Desafio Final do Modulo 3

Título: Relatório de Teste de Intrusão (Pentest Reporte)

TechCorp Solutions - Análise de Segurança

Data: 01/12/2025

Versão: 1.0

Responsável: Gonçalo Quissola Dala

1. Informações do Projeto

Item	Detalhes
Cliente	TechCorp Solutions
Endereço IP	98.95.207.28
URL	http://98.95.207.28/
Data do Teste	18 – 27 de novembro de 2025
Metodologia	OWASP, PTES
Tipo de Teste	Black Box Testing (Teste Caixa-Preta)

---

2. Sumário Executivo

Durante o teste de intrusão realizado no ambiente da TechCorp Solutions, foram identificadas **múltiplas vulnerabilidades críticas** que comprometem seriamente a confidencialidade, integridade e disponibilidade dos sistemas. O ambiente apresentou falhas graves de configuração, exposição indevida de informações sensíveis e falta de controles básicos de segurança.

Principais descobertas:

- Exposição de credenciais em arquivos públicos
- Acesso FTP anônimo ativado
- Vulnerabilidades de injeção SQL críticas
- Diretórios e arquivos sensíveis acessíveis publicamente
- Falhas de Cross-Site Scripting (XSS) refletidas
- Vazamento de código fonte e credenciais no Git

Classificação de Risco: CRÍTICO

3. Objetivo e Escopo

3.1 Objetivos

O objetivo principal deste teste de intrusão foi avaliar a postura de segurança dos sistemas da TechCorp Solutions, identificando vulnerabilidades que pudessem ser exploradas por atacantes mal-intencionados. Os objetivos específicos incluíram:

1. Identificar e explorar vulnerabilidades em serviços expostos
2. Avaliar a configuração de segurança de servidores web e FTP
3. Testar a resistência contra ataques comuns (SQLi, XSS, LFI)
4. Verificar a exposição de dados sensíveis
5. Validar controles de acesso e autenticação
6. Capturar flags de segurança como prova de conceito

3.2 Escopo do Teste

Sistemas Incluídos:

- Servidor Web: 98.95.207.28:80 (HTTP)
- Servidor FTP: 98.95.207.28:21 (FTP)
- Aplicações Web: Painéis administrativos, formulários
- Arquivos e diretórios acessíveis publicamente

Limitações:

- Teste realizado apenas em ambientes de produção especificados
- Horário de execução: 22:00-06:00 (janela de manutenção)
- Exclusão de ataques DoS/DDoS
- Testes sociais de engenharia não incluídos

---

4. Flags Capturadas e Explorações

4.1 Flags de Credenciais Expostas

Flag	Localização	Exploração
FLAG{p4ssw@rd_f113_disc0v3ry}	passwords.txt	Arquivo com senhas corporativas deixado em diretório acessível
FLAG{git_cr3d3nt1418_134k}	/.git-credentials	Arquivo Git com token de acesso ao GitHub exposto
FLAG{d4t4b4s3_cr3d3nt141s_3xp0s3d}	/config/database.php.txt	Credenciais de banco de dados em arquivo texto acessível

4.2 Flags de Acesso e Descoberta

Flag	Localização	Exploração
FLAG{ftp_4n6nym0us_4cc3ss}	FTP Server (porta 21)	Acesso FTP anônimo permitido sem autenticação
FLAG{s3cr3t_p4n3l_disc0v3ry}	/panel.php	Painel administrativo exposto publicamente
FLAG{c0nfig_fil3_r34d}	users.conf	Arquivo de configuração do FTP acessível
FLAG{h1dd3n_d4t4_1n_d4t4b4s3}	Banco de dados	Dados ocultos descobertos via injeção SQL
FLAG{sql_1nj3ct10n_m4st3r}	Parâmetros da aplicação	Exploração bem-sucedida de vulnerabilidade SQLi
FLAG{d4t4b4s3_1nj3ct10n_m4st3r}	Formulários de login	Bypass de autenticação via SQL injection

4.3 Flags de Vulnerabilidades

Flag	Localização	Exploração
FLAG{b4sic_s0urc3_c0d3_insp3cti0n}	Código fonte do painel	Exposição de comentários no código fonte HTML
FLAG{lfi_vuln3r4b1lity}	Parâmetro ?file= em /panel.php	Vulnerabilidade de Local File Inclusion identificada
FLAG{xss_r3fl3ct3d_vuln3r4b1l1ty}	Parâmetros de entrada	Cross-Site Scripting refletido descoberto

5. Vulnerabilidades Identificadas

5.1 Falhas Críticas (Risco Alto)

VULN-001: Exposição de Credenciais em Arquivos Públicos

- **Severidade:** Crítica
- **Local:** Vários arquivos (passwords.txt, .git-credentials, database.php.txt)
- **Descrição:** Credenciais de sistemas críticos (SSH, FTP, Banco de Dados, VPN) armazenadas em arquivos de texto acessíveis
- **Impacto:** Comprometimento total da infraestrutura
- **Recomendação:** Remover arquivos sensíveis, implementar gestão segura de segredos

VULN-002: FTP Anônimo Habilitado

- **Severidade:** Crítica
- **Local:** Porta 21/TCP (98.95.207.28)
- **Descrição:** Servidor vsFTPd configurado para permitir login anônimo
- **Impacto:** Acesso não autorizado a arquivos do servidor
- **Evidência:** ftp-anon: Anonymous FTP login allowed (FTP code 230)
- **Recomendação:** Desabilitar acesso anônimo, implementar autenticação forte

VULN-003: Injeção SQL Crítica

- **Severidade:** Crítica
- **Local:** Formulários de login e parâmetros da aplicação
- **Descrição:** Vulnerabilidade de SQL Injection permitindo bypass de autenticação
- **Impacto:** Acesso não autorizado, exfiltração de dados, comprometimento do BD
- **Evidência:** Flags FLAG{sql_1nj3ct10n_m4st3r} e FLAG{d4t4b4s3_1nj3ct10n_m4st3r} ca pturadas
- **Recomendação:** Implementar prepared statements, validar e sanitizar entradas

5.2 Falhas Graves (Risco Médio)

VULN-004: Cross-Site Scripting (XSS) Refletido

- **Severidade:** Alta
- **Local:** Parâmetros de entrada em formulários
- **Descrição:** XSS refletido permitindo execução de scripts arbitrários
- **Impacto:** Roubo de sessões, phishing, defacement
- **Evidência:** Flag FLAG{xss_r3fl3ct3d_vuln3r4b1l1ty} capturada
- **Recomendação:** Implementar escaping de output, validar Content-Type

VULN-005: Traversal de Diretórios / Divulgação de Caminho (Path Disclosure)

- **Severidade:** Alta
- **Local:** Parâmetro file em /panel.php
- **Descrição:** Possível vulnerabilidade de Local File Inclusion
- **Impacto:** Leitura arbitrária de arquivos do sistema
- **Recomendação:** Validar e sanitizar entradas de usuário

VULN-006: Enumeração de Diretórios

- **Severidade:** Média
- **Local:** Servidor Web Apache
- **Descrição:** Diretórios sensíveis descobertos via ferramentas de enumeração
- **Evidência:** /config/, /admin.php, /panel.php identificados
- **Recomendação:** Implementar restrições de acesso, usar arquivos .htaccess

VULN-007: Dados Ocultos em Banco de Dados

- **Severidade:** Baixa
- **Local:** Estrutura do banco de dados
- **Descrição:** Tabelas ou dados não documentados descobertos
- **Evidência:** Flag FLAG{h1dd3n_d4t4_1n_d4t4b4s3} capturada
- **Recomendação:** Revisar estrutura do BD, documentação adequada

5.3 Falhas Moderadas (Risco Baixo)

VULN-008: Exposição de Informações do Sistema

- **Severidade:** Média
- **Local:** Headers HTTP e páginas de erro
- **Descrição:** Versões de software expostas (Apache/2.4.54, PHP)
- **Impacto:** Facilita ataques direcionados
- **Recomendação:** Ocultar headers, customizar páginas de erro

---

6. Metodologia de Teste

6.1 Reconhecimento

- **Ferramentas:** Nmap, Gobuster, Dirb

Serviços Encontrados:

- **Porta 80:** Servidor Web Apache/PHP
- **Porta 21:** Servidor vsFTPd 3.0.5
- **Porta 3306:** MySQL Server
- **Porta 2222:** SSH Server
- **Porta 22:** SSH alternativo
- **Diretórios:** /config, /admin, /panel

6.2 Varredura de Vulnerabilidades

- **Ferramentas:** Nmap scripts, enumeração manual, SQLmap
- **Descobertas:**

  FTP anônimo ativo

  Vulnerabilidades SQLi em formulários

  Arquivos sensíveis expostos

  Diretórios listáveis

6.3 Exploração

- **Técnicas utilizadas:**
  1. Acesso FTP anônimo para coleta de dados
  2. Enumeração de diretórios web
  3. Teste de injeção SQL em formulários
  4. Análise de arquivos expostos
  5. Teste de XSS em parâmetros

6.4 Pós-Exploração

- Coleta de evidências
- Análise de impacto
- Documentação de falhas
- Extração de dados do banco

---

7. Evidências Coletadas

7.1 Credenciais Exposed

plaintext

passwords.txt

SSH: techcorp:TechCorp2024!

FTP Admin: ftpadmin:ftp@dmin123

Database: backup_user:B@cKup_S3cr3t_2024

WiFi: TechCorp_WiFi_2024

VPN: vpn_user:VPN_P@ssw@rd/

.git-credentials

https://admin:gh_pkt_53cr3tT0k3n_2024_TechCorp@github.com

database.php

$db_user = 'techcorp_user';

$db_pass = 'TechCorp_DB_P@ss_2024!';

7.2 Configurações Vulneráveis

plaintext

vsFTPd - Anonymous login enabled

Apache - Directory listing enabled

PHP - Error reporting possibly enabled

MySQL - Permissões excessivas

---

8. Recomendações de Correção

8.1 Ações Imediatas (24-48 horas)

1. **Desabilitar FTP anônimo**

bash

anonymous_enable = NO

2. **Remover arquivos sensíveis**

.git-credentials, passwords.txt, arquivos de configuração

3. **Restringir acesso a diretórios**

Apache Options - Indexes

4. **Corrigir vulnerabilidades SQLi**

Implementar prepared statements

Validar e sanitizar todas as entradas

5. **Alterar todas as credenciais expostas**

8.2 Ações de Médio Prazo (1-2 semanas)

1. Implementar gestão de segredos
2. Configurar WAF (Web Application Firewall)
3. Implementar logging e monitoramento
4. Realizar treinamento de segurança para equipe
5. Corrigir vulnerabilidades XSS

8.3 Ações de Longo Prazo (1 mês)

1. Revisão arquitetural de segurança
2. Implementação de SDLC seguro
3. Pentest regular agendado
4. Programa de bug bounty interno
5. Implementação de controle de acesso baseado em roles (RBAC)

8.4 Recomendações - Princípio 80/20 (Pareto)

Ação (20% de Esforço)	**Impacto Esperado (80% de Melhoria)**
Desabilitar FTP anônimo	Elimina acesso não autorizado a arquivos
Corrigir 3 principais SQLi	Previne 80% dos ataques de injeção
Remover arquivos sensíveis	Elimina 80% das credenciais expostas
Implementar WAF básico	Bloqueia 80% dos ataques automatizados
Alterar senhas padrão	Previne 80% dos acessos não autorizados
Configurar logging básico	Detecta 80% das atividades maliciosas
Validar entradas em formulários críticos	Previne 80% das vulnerabilidades de entrada
Restringir acesso a diretórios	Elimina 80% da enumeração de informações
Implementar HTTPS	Protege 80% do tráfego sensível
Treinamento básico de segurança	Reduz 80% dos erros humanos

Explicação do Princípio 80/20:

Foco nas correções que proporcionam o maior retorno sobre o investimento em segurança. As 10 ações acima, representando aproximadamente 20% do esforço total necessário, devem resolver cerca de 80% dos problemas de segurança identificados.

Lições Aprendidas

1. **Configurações Padrão São Perigosas:** Serviços instalados com configurações padrão representam risco significativo
2. **Informação é Poder:** Exposição de informações mínimas pode levar a comprometimento total
3. **Defesa em Profundidade:** Múltiplas camadas de segurança são essenciais
4. **Monitoramento Contínuo:** Sistemas devem ser regularmente auditados

9. Conclusão

O ambiente da TechCorp Solutions apresentou **falhas críticas de segurança** que permitiriam a um atacante comprometer completamente a infraestrutura. As principais vulnerabilidades estão relacionadas a **configurações inadequadas**, **exposição indevida de informações** e **falhas de validação de entrada**.

Pontos mais críticos:

1. Credenciais armazenadas em texto plano
2. Vulnerabilidades de injeção SQL críticas
3. Serviços expostos sem autenticação adequada
4. Falta de controles básicos de acesso

Status de Segurança: INSEGURO

Recomenda-se a **implementação imediata** das correções propostas, começando pelas ações do Princípio 80/20, seguida de um **reteste completo** para validação das correções.

---

10. ANEXOS, APÊNDICE - EVIDÊNCIAS COLETADAS

10.1 Logs de Comandos Executados

- Arquivo: logs_comandos.pdf
- Arquivo: sessao.log (sessão completa do terminal)
- Arquivo: comandos_usados.txt (comandos principais executados)

10.2 Capturas de Tela

- imagens documentando o processo de exploração
- Capturas de tela das explorações
- Evidências visuais de cada flag capturada
- Interface dos serviços explorados
- Saídas de enumeração

10.3 Arquivos Coletados

- database_backup_2024.sql - Backup do banco de dados
- Configurações diversas dos serviços
- Credenciais e chaves de acesso

10.4 Ferramentas Utilizadas

- Nmap 7.98: Varredura de portas e serviços
- Gobuster v3.8: Enumeração de diretórios web
- SQLmap
- Curl: Testes de requisições HTTP e coleta de dados
- Cliente FTP nativo
- Telnet: Testes de conectividade em portas específicas
- MySQL Client: Conexão ao banco de dados
- SSH Client: Tentativas de acesso remoto
- Script de Log: Registro de sessão (script -a sessao.log)

Assinatura do Responsável pelo Teste:

Nome: Gonçalo Quissola Dala
Data: 27 de novembro de 2025
Assinatura: GD

Documento Confidencial - TechCorp Solutions