



**ESCOLA VAI NA WEB
TURMA CYBERSEC 2025**

Lucas Ribeiro G. Da Silva

Módulo 3 - Relatório de PenTest

Professor: José Menezes

**Rio de Janeiro
2025**

Relatório de Teste de Intrusão (Pentest)

Autor: Lucas Ribeiro Gomes da Silva

Data: 28 de Novembro de 2025 **Versão:** 1.0

Cliente: TechCorp Solutions.

Declaração de Limites de Responsabilidade e Confidencialidade

Este documento contém informação confidencial e privilegiada. Todos os resultados obtidos neste relatório serão utilizados apenas para avaliação [acadêmica / interna de segurança], sem nenhum objetivo de causar dano à empresa, nem a exposição das possíveis vulnerabilidades para terceiros não autorizados.

A execução deste teste seguiu estritamente as leis vigentes e as políticas de segurança previamente acordadas com a contratante. Qualquer reprodução parcial ou total deste documento sem autorização é proibida.

Cronograma de Execução

Os testes documentados neste relatório foram realizados entre os dias 17/11/2025 a 28/11/2025.

Introdução e descrição do alvo

A TechCorp Solutions é uma organização consolidada no setor de tecnologia, atuando há mais de 15 anos no mercado de soluções corporativas. A empresa posiciona-se como parceira estratégica para a transformação digital, com foco em "Inovação e Tecnologia para Negócios".

Sua atuação principal divide-se em três pilares estratégicos, conforme identificado em seus canais institucionais:

- Cloud Computing: Oferecimento de soluções em nuvem escaláveis e seguras.
- Segurança da Informação: Serviços voltados à proteção de dados e compliance corporativo.
- Consultoria em TI: Expertise técnica para otimização de processos de negócio.

Para fins deste teste de intrusão, o alvo primário foi a infraestrutura web e os serviços externos hospedados pela TechCorp Solutions.

Durante a fase de reconhecimento (Fingerprinting), foi possível mapear as seguintes características do ambiente tecnológico da empresa, que compõem a superfície de ataque analisada:

Componente	Tecnologia Identificada	Detalhes
Sistema Operacional	Linux (Debian)	Identificado via análise de banners e comportamento do servidor.
Servidor Web	Apache/2.4.54	Versão exposta nos cabeçalhos HTTP.
Linguagem de Backend	PHP 7.4.33	Tecnologia utilizada para o processamento da aplicação web.
Banco de Dados	MySQL	Identificado através de exposição de código e testes de injeção.
Endereço IP	98.95.207.28	IPv4 público onde os serviços (HTTP, FTP, SSH) estão hospedados.

Escopo do Teste (Scope)

A definição do escopo estabelece os limites operacionais da auditoria, listando explicitamente quais ativos, endereços IP e domínios foram autorizados para a análise de segurança e quais vetores de ataque foram proibidos.

Ativos no escopo: A auditoria concentrou-se na identificação de vulnerabilidades na infraestrutura externa e nos serviços web da contratante. Os seguintes ativos foram alvo dos testes de intrusão:

Ativo / Serviço	Endereço (Target)	Descrição do Teste
Aplicação Web Principal	http://98.95.207.28	Análise completa da interface web, incluindo painéis administrativos, formulários de autenticação, gestão de sessão e validação de input de usuários.
Servidor de Arquivos (FTP)	98.95.207.28 (Porta 21)	Verificação de configurações de acesso anônimo, permissões de arquivos e exposição de dados sensíveis em diretórios públicos.
Administração Remota (SSH)	98.95.207.28 (Porta 22)	Testes de força bruta (brute-force), reutilização de credenciais e verificação de segurança no protocolo de acesso remoto.
Banco de Dados (MySQL)	[Interno]	Testes de injeção de código SQL (SQLi) através da aplicação web para verificar a integridade e o isolamento dos dados armazenados.

Fora do Escopo: Para garantir a estabilidade das operações da empresa e focar na identificação de vulnerabilidades exploráveis sem causar interrupção de negócios, os seguintes itens e técnicas foram considerados fora do escopo:

- Negação de Serviço (DoS/DDoS): Testes de carga ou estresse que visam indisponibilizar serviços ou saturar a largura de banda da rede.
- Engenharia Social Direcionada: Ataques de *Phishing* ou *Spear Phishing* contra diretores (C-Level) ou funcionários específicos não foram realizados nesta etapa.
- Acesso Físico: Tentativas de invasão física aos escritórios ou data centers da empresa.
- Dispositivos de Usuários Finais: A exploração de laptops, smartphones ou estações de trabalho pessoais de funcionários não foi autorizada.
- Destruição de Dados: Em hipótese alguma foram realizadas ações que pudessem corromper ou deletar dados reais do banco de dados de produção; as provas de conceito limitaram-se à leitura de dados (flags).

Metodologia e Ferramentas utilizadas

A avaliação de segurança seguiu uma abordagem estruturada, iniciando-se na modalidade Black Box (sem conhecimento prévio ou credenciais da infraestrutura), simulando o comportamento de um atacante externo real. À medida que vetores de acesso foram comprometidos, a auditoria evoluiu para Grey Box, utilizando as informações obtidas para explorar camadas mais profundas do sistema.

A metodologia de testes baseou-se nas diretrizes do OWASP Top 10 (Open Web Application Security Project) para identificação das falhas web mais críticas, e no PTES para a estruturação das fases do ataque.

O trabalho foi conduzido em quatro etapas distintas:

1. Reconhecimento e Coleta de Informações (Information Gathering):
 - Análise passiva da aplicação web para identificação de tecnologias (Fingerprinting).
 - Inspeção manual do código-fonte HTML para busca de comentários de desenvolvedores, credenciais esquecidas e caminhos ocultos.
 - Verificação de arquivos de indexação, como robots.txt, para mapeamento de diretórios sensíveis.
2. Enumeração e Mapeamento (Scanning and Enumeration):
 - Varredura de portas TCP para identificar serviços ativos além do servidor web (como FTP e SSH).
 - Análise de cabeçalhos HTTP (Headers) para identificar versões de servidor (Apache/PHP) e configurações de cookies.
 - Interação com o servidor FTP para verificar permissões de acesso anônimo.
3. Análise de Vulnerabilidades e Exploração (Exploitation):
 - Testes manuais de injeção de código, especificamente SQL Injection (SQLi) em formulários de autenticação.

- Testes de Cross-Site Scripting (XSS) Refletido para validar a falta de sanitização de inputs do usuário.
 - Tentativas de escalação de privilégios através da manipulação de Cookies e Sessões.
 - Acesso não autorizado ao servidor via SSH utilizando credenciais obtidas na fase de enumeração.
4. Pós-Exploração (Post-Exploitation):
- Coleta de "Flags" (evidências) que comprovam o comprometimento do sistema.
 - Identificação de dados sensíveis armazenados no servidor (arquivos de senhas e backups).

Para a execução técnica dos testes, foram empregadas as seguintes ferramentas e recursos:

Ferramenta / Recurso	Finalidade no Teste
Nmap (Network Mapper)	Utilizado para o <i>Port Scanning</i> inicial, identificando as portas 21 (FTP), 22 (SSH) e 80 (HTTP) abertas no servidor alvo.
Browser DevTools	Ferramenta nativa do navegador utilizada para inspeção do DOM, manipulação de Cookies de sessão e análise do tráfego de rede (Request/Response Headers).
Cliente FTP (CLI)	Utilizado para estabelecer conexão com o servidor de arquivos, permitindo a navegação em diretórios e download de arquivos confidenciais encontrados.
Cliente SSH / Terminal	Utilizado para acesso remoto administrativo ao servidor, confirmado a reutilização de senhas e comprometimento total do host.
Scripts Manuais (Payloads)	Criação de <i>queries</i> maliciosas customizadas (ex: ' OR 1=1 --) para contornar mecanismos de login e validar falhas de injeção.

Detalhamento técnico das vulnerabilidades

Abaixo estão descritas as vulnerabilidades identificadas, classificadas por nível de severidade, incluindo a metodologia de exploração e as evidências coletadas (Flags).

Critérios de Classificação de Severidade: Para priorização das correções, as vulnerabilidades foram classificadas de acordo com o impacto no negócio e a facilidade de exploração:

- **CRÍTICA:** Falha que permite comprometimento total do servidor, acesso administrativo ou exfiltração massiva de dados. Requer correção imediata.
- **ALTA:** Falha que permite acesso a dados sensíveis ou escalação de privilégios, mas requer condições específicas ou acesso prévio.

- ● **MÉDIA:** Falha que afeta usuários individuais (ex: XSS) ou expõe informações parciais.
- ● **BAIXA/INFORMATIVA:** Mais práticas de configuração ou divulgação de informações técnicas que não permitem invasão direta, mas auxiliam um atacante.

ID	Vulnerabilidade	Severidade	Ativo Afetado
VULN-01	SQL Injection (Data Exfiltration)	● CRÍTICA	Banco de Dados / Login
VULN-02	Credenciais Hardcoded e Acesso SSH	● CRÍTICA	Servidor Linux (Porta 22)
VULN-03	Exposição de Credenciais Git	● ALTA	Arquivo <code>/ .git-credentials</code>
VULN-04	Acesso Anônimo FTP e Arquivos Sensíveis	● ALTA	Servidor FTP (Porta 21)
VULN-05	Cross-Site Scripting (XSS) Refletido	● MÉDIA	Busca / Cookies de Sessão
VULN-06	Information Disclosure (Robots.txt)	● BAIXA	Arquivo <code>/ robots.txt</code>
VULN-07	Information Disclosure (HTML Comment)	● BAIXA	Código Fonte da Home

VULN-01: Exfiltração de Dados via SQL Injection

- **Severidade:** ● Crítica
- **Vetor de Ataque:** Parâmetros de entrada no Login/Dashboard.
- **Referência:** `FLAG_SQL_INJECTION_BUFFED.jpg`

Descrição Técnica: Além do bypass de autenticação, a falha de injeção SQL permitiu a extração completa (dump) da estrutura do banco de dados. Utilizando ferramentas de exploração automatizada (`sqlmap`) ou injeções manuais baseadas em `UNION SELECT`, foi possível ler tabelas arbitrárias.

Evidência de Exploração (PoC): Foi identificada e extraída a tabela `secret_data`, contendo chaves de API, tokens de administração e caminhos de backup.

- **Dados Extraídos:**
 - `database_flag: FLAG{sql_1nj3ct10n_m4st3r}`
 - `admin_token: FLAG{h1dd3n_d4t4_1n_d4t4b4s3}`
 - `api_secret: sk_prod_A7x9...`



Impacto: Comprometimento total da confidencialidade dos dados armazenados, incluindo segredos de negócio e credenciais de acesso.

Recomendação: Implementar *Prepared Statements* em todas as consultas SQL e aplicar princípio de menor privilégio ao usuário do banco de dados.

VULN-02: Acesso SSH e Segredos em Texto Claro

- **Severidade:** ● Crítica
- **Vetor de Ataque:** Reutilização de credenciais (Credential Stuffing).
- **Referência:** FLAG SSH HOME DIRECTORY EXPLORATION.png

Descrição Técnica: Utilizando credenciais obtidas em outras etapas do ataque (ver VULN-04), foi possível realizar login remoto no servidor via protocolo SSH. Dentro do diretório do usuário `techcorp`, foi encontrado um arquivo de texto não protegido contendo anotações críticas da infraestrutura.

Evidência de Exploração (PoC): Acesso ao arquivo `secret.txt` revelou:

- Senha de Root do MySQL: `r00t_P4ssw0rd_2024`
- Credenciais do Painel Admin.
- Chaves de API de Produção e Desenvolvimento.
- **Flag Identificada:** `FLAG{ssh_h0m3_d1r3ct0ry_3xp10r4t10n}`

```
PS C:\ Prompt de Comando - powershell
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 77 Nov 20 23:36 .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 23 02:19 index.html
-rw-r--r-- 1 techcorp techcorp 456 Nov 17 14:28 secret.txt
-rw-r--r-- 1 techcorp techcorp 369 Nov 17 14:28 todo.txt
techcorp@024a36a8e6ca:~$ cat secret.txt
TechCorp Solutions - Internal Notes
=====
Senhas importantes:
- Root MySQL: r00t_P4ssw0rd_2024
- Admin Panel: admin / admin123

Backup Location: /var/backups/techcorp/

API Keys:
- Production: tc_sk_prod_9Kx7mN2pQ4rT8wY
- Development: tc_sk_dev_1Aa2Bb3Cc4Dd5Ee

FLAG{ssh_h0m3_d1r3ct0ry_3xp10r4t10n}

Notas:
- Fazer backup toda segunda-feira
- Verificar logs de segurança semanalmente
- Atualizar certificados SSL em março
techcorp@024a36a8e6ca:~$
```

Impacto: Controle total sobre o servidor e a infraestrutura de backend, permitindo alteração de código, persistência de malware e acesso lateral à rede interna.

Recomendação: Desabilitar login por senha no SSH (usar apenas chaves RSA/Ed25519), rotacionar todas as credenciais expostas e remover arquivos sensíveis do diretório home dos usuários.

VULN-03: Exposição de Credenciais Git

- **Severidade:** ● Alta
- **Vetor de Ataque:** Navegação direta (Insecure Direct Object Reference).
- **Referência:** [Flag git credentials leak.png](#)

Descrição Técnica: O servidor web está configurado incorretamente, permitindo o acesso público a arquivos de configuração do Git. O arquivo `.git-credentials` estava acessível via navegador sem autenticação.

Evidência de Exploração (PoC):

Acesso à URL <http://98.95.207.28/.git-credentials> retornou um token de acesso pessoal (PAT) do GitHub.

- **Conteúdo:** https://admin:gh_p4t_S3cr3tT0k3n...@github.com
- **Flag Identificada:** FLAG{glt_cr3d3nt141s_134k}

98.95.207.28/.git-credentials Novo separador anónimo

Inseguro 98.95.207.28/.git-credentials

```
https://admin:gh_p4t_S3cr3tT0k3n_2024_TechCorp@github.com
# FLAG{g1t_cr3d3nt14ls_l34k}
```

Impacto: Permite que atacantes acessem repositórios de código privado da empresa, podendo inserir backdoors no código-fonte ou roubar propriedade intelectual.

Recomendação: Configurar o servidor web (Apache/Nginx) para negar acesso a qualquer arquivo ou diretório iniciado por . (dotfiles), especificamente `.git` e `.git-credentials`.

VULN-04: Acesso Anônimo ao FTP e Arquivos Sensíveis

- **Severidade:** ● Alta
- **Vetor de Ataque:** Configuração insegura de serviço.
- **Referência:** `Flag password File discovery.png` e `STEPS.png`

Descrição Técnica: O serviço FTP permite login com o usuário `anonymous` sem senha. Além disso, as permissões de diretório permitiram acesso a uma pasta chamada `/confidential`, contendo listas de senhas em texto claro.

Evidência de Exploração (PoC):

1. Conexão via `ftp 98.95.207.28`.
 2. Navegação até `/confidential`.
 3. Download do arquivo `passwords.txt` contendo senhas de SSH, Banco de Dados, Wi-Fi e VPN.
- **Flag Identificada:** `FLAG{p4ssw0rd_f113_d1sc0v3ry}`

```

drwxr-xr-x    2 1000      1000        4096 Nov 17 14:28 public
-rw-rxr-xr-x    1 1000      1000         135 Nov 17 14:28 users.conf
-rw-rxr-xr-x    1 1000      1000         329 Nov 17 14:28 welcome.txt
226 Directory send OK.
ftp: 403 bytes recebidos em 0.02Segundos 17.52Kbytes/s.
ftp> get users.conf
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for users.conf (135 bytes).
226 Transfer complete.
ftp: 135 bytes recebidos em 0.00Segundos 135000.00Kbytes/s.
ftp> type users.conf
users.conf: modo desconhecido.
ftp> type users.conf.txt
users.conf.txt: modo desconhecido.
ftp> cd confidential
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwrxr-xr-x    1 1000      1000        542 Nov 17 14:28 passwords.txt
226 Directory send OK.
ftp: 74 bytes recebidos em 0.58Segundos 0.13Kbytes/s.
ftp> get passwords.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for passwords.txt (542 bytes).
226 Transfer complete.
ftp: 542 bytes recebidos em 0.00Segundos 542000.00Kbytes/s.
ftp>

```

```

# 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_f113_d1sc0v3ry}

# NOTA: Estas senhas devem ser trocadas mensalmente!
# Última atualização: 15/01/2024

```

Impacto: Vazamento massivo de credenciais que possibilitou a escalada para ataques críticos (como o acesso SSH descrito na VULN-02).

Recomendação: Desabilitar o acesso anônimo no servidor FTP e criptografar ou remover arquivos de senhas armazenados no servidor.

VULN-05: Cross-Site Scripting (XSS) Refletido

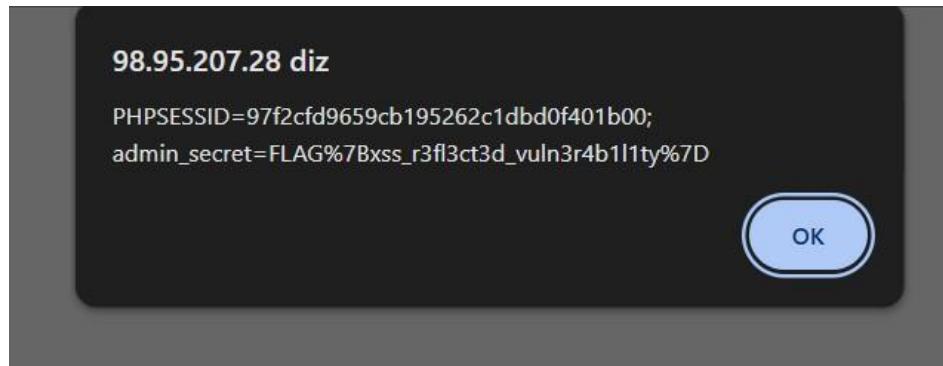
- **Severidade:** ● Média
- **Vetor de Ataque:** Falta de sanitização na busca/output.
- **Referência:** `Flag XSS cross side script.png`

Descrição Técnica: A aplicação reflete a entrada do usuário diretamente na página sem codificação HTML adequada. Isso permitiu a injeção de código JavaScript malicioso.

Evidência de Exploração (PoC):

Ao injetar `<script>alert(document.cookie)</script>`, o navegador executou o script e exibiu os cookies de sessão, incluindo um segredo codificado.

- **Payload Decodificado:** `FLAG{xss_r3fl3ct3d_vuln3r4b1ll1ty}`



Impacto: Risco de roubo de sessão (Session Hijacking), onde um atacante pode assumir a identidade de um administrador logado.

Recomendação: Implementar sanitização de saída (Output Encoding) convertendo caracteres especiais em entidades HTML.

VULN-06 e VULN-07: Information Disclosure (Robots e HTML)

- **Severidade:** ● Baixa (mas facilita ataques complexos)
- **Referência:** `FLAG ROBOTSTXT.png` e `Flag Ispcionar elemento basico.png`

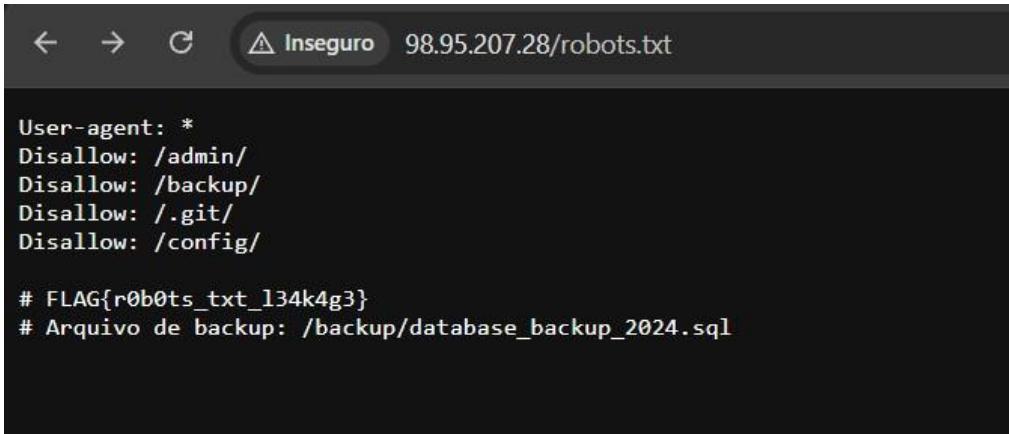
Descrição Técnica: Informações sensíveis foram deixadas expostas em locais públicos propositalmente ou por erro de configuração.

Evidência de Exploração (PoC):

1. **Robots.txt:** O arquivo revelou o diretório `/backup` e o nome de um arquivo de dump SQL crítico.
 - **Flag:** `FLAG{r0b0ts_txt_134k4g3}`

2. **Comentário HTML:** O código fonte da página inicial continha uma flag deixada por desenvolvedores.

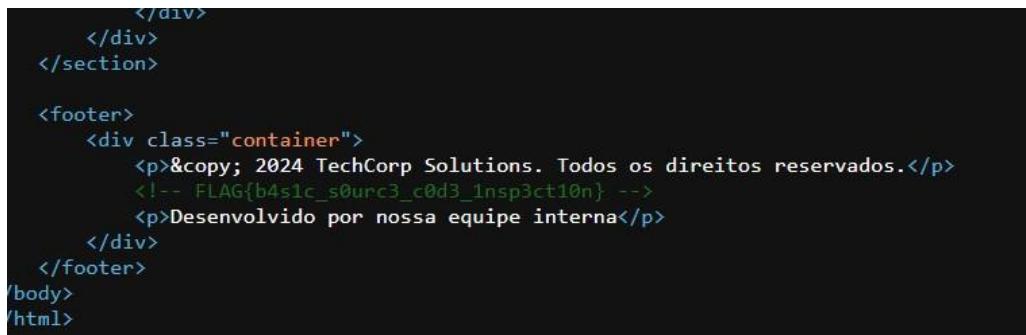
o **Flag:** FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n}



The screenshot shows a browser window with the address bar displaying "98.95.207.28/robots.txt". The page content is a plain text file containing the following:

```
User-agent: *
Disallow: /admin/
Disallow: /backup/
Disallow: /.git/
Disallow: /config/

# FLAG{r0b0ts_tx134k4g3}
# Arquivo de backup: /backup/database_backup_2024.sql
```



The screenshot shows a browser window with the address bar blurred. The page content is the source code of a website, showing HTML structure and comments. Key parts include:

```
</div>
</div>
</section>

<footer>
    <div class="container">
        <p>&copy; 2024 TechCorp Solutions. Todos os direitos reservados.</p>
        <!-- FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n} -->
        <p>Desenvolvido por nossa equipe interna</p>
    </div>
</footer>
</body>
</html>
```

Impacto: Facilita a fase de reconhecimento (Recon) do atacante, fornecendo caminhos para arquivos de backup e estrutura interna do site.

Recomendação: Remover comentários de desenvolvimento em ambiente de produção e auditar o arquivo `robots.txt` para não listar arquivos sensíveis (como backups SQL).

Quadro SWOT da Segurança (Análise de Risco)

Baseado na avaliação realizada, foi elaborado uma análise SWOT (Forças, Fraquezas, Oportunidades e Ameaças) para visualizar o cenário atual da segurança da informação da TechCorp Solutions.

Forças (Strengths)	Fraquezas (Weaknesses)
<ul style="list-style-type: none">O servidor utiliza sistema operacional Linux (Debian) estável.Separação de serviços em portas distintas (Web, FTP, SSH).	<ul style="list-style-type: none">Gestão de Segredos: Senhas críticas armazenadas em texto claro no código-fonte e arquivos de texto. ☠Validação de Input: Falta de sanitização permitindo SQL Injection e XSS.Configuração: Permissão de acesso anônimo no FTP e exposição de arquivos <code>.git</code>.
Oportunidades (Opportunities)	Ameaças (Threats)
<ul style="list-style-type: none">Implementação de ferramentas de análise estática de código (SAST) para detectar senhas <i>hardcoded</i>. ☠Adoção de um Cofre de Senhas (Vault) corporativo.Implementação de WAF (Web Application Firewall) para bloquear injeções.	<ul style="list-style-type: none">Exfiltração Total: Vazamento completo da base de dados de clientes e propriedade intelectual. ☠Ransomware: O acesso SSH privilegiado facilita a encriptação maliciosa de todos os arquivos do servidor.Danos à Reputação: Perda de confiança dos clientes devido à exposição de dados.

Plano de ação e mitigação (Roadmap)

Visando orientar a equipe técnica da TechCorp Solutions na correção das falhas encontradas, as recomendações foram estruturadas em uma matriz de prioridades baseada na criticidade do risco para o negócio.

Prioridade	Ação Necessária (O que fazer)	Vulnerabilidade Mitigada (Por que fazer)	Prazo Sugerido
 CRÍTICA	<p>Rotação Imediata de Credenciais</p> <p>Alterar senhas de todos os serviços (SSH, Banco de Dados, FTP) e remover credenciais <i>hardcoded</i> (texto claro) dos códigos-fonte e arquivos de texto.</p>	VULN-02 (Credenciais Hardcoded) VULN-03 (Git Credentials)	Imediato (24h)
 CRÍTICA	<p>Implementação de Prepared Statements</p> <p>Refatorar o código de login e busca para utilizar consultas SQL parametrizadas, impedindo a injeção de comandos.</p>	VULN-01 (SQL Injection)	Imediato (24h)
 ALTA	<p>Hardening de Serviços (FTP e Web)</p> <p>Desabilitar o login <code>anonymous</code> no FTP e configurar o servidor web para bloquear acesso a arquivos ocultos (como <code>/git</code> e <code>/backup</code>).</p>	VULN-03 (Git Leak) VULN-04 (FTP Anônimo)	Curto Prazo (48h)

 ALTA	Autenticação em Dois Fatores (2FA) Obrigatóriedade de segundo fator para acessos administrativos e VPN, conforme melhores práticas de segurança.	Acesso SSH e Painel Admin	Curto Prazo (1 semana)
 MÉDIA	Sanitização de Input/Output (XSS) Implementar filtros de entrada e <i>encoding</i> de saída HTML para neutralizar scripts maliciosos.	VULN-05 (XSS Refletido)	Médio Prazo (2 semanas)
 MÉDIA	Política de Senhas Fortes Impor complexidade mínima, rotação periódica e proibir reutilização de senhas antigas.	Gestão de Acesso Geral	Médio Prazo (2 semanas)
 BAIXA	Limpeza de Ambiente (Clean-up) Remover comentários de desenvolvimento, arquivos de teste e configurações padrão (ex: robots.txt revelador).	VULN-06 e VULN-07	Longo Prazo (30 dias)

Fluxo de Melhoria Contínua

Além das correções técnicas acima, sugere-se a adoção de processos contínuos para elevar a maturidade de segurança da organização:

1. Auditoria Pós-Correção (Retest): Solicitar uma nova validação após a aplicação das correções críticas para garantir que as falhas foram efetivamente mitigadas ("Patch Verification").
2. Educação e Cultura: Realizar treinamentos periódicos com desenvolvedores sobre Secure Coding e conscientização sobre vazamento de dados em redes sociais e locais públicos.
3. Gestão de Segredos: Implementar um Cofre de Senhas (Vault) corporativo para evitar o armazenamento de chaves em arquivos de texto ou repositórios de código.

Conclusão

Foram realizados diversos testes de segurança e tentativas de exploração contra a infraestrutura da TechCorp Solutions.

Diferente do cenário ideal, onde se espera encontrar medidas efetivas de proteção, a análise constatou um nível de segurança **CRÍTICO**. A combinação de falhas de configuração (FTP anônimo, `.git` exposto) com erros de desenvolvimento (SQL Injection, senhas no código) permitiu o comprometimento total do servidor.

Foi possível obter acesso administrativo à aplicação web, exfiltrar o banco de dados completo e assumir o controle do sistema operacional via SSH. O ambiente atual apresenta riscos iminentes à continuidade do negócio e requer intervenção imediata.