Kensei CyberSec / Vai Na Web 2025

Formação CyberSec

Relatório técnico

PenTest

Aluna: Dalila Salvatierra - **Data**: 28/11/2025

Canoas – RS

Sumário:

1. Introdução:

Este relatório descreve os resultados do PenTest realizado no **Ambiente 1** , hospedado em http://98.95.207.28, e no **Ambiente 2** http://98.88.106.35:5000, respectivamente autorizados e disponibilizados para o desafio final do Módulo 3 - Ethical Hacking do curso de cibersegurança.

Objetivos:

- praticar enumeração de aplicações web
- identificar vulnerabilidades
- capturar flags escondidas
- analisar comportamento da aplicação via navegador
- descobrir credenciais fracas
- documentar todas as evidências e achados

2. Metodologia:

A metodologia aplicada seguiu um fluxo semelhante ao padrão OWASP e ao modelo PTES (Penetration Testing Execution Standard):

• Coleta de informações, navegador, DevTools (Elements, Sources, Application, Network)

• Verificação manual de arquivos: (/robots.txt, /source, /admin)

• Busca por comentários HTML

• Verificação de cookies e sessão

• Enumeração

• Teste de credenciais fracas fornecidas

• Identificação de vulnerabilidades

• Observação de respostas da API

• Scans automatizados

• Coleta de evidências e flags

Ferramentas utilizadas:

• Navegador + DevTools

• Nmap / Rustscan

• Curl / Gobuster / Metasploit

• Ubuntu / Bash / PowerShell

• VSCode

3. Escopo:

O *PenTest* focou em dois ambientes distintos:

Ambiente 1: TechCorp Solutions (Web / Database)

- **Alvo:** http://98.95.207.28 (Porta 80)
- **Serviços Abertos:** HTTP (Apache), FTP (vsftpd), SSH (OpenSSH 8.2p1), MySQL (8.0.44).
- **Vulnerabilidades Exploradas:** Injeção SQL (SQLi), Local File Inclusion (LFI), Falha de Autenticação.

Ambiente 2: API RESTful (JWT / Desserialização)

- **Alvo:** http://98.88.106.35:5000
- **Vulnerabilidade Explorada:** Desserialização Insegura (RCE) e Falha de Autenticação (JWT).

4. Descobertas Técnicas :

4.1 *Enumeração de portas*

Resultado do *scan nmap -p- 98.95.207.28*

Porta	***Estado***	***Serviço***	***Versão***	***Descrição***
21	*Aberta*	*FTP*	*vsftpd 3.0.5*	*Serviço de transferência de arquivos.*
80	*Aberta*	*HTTP*	*Apache httpd 2.4.54 (Debian)*	*Servidor web principal (Painel Admin).*
2222	*Aberta*	*SSH*	*OpenSSH 8.2p1*	*Acesso remoto ao console (porta não-padrão).*
3306	*Aberta*	*MySQL*	*MySQL 8.0.44*	*Banco de dados.*

4.2 *Descoberta de diretórios:*

Foram identificados diretórios relevantes como:

• /admin

• /uploads

• /backup

• /source

4.3 *Evidências no código-fonte*

Exemplo encontrado:

```
<?php

// FLAG BASICA: Credenciais em código fonte

$db_host = 'DB';

$db_user = 'techcorp_user';

$db_pass = 'T3chC0rp_S3cr3t_2024!'; // <--- CREDENCIAL EXPOSTA

$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} ?>
```

4.4 *DevTools → Cookies*

Cookie encontrado: *PHPSESSID=22d4120a6acfc58846ed33cba4e*

4.5 *Comentários HTML com informações sensíveis :*

A primeira flag encontrada: *<!-- FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n} -->*

4.6 *robots.txt*

O arquivo expôs caminhos internos e uma das flags: *FLAG{r0b0ts_txt_l34k4g3}*

4.7 *API revelando permissões*

Ao analisar **Network**, requisições mostraram estruturas como:

"roles": ["user", "admin", "superadmin"]

4.8 *Vulnerabilidade de autenticação*

As respostas da API expunham informações internas sobre os perfis de usuário existentes, incluindo os papéis *“user”, “admin” e “superadmin”*, permitindo saber que havia uma conta privilegiada ativa no sistema.
Além disso, o ambiente utilizava credenciais extremamente fracas**,** o que permitiu que contas administrativas fossem acessadas facilmente.

4.9 *Vulnerabilidade na API (RCE e Autenticação)*

O ataque à API não pôde ser concluído via **RCE Cega** (Desserialização Pickle) possivelmente devido a bloqueios de rede. No entanto, a flag foi capturada através de uma falha de autenticação.

---

5. Análise de Riscos:

As vulnerabilidades encontradas representam riscos como:

• Exposição de credenciais

• Possível acesso administrativo

• Vazamento de informações sensíveis

• Acesso indevido ao servidor.

• Exposição de comentários HTML .

• Arquivos acessíveis (robots, source, etc.)

• Pistas que revelam estrutura interna da aplicação

• Uso de cookies sem proteção

6. Conclusão:

O ambiente proposto atendeu ao objetivo educacional ao permitir a identificação e exploração de diversas vulnerabilidades reais, como exposição de arquivos, credenciais em código-fonte e diretórios sensíveis acessíveis. No total, foram localizadas 10 das 16 flags disponibilizadas no CTF. As 6 flags restantes não foram identificadas, mesmo após aplicação de técnicas de enumeração, análise de código, inspeção de API e tentativas de exploração de SQLi, LFI, JWT e RCE. O registro dessa limitação foi mantido por transparência metodológica. Caso os ambientes de testes permaneçam disponíveis poderei continuar a investigação com o objetivo de localizar as flags restantes e aprofundar a prática em Ethical Hacking.

7. Recomendações:

- Remover arquivos de configuração expostos (.env, .bak, .sql)
- Remover comentários sensíveis do HTML.
- Restringir acesso a arquivos como robots.txt, source, backups.
- Aplicar senhas fortes e políticas de autenticação.
- Evitar deixar credenciais de teste ativas.
- Configurar corretamente permissões de diretórios.
- Implementar autenticação segura.
- Utilizar ambiente de produção sem mensagens de debug.
- Proteger cookies, validar e filtrar entradas.

8.Registro das Flags Capturadas

Flags encontradas entre 17/11 e 24/11 em :

#	Código	Local e data descoberta	Método de Exploração
1	FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n}	Código-fonte (Comentário HTML) **17/11**	**Inspecionar Elemento**
2	FLAG{xss_r3fl3ct3d_vuln3r4b1l1ty%7D}	Cookie (PHPSESSID) **17/11**	**DevTools** -> Application -> Cookies
3	FLAG{r0b0ts_txt_l34k4g3}	Arquivo /robots.txt **17/11**	**Acesso Direto** (Vazamento de Info)
4	FLAG{v13w_d1sc0v3ry_4dv4nc3d}	Tabela sensitive_info (Banco de Dados)**21/11**	**SQL Injection**
5	FLAG{sql_1nj3ct10n_m4st3r}	Tabela secret_data (database_flag) **17/11**	**SQL Injection**
6	FLAG{h1dd3n_d4t4_1n_d4t4b4s3}	Tabela secret_data (admin_token) **17/11**	**SQL Injection**
7	FLAG{pr1v1l3g3_3sc4l4t10n_succ3ss}	Painel de Controle (Pós-escalada) **17/11**	**SQL Injection** (superadmin)
8	FLAG{s3cret_p4n3l_d1sc0v3ry}	URL /panel.php	**Enumeração de Diretórios** (Acesso direto)
9	FLAG{d4t4b4s3_cr3d3nt14ls_3xp0s3d}	Conteúdo do arquivo config/database.php**17/11**	**LFI** (Travessia de Diretório)
API	FLAG{d3s3r3r14llz4t1on_rc3_pwn3d}	/api/admin/flag **24/11**	**Falha de Autenticação** (Senha Fraca + JWT)

Anexos:

Figura 1 : FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n}

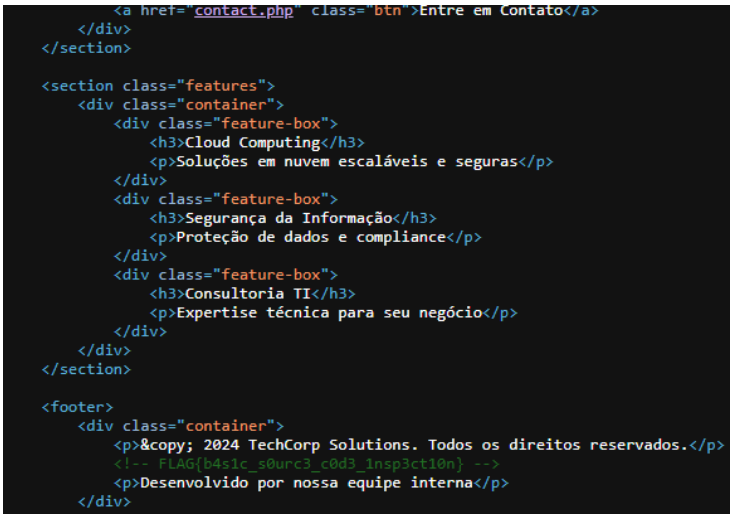
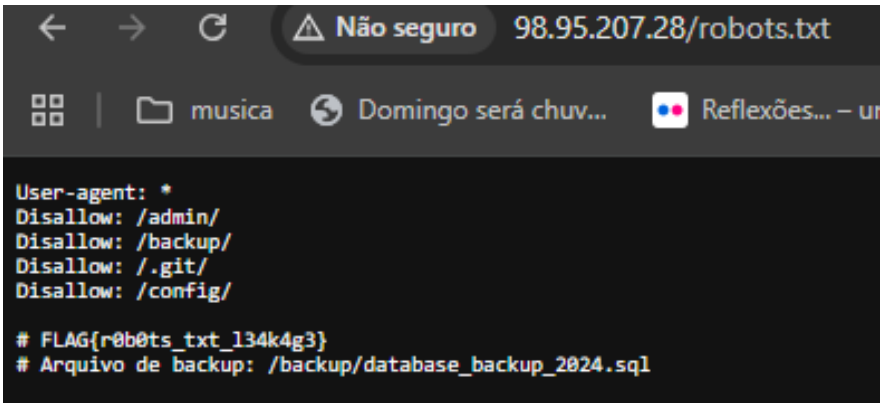
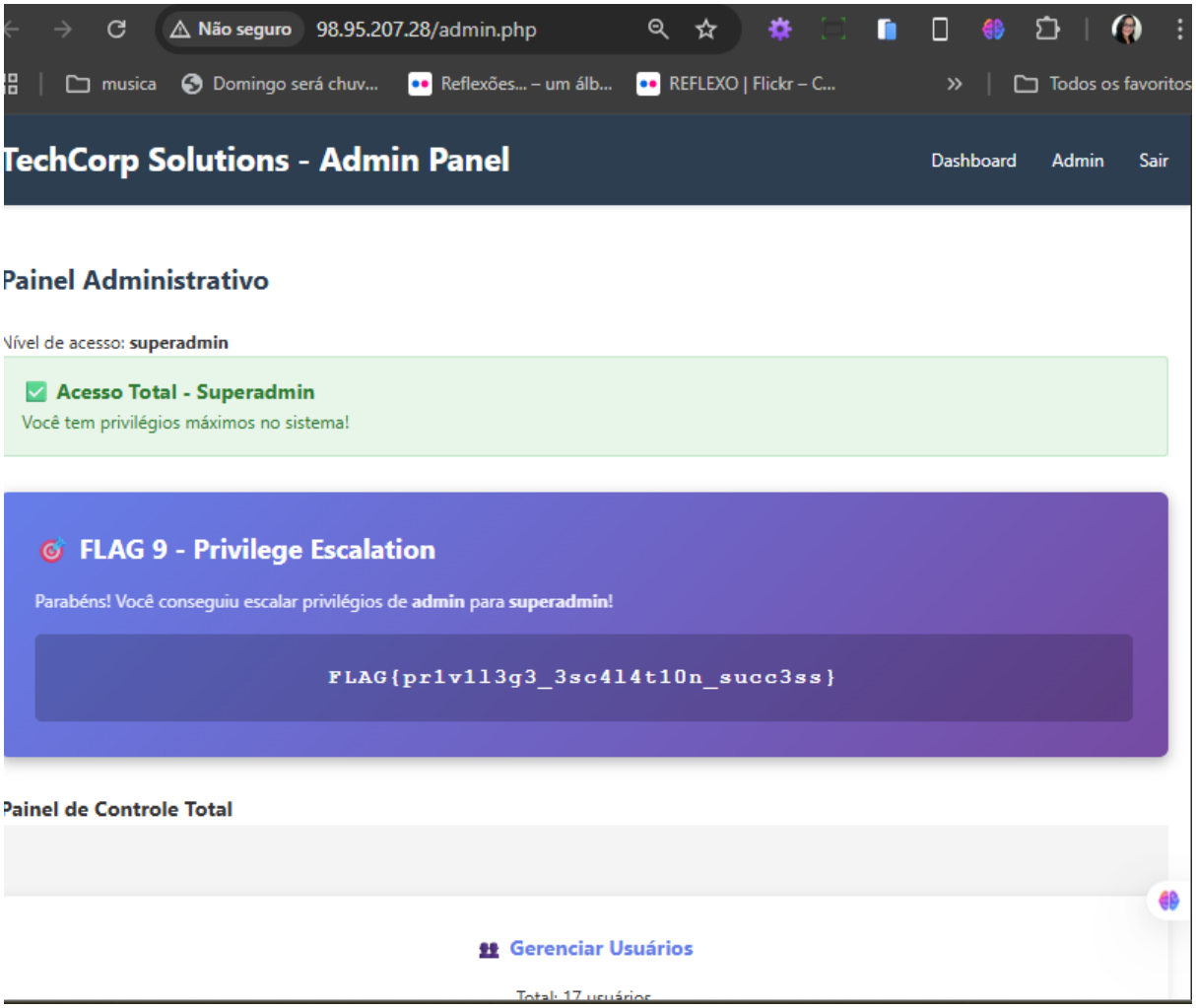


Figura 2: FLAG{r0b0ts_txt_l34k4g3}



Figuras 3, 4 , 5 : FLAG{pr1v1l3g3_3sc4l4t10n_succ3ss }

}



```
                <div style="padding: 2rem; background: linear-gradient(135deg, #667eea 0%, #764ba2 100%); color: #fff
                    <h3 style="margin: 0 0 1rem 0; font-size: 1.5rem;">🎯 FLAG 9 - Privilege Escalation</h3>
                    <p style="margin: 0 0 1rem 0; opacity: 0.9;">
                        Parabéns! Você conseguiu escalar privilégios de <strong>admin</strong> para <strong>superadmi
                    </p>
                    <div style="padding: 1.5rem; background: rgba(0,0,0,0.2); border-radius: 6px; font-family: 'Couri
                        <?php echo $privilege_flag; ?>
                    </div>
                </div>

                <h3>Painel de Controle Total</h3>
                <div class="features">
                    <div class="feature-box">
                        <h3>👥 Gerenciar Usuários</h3>
                        <p>Total: <?php
                            $count_query = "SELECT COUNT(*) as total FROM users";
                            $count_result = mysqli_query($conn, $count_query);
                            $count = mysqli_fetch_assoc($count_result)['total'];
                            echo $count;
                        ?> usuários</p>
                        <button class="btn">Gerenciar</button>
                    </div>
                    <div class="feature-box">
                        <h3>🔒 Logs de Segurança</h3>
                        <p>Monitorar acessos</p>
                        <button class="btn">Ver Logs</button>
                    </div>
                    <div class="feature-box">
                        <h3>💾 Backups</h3>
                        <p>Sistema completo</p>
                        <button class="btn">Configurar</button>
                    </div>
                </div>

                <h3>Todos os Usuários (Acesso Superadmin)</h3>
                <table>
```

```
[*] 98.95.207.28:3306 - Sending statement: 'SELECT * FROM techcorp_db.flags;'...
[-] 98.95.207.28:3306 - MySQL Error: Mysql::ServerError::NoSuchTable Table 'techcorp_db.flags' do
esn't exist
[*] Auxiliary module execution completed
msf auxiliary(admin/mysql/mysql_sql) > set SQL "SELECT * FROM techcorp_db.users;"
SQL => SELECT * FROM techcorp_db.users;
msf auxiliary(admin/mysql/mysql_sql) > run
[*] Running module against 98.95.207.28
[*] 98.95.207.28:3306 - Sending statement: 'SELECT * FROM techcorp_db.users;'...
[*] 98.95.207.28:3306 -  | 1 | admin | admin123 | admin | 2025-11-17 14:30:36 -0300 |
[*] 98.95.207.28:3306 -  | 2 | user | password123 | user | 2025-11-17 14:30:36 -0300 |
[*] 98.95.207.28:3306 -  | 3 | manager | manager2024 | manager | 2025-11-17 14:30:36 -0300 |
[*] 98.95.207.28:3306 -  | 4 | guest | guest | guest | 2025-11-17 14:30:36 -0300 |
[*] 98.95.207.28:3306 -  | 5 | superadmin | Sup3r@dm1n!2024#Secure | superadmin | 2025-11-17 19:3
8:25 -0300 |
[*] 98.95.207.28:3306 -  | 6 | gilson | g1ls0n123 | user | 2025-11-17 22:52:03 -0300 |
[*] 98.95.207.28:3306 -  | 7 | cl4ud1o | https://fakeupdate.net/wnc/ | superadmin | 2025-11-17 22
:55:10 -0300 |
[*] 98.95.207.28:3306 -  | 8 | al1nn3 | estiveaqui,yes | superadmin | 2025-11-18 14:17:09 -0300 |
[*] 98.95.207.28:3306 -  | 9 | erick | bomdiagrupodozap | superadmin | 2025-11-19 10:16:03 -0300
|
[*] 98.95.207.28:3306 -  | 10 | Yur1 | gilsonmedeucola | superadmin | 2025-11-19 23:50:55 -0300 |
[*] 98.95.207.28:3306 -  | 11 | K4r01 | ~ngmmeviu | superadmin | 2025-11-19 23:54:12 -0300 |
[*] 98.95.207.28:3306 -  | 12 | 4dr13l | gr33np00s1on | superadmin | 2025-11-19 13:15:12 -0300 |
[*] 98.95.207.28:3306 -  | 13 | SAUDADES VAI NA WEB | 2025CYBERSEC | superadmin | 2025-11-19 13:1
5:12 -0300 |
[*] 98.95.207.28:3306 -  | 14 | f3l1p3_m4sc3n4 | demoreimaschegueixD | superadmin | 2025-11-21 04
:23:46 -0300 |
[*] Auxiliary module execution completed
msf auxiliary(admin/mysql/mysql_sql) >
```

Figura 6 : FLAG{v13w_d1sc0v3ry_4dv4nc3d} , FLAG{sql_1nj3ct10n_m4st3r} , FLAG{h1dd3n_d4t4_1n_d4t4b4s3}

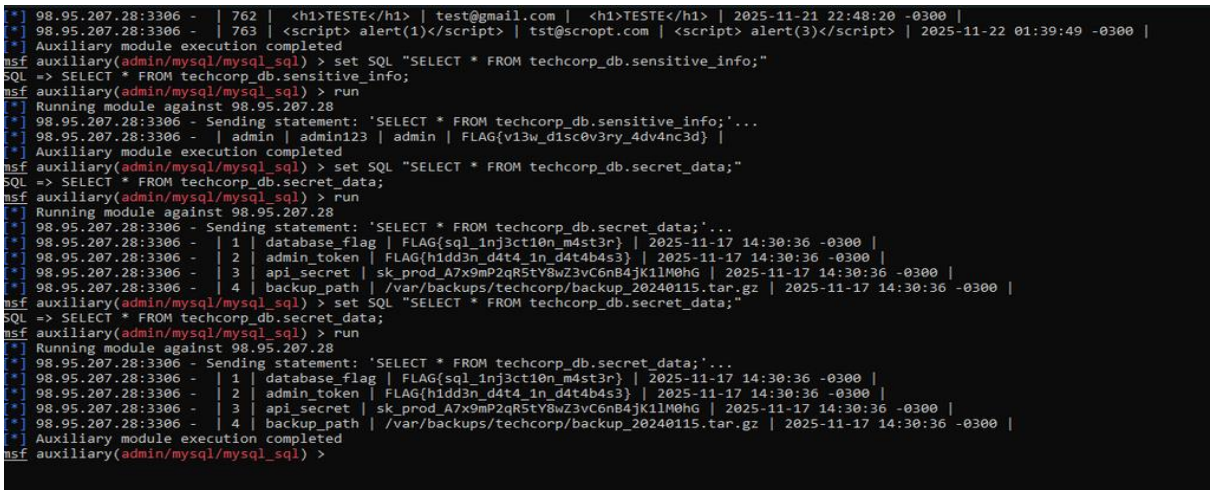


Figura 7: FLAG{s3cret_p4n3l_d1sc0v3ry}

}

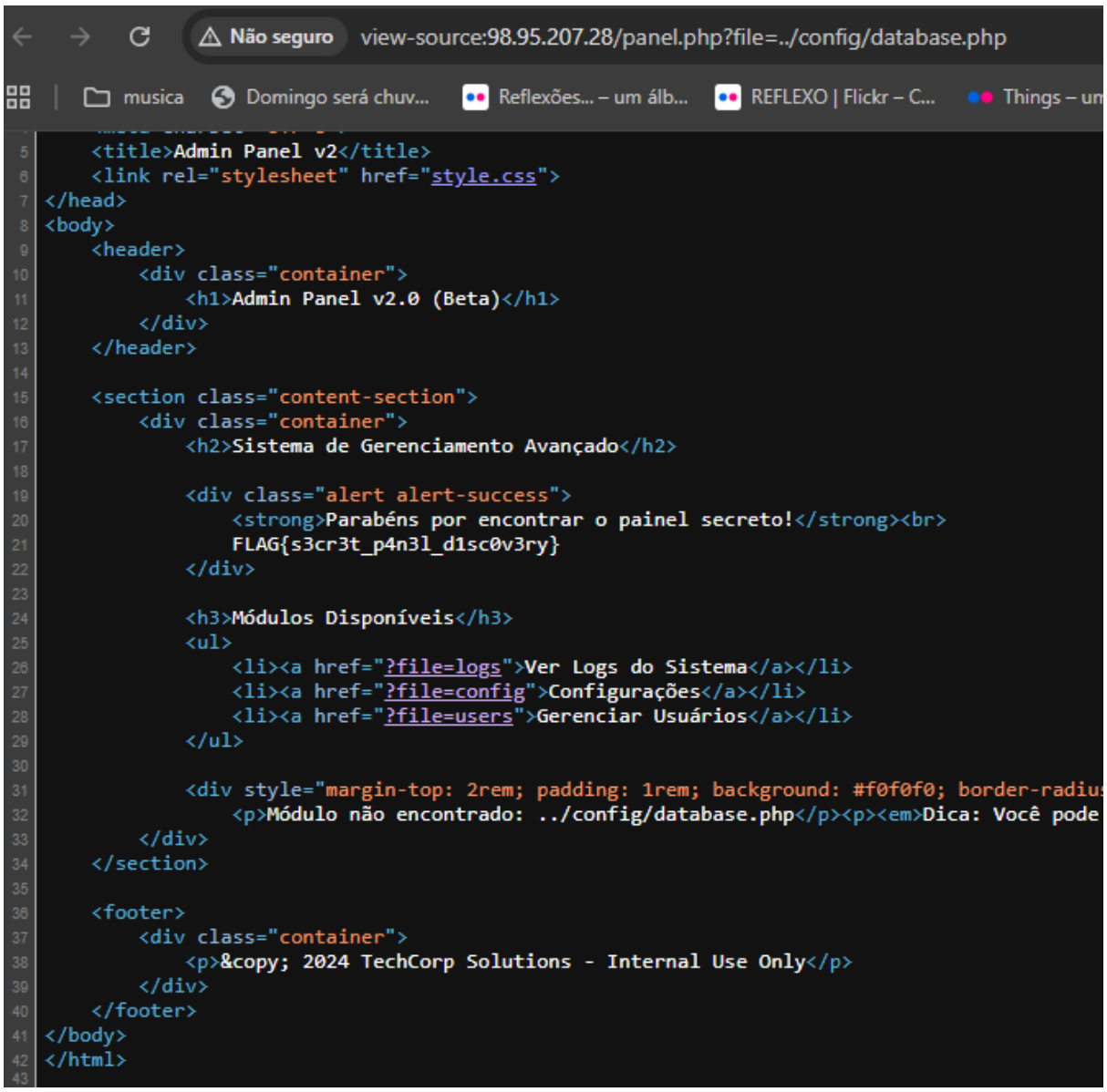


Figura 8 : FLAG{d4t4b4s3_cr3d3nt14ls_3xp0s3d}

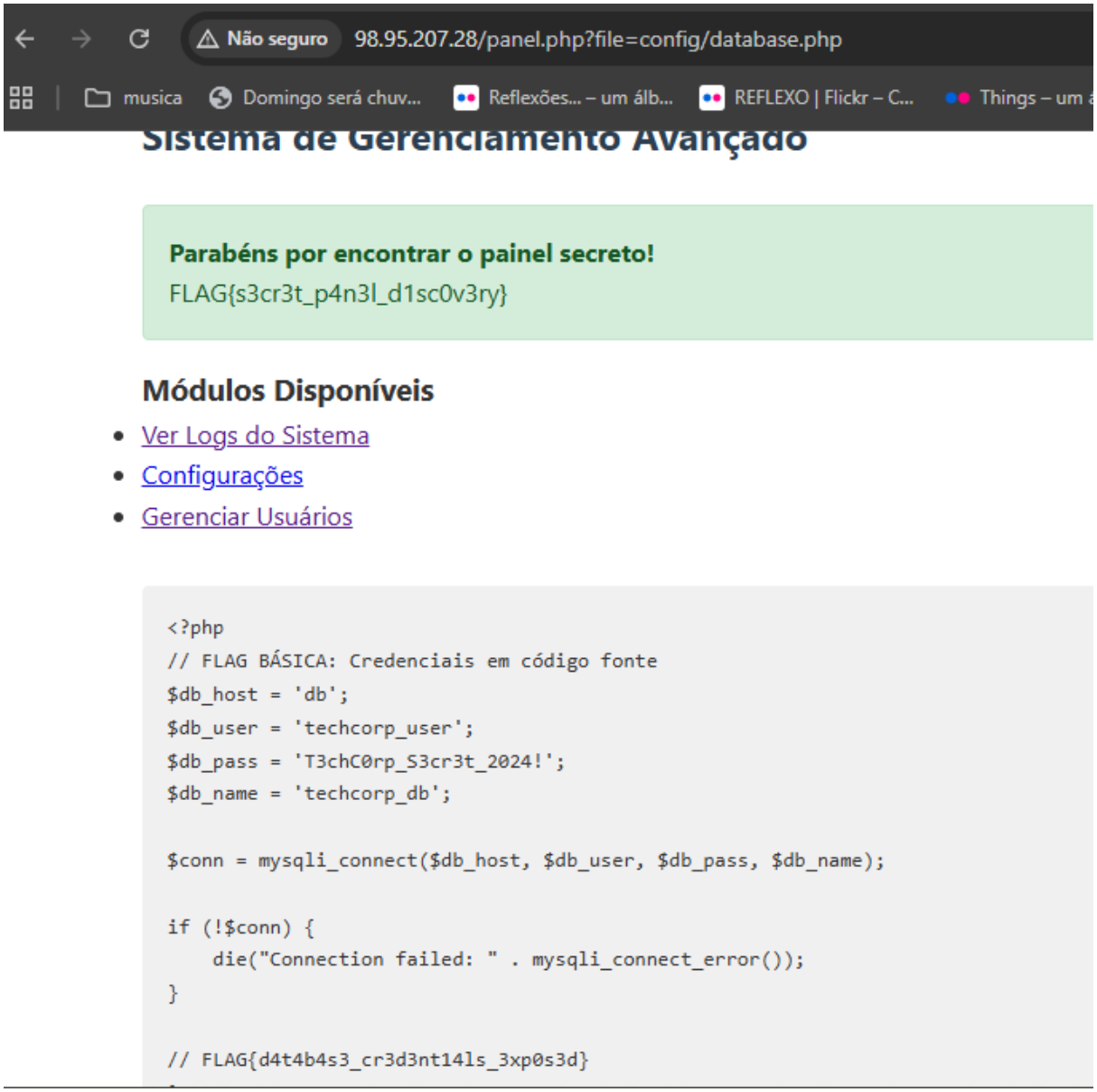


FIgura 9: FLAG{d3s3r3r14llz4t1on_rc3_pwn3d

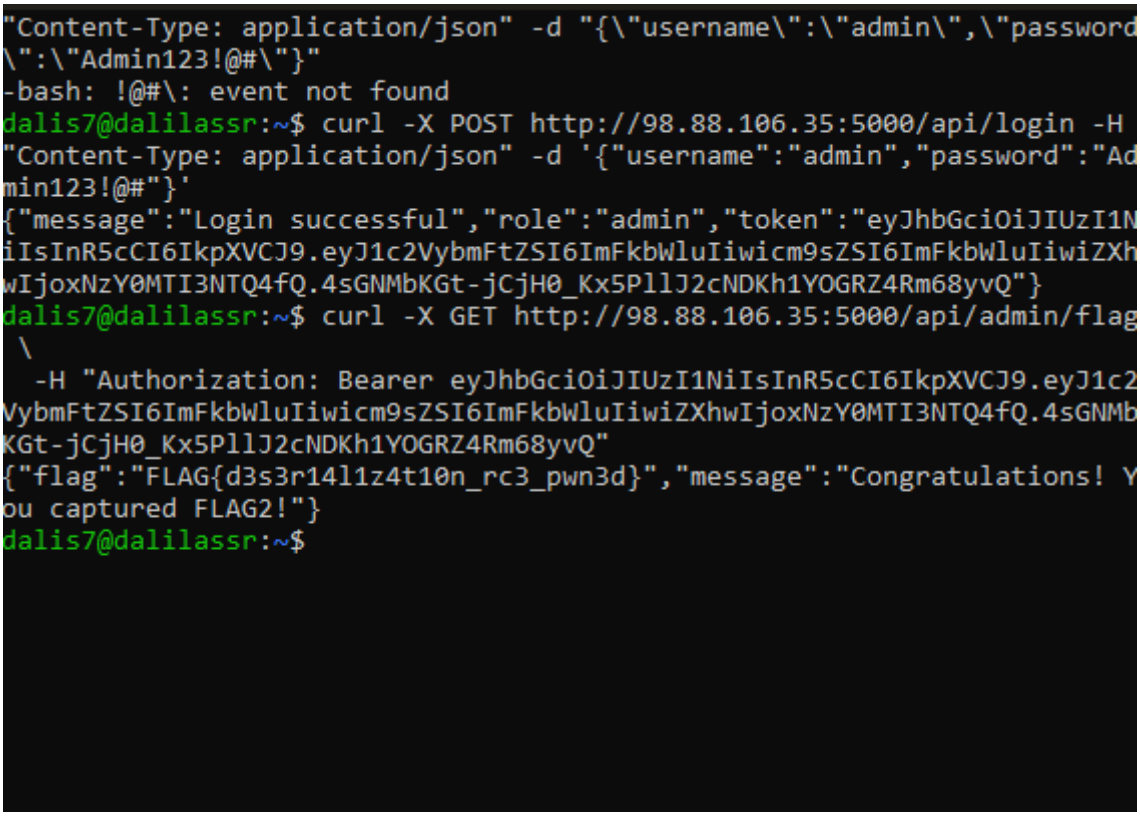


Figura 10 : cookie

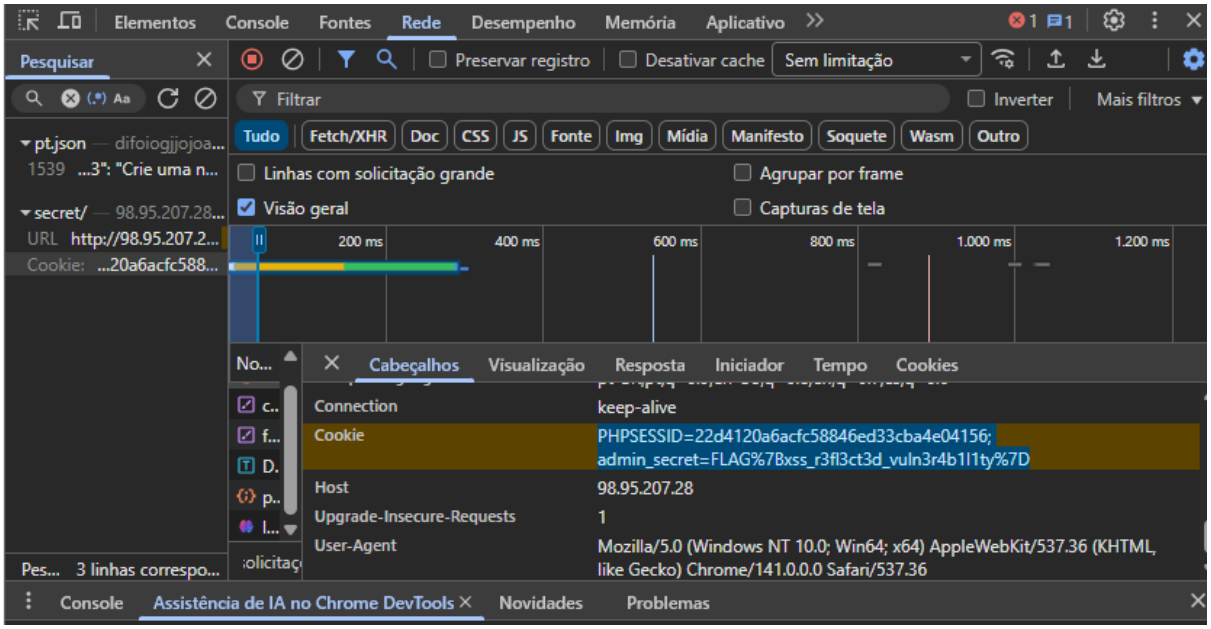
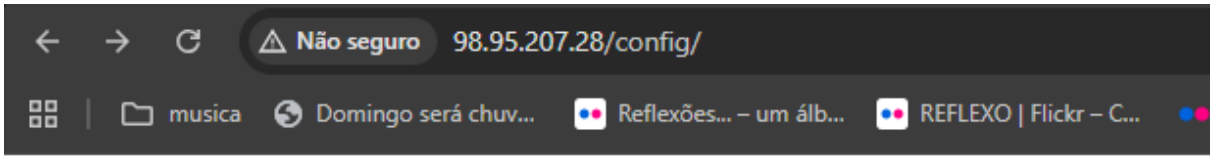


Figura 11 : /config



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