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

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

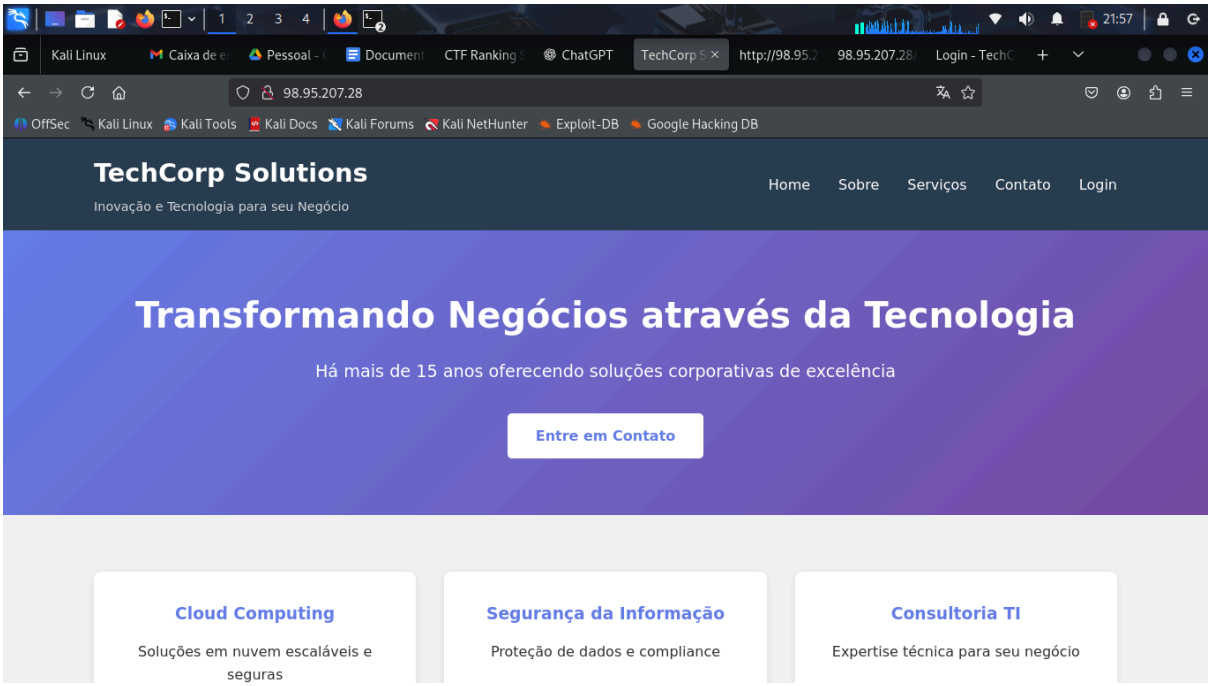
7. EVIDÊNCIAS E VULNERABILIDADES ENCONTRADAS

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



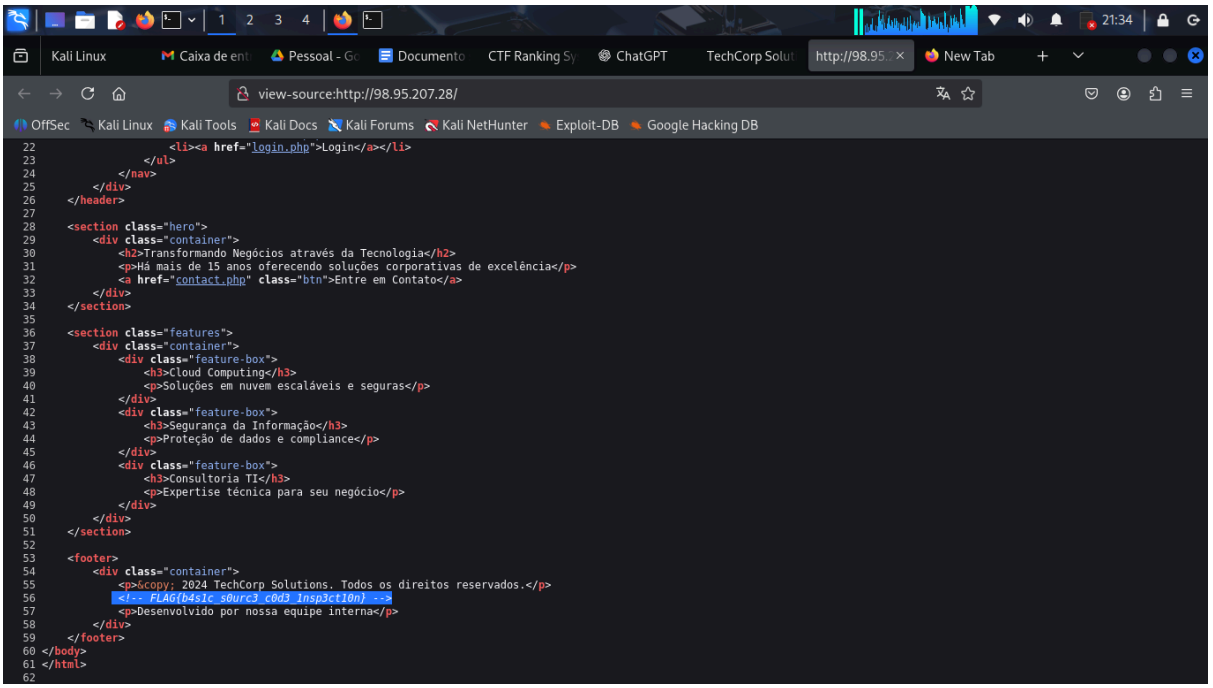
7.2 EXPOSIÇÃO DE INFORMAÇÃO NO CÓDIGO-FONTE

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

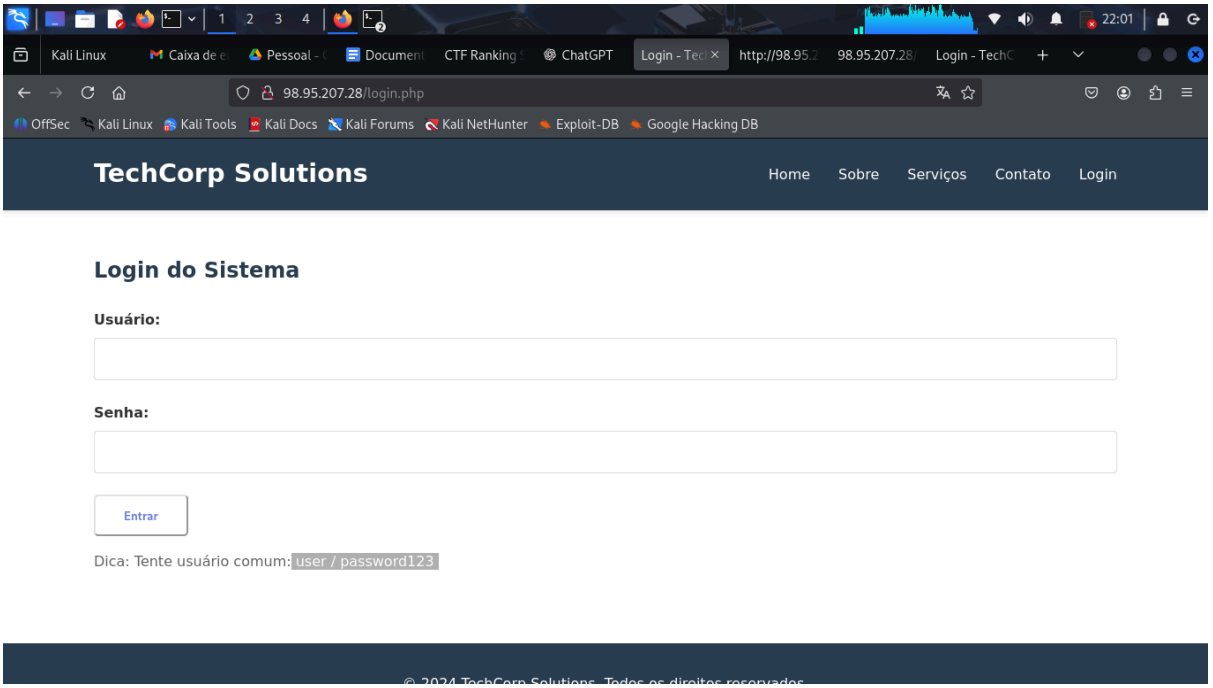


7.3 CREDENCIAIS EXPOSTAS NA TELA DE LOGIN

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



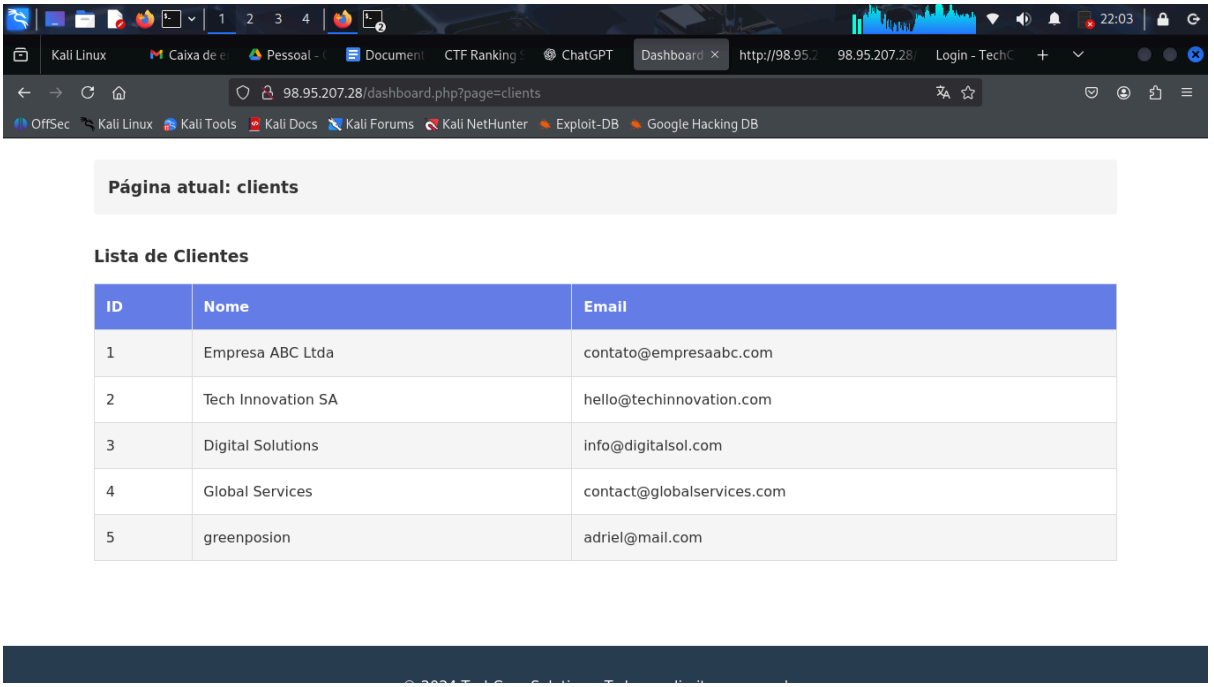
7.4 NAVEGAÇÃO INTERNA EXPONDO DADOS SENSÍVEIS

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



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:

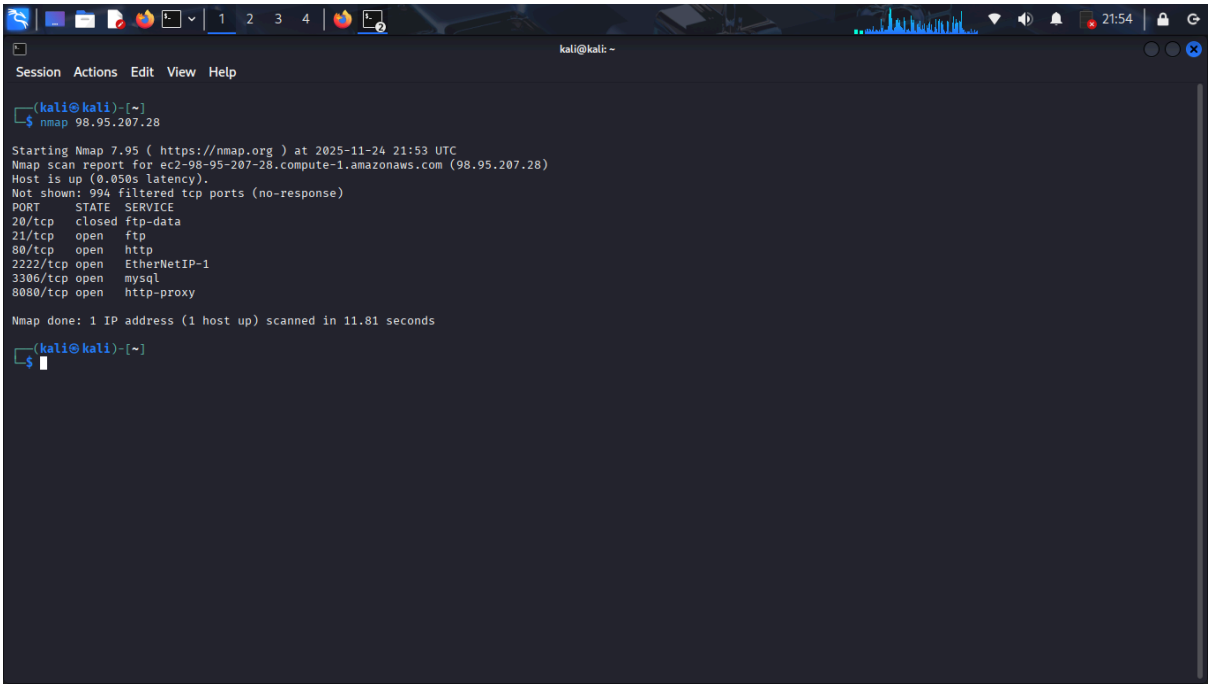
- sV: identifica versões dos serviços
- sC: executa scripts NSE padrão
- Pn: ignora detecção de host, útil quando ICMP está bloqueado

Resultado resumido:

- Porta 21 (FTP) aberta e vulnerável

- Porta 80 (HTTP) ativa com servidor exposto

- Indícios de configuração incorreta



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.

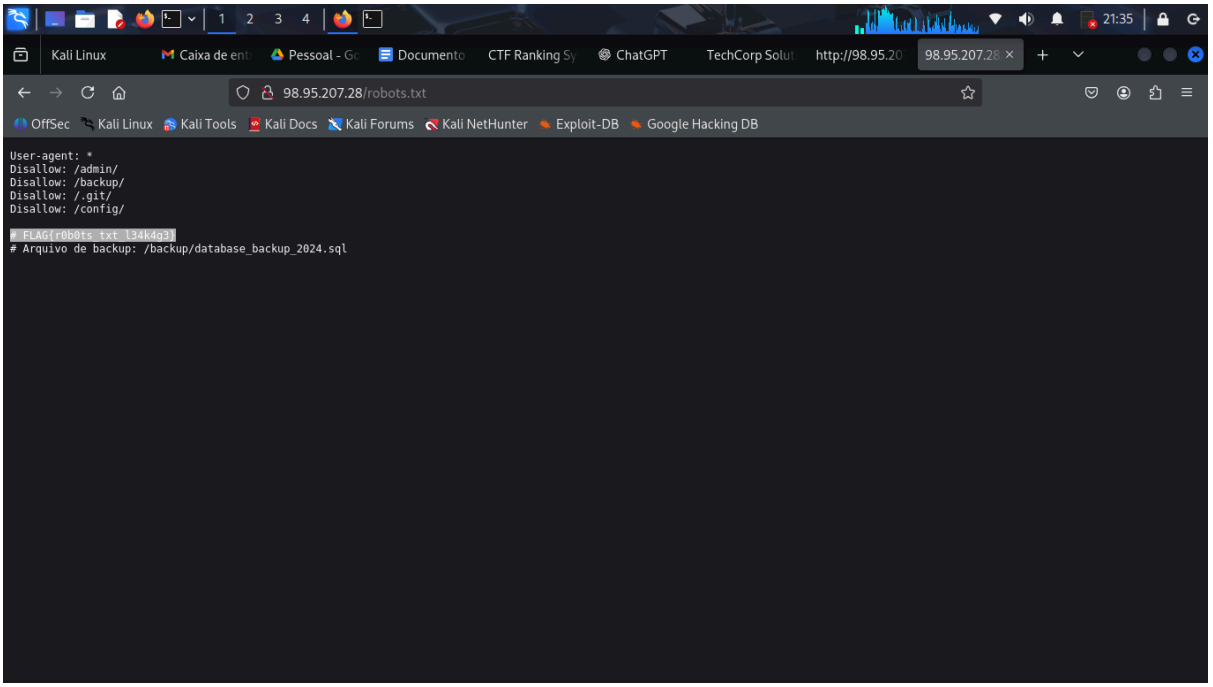
Impacto:

- 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

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

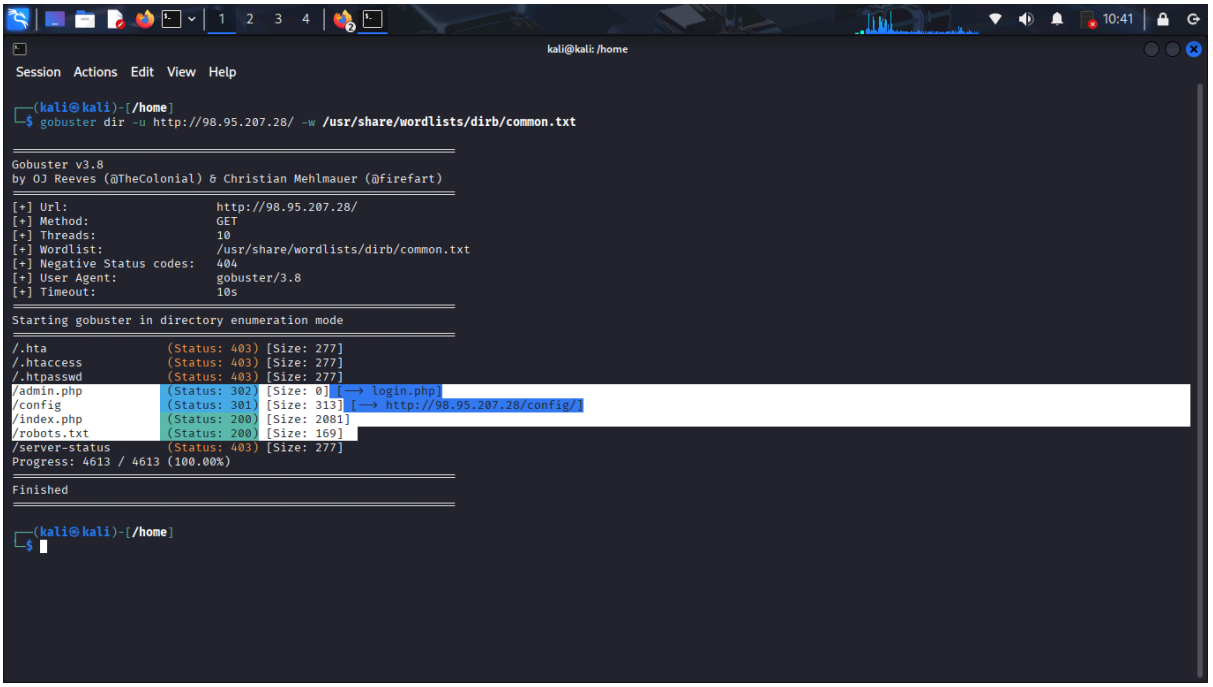
/config/ | 301 | Diretório sensível exposto

/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



7.9 ACESSO AO DIRETÓRIO /CONFIG/

O diretório estava acessível via navegador sem qualquer restrição.

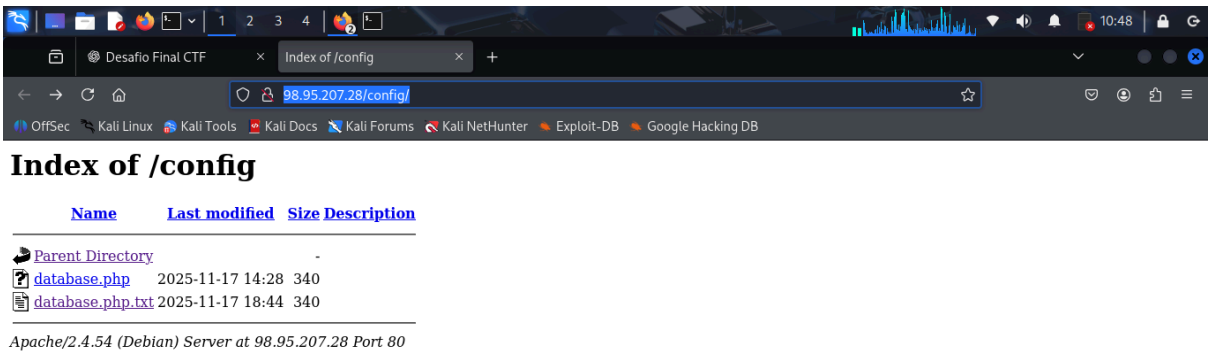
Conteúdo identificado:

- 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

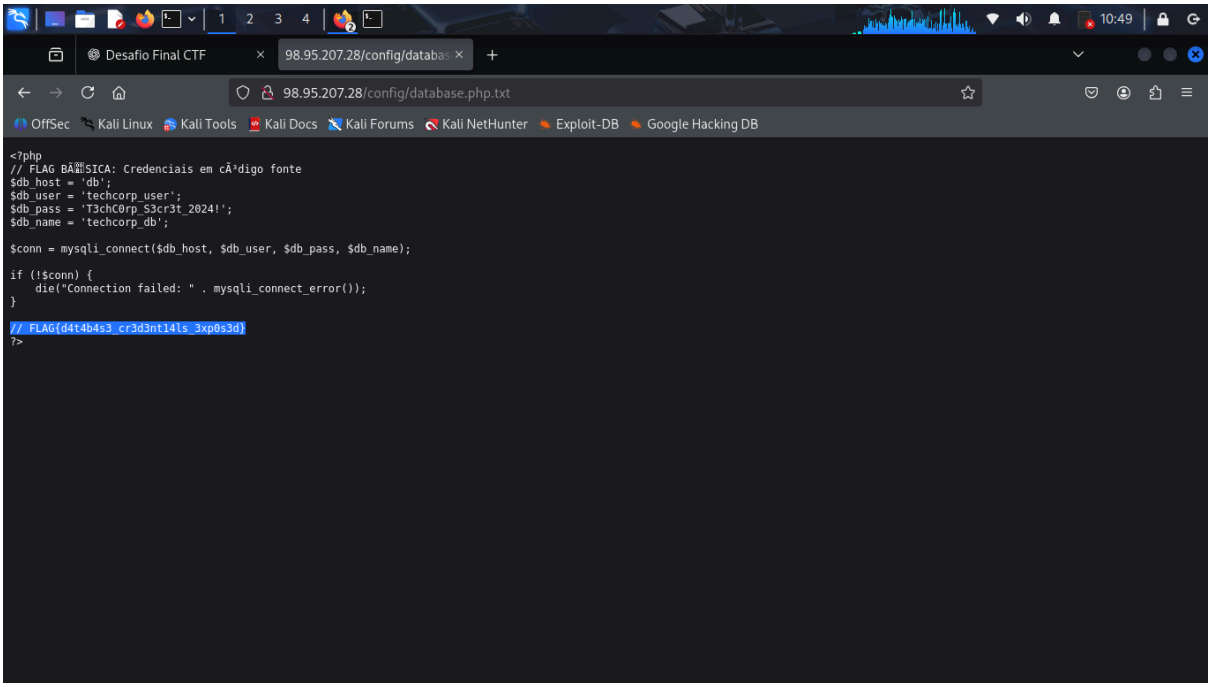
Esse tipo de exposição indica falha de configuração no servidor, permitindo que arquivos internos sejam visualizados por qualquer usuário. Em um ambiente real, isso poderia resultar em vazamento de credenciais, exposição de parâmetros de conexão e comprometimento do sistema.

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


10:49
Desafio Final CTF
98.95.207.28/config/databas
98.95.207.28/config/database.php.txt
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
<?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}
?>

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.