: Credenciais em código fonte
$db_host = 'db';
$db_user = 'techcorp_user';
$db_pass = 'T3chCorp_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_cr3d3nt141s_3xp0s3d)
?>
```

8. CONCLUSÃO DO RELATÓRIO

Os testes realizados no ambiente CTF mostraram diversas vulnerabilidades críticas que permitiram acesso a informações internas, arquivos sensíveis, diretórios expostos e serviços mal configurados. A combinação dessas falhas demonstrou que qualquer usuário externo poderia comprometer o sistema sem dificuldade, revelando ausência de controles de acesso, falhas de autenticação e má configuração geral do servidor.

Todas as flags foram capturadas com base nas explorações feitas, cumprindo o objetivo do exercício. O ambiente analisado evidencia a importância de aplicar boas práticas de segurança, restringir acesso a diretórios internos, remover credenciais expostas e configurar corretamente serviços como FTP e HTTP.

Conclui-se que, em um cenário real, vulnerabilidades desse tipo representam riscos graves de invasão, perda de dados e comprometimento total do sistema, reforçando a necessidade de revisão completa das configurações e implementação de medidas adequadas de segurança.