vantico®

Web Penetration Testing Report

Preparado para Acme

Emissão:

São Paulo, 12 de março de 2026

Sumário

1.0 AVISO LEGAL

1.1 ISENÇÃO DE RESPONSABILIDADE

As descobertas, análises e recomendações aqui apresentadas refletem a avaliação técnica realizada no momento do trabalho e não garantem a segurança total ou permanente dos ativos, sistemas ou ambientes analisados.

Em razão da constante evolução das ameaças e das limitações inerentes a qualquer teste com prazo e escopo definidos, podem existir vulnerabilidades não identificadas. A decisão de aceitar, mitigar ou corrigir os riscos apresentados é de responsabilidade exclusiva do cliente.

Por se tratar de uma atividade com tempo limitado e baseada em melhor esforço, a natureza do teste de intrusão não garante a inexistência de outras falhas de segurança no escopo avaliado, nem impede a ocorrência de incidentes de segurança no futuro. Os resultados apresentados neste documento não devem ser interpretados como aconselhamento de investimento.

1.2 DECLARAÇÃO DE CONFIDENCIALIDADE

Este documento é de propriedade exclusiva das partes envolvidas e contém informações proprietárias e confidenciais. A duplicação, redistribuição ou utilização, total ou parcial, em qualquer forma, requer consentimento expresso das partes.

A Vantico autoriza o cliente a compartilhar este documento com parceiros comerciais, auditores e órgãos reguladores, exclusivamente quando houver necessidade de comprovar a realização de um teste de intrusão. Esta permissão é concedida para fins específicos de conformidade com normativas, auditorias, requisições ou outros procedimentos que requeiram comprovação da execução de um teste de intrusão.

2.0 SUMÁRIO EXECUTIVO

A **Vantico** conduziu um teste de intrusão para avaliar a postura de segurança da Acme e identificar vulnerabilidades que possam impactar negativamente seus dados, sistemas ou reputação.

Com este relatório final, a Acme recebe um recurso valioso para orientar o processo de mitigação e aprimoramento de suas defesas de forma eficaz, baseando-se na gravidade dos riscos identificados.

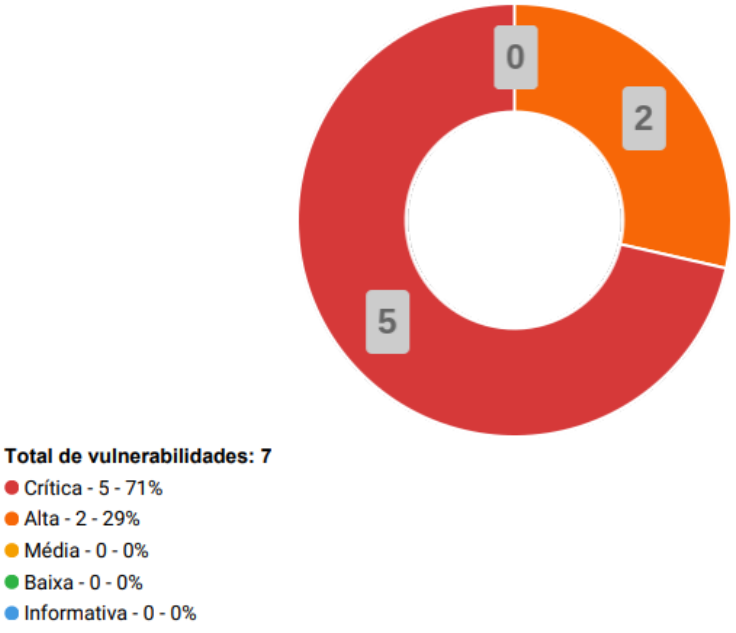
O teste foi realizado no período de **22/04/2024** a **03/06/2024**.

Este teste teve como principal objetivo simular ataques direcionados e customizados de maneira sistemática, visando obter uma compreensão abrangente da resiliência dos sistemas frente a ameaças potenciais.

Com esse foco, a metodologia adotada buscou extrair a maior quantidade possível de informações sensíveis e acessos indevidos, explorando ao máximo as possibilidades de cada falha encontrada dentro do prazo estipulado.

Os testes realizados revelaram a presença de **7** vulnerabilidades, categorizadas da seguinte forma: **5** de risco crítico, **2** de risco alto, **nenhuma** de risco médio, **nenhuma** de risco baixo e **nenhuma** de risco informativo.

O gráfico abaixo apresenta uma distribuição das vulnerabilidades por severidade geral estimada



3.0 ESCOPO DO TESTE

Os testes conduzidos foram inteiramente realizados através da internet.

O modelo de teste de invasão adotado é denominado "**Black-Box**", caracterizando-se por uma abordagem em que os testadores atuam sem qualquer conhecimento prévio dos sistemas internos, processos operacionais e estruturas organizacionais do cliente.

Esta modalidade de teste simula a perspectiva de um agente externo, como um cibercriminoso sem informações privilegiadas, oferecendo uma análise rigorosa e objetiva da exposição do cliente a ameaças externas.

Alvo(s)
app.acme.com

Fora do escopo

Destaca-se que atividades ou ataques de engenharia social, visando explorar a confiança dos usuários ou influenciar seu comportamento em relação ao uso dos serviços, não foram incluídos no escopo deste trabalho. Além disso, ressaltamos que ataques de negação de serviço distribuídos (DDoS) também não fazem parte do escopo definido.

4.0 METODOLOGIA

Para conduzir os testes, foram analisadas centenas de cenários visando identificar ou induzir vulnerabilidades, além de coletar o máximo de informações possíveis sobre a aplicação e o ambiente em que está hospedada. Com base nessas informações, avaliam-se os riscos associados ao negócio.

O foco principal recai sobre as dez categorias de vulnerabilidades mais frequentes nos últimos anos, conhecidas como OWASP Top 10, que englobam uma parcela significativa das falhas relatadas em aplicações web. A OWASP (Open Web Application Security Project) é uma comunidade internacional sem fins lucrativos que ajuda organizações a conceber, desenvolver, adquirir, operar e manter aplicações seguras.

As top 10 vulnerabilidades referentes a aplicação Web que daremos foco nesse relatório são do último relatório da OWASP de 2025:

- A01: Broken Access Control
- A02: Security Misconfiguration
- A03: Software Supply Chain Failures
- A04: Cryptographic Failures
- A05: Injection
- A06: Insecure Design
- A07: Authentication Failures
- A08: Software or Data Integrity Failures
- A09: Logging & Alerting Failures
- A10: Mishandling of Exceptional Conditions

O Padrão de Execução de Testes de Penetração (PTES) é um framework abrangente que delineia uma abordagem estruturada para testes de invasão. Ele consiste em várias fases, incluindo:

- Interações pré-engajamento
- Coleta de Inteligência
- Modelagem de Ameaças
- Análise de Vulnerabilidades
- Exploração
- Pós-Exploração
- Relatório

Ao utilizar estas metodologias em conjunto, o processo de teste garante uma avaliação abrangente da postura de segurança.

O objetivo é identificar vulnerabilidades e fornecer recomendações práticas para mitigar riscos potenciais de forma eficaz.

5.0 CLASSIFICAÇÃO DE RISCOS

Utilizamos uma categorização de risco simples e objetiva para cada vulnerabilidade, com o objetivo de direcionar o processo de triagem para os riscos que realmente são relevantes para o negócio. Como base, é utilizado o Common Vulnerability Scoring System (CVSS), um padrão amplamente reconhecido pela indústria, que atribui pontuações de risco em uma escala de 0,0 a 10,0.

Embora o CVSS forneça uma classificação objetiva, é necessário realizar uma análise complementar que leva em conta as particularidades do ambiente tecnológico e do contexto de negócio da organização. Essa contextualização é essencial, pois uma mesma vulnerabilidade pode representar níveis de risco distintos, dependendo do valor estratégico dos ativos afetados, dos controles de segurança já implementados e do cenário de ameaças específico do setor de atuação.

A tabela a seguir apresenta as categorias de risco adotadas e sua equivalência geral com as pontuações do CVSS, servindo como referência para a priorização das vulnerabilidades identificadas.

Severidade	CVSS	Descrição
Crítica	9.0-10	Implicam no comprometimento de sistemas e informações. Pode ser explorada por um atacante sem muitos conhecimentos técnicos e que podem utilizar ferramentas e exploits disponíveis na Internet. Deve ser tratado imediatamente.
Alta	7.0-8.9	Implicam no comprometimento de sistemas e informações.
Média	4.0-6.9	Não implicam no comprometimento direto do sistema, exigindo, porém, atenção no seu tratamento.
Baixa	0.1-3.9	Não implicam no comprometimento direto do sistema, exigindo, porém, atenção no seu tratamento. Não representam risco imediato, porém, utilizadas em conjunto com outras vulnerabilidades de severidade maior ou igual podem servir de catalisador ou facilitador para comprometimento do sistema.
Informativa	0.0	Nenhuma vulnerabilidade real foi identificada, mas há informações que podem ser relevantes para melhorar a segurança do ambiente.

6.0 TABELA DE VULNERABILIDADES

A tabela a seguir apresenta um resumo das vulnerabilidades identificadas, acompanhado de uma referência ao respectivo grau de severidade.

ID	Vulnerabilidade	Severidade	Status
PT_01	EXPOSIÇÃO DE CREDENCIAIS DA API EM TEXTO CLARO NO FRONT-END	Crítica	Não corrigido
PT_02	REFERÊNCIA A OBJETOS DE FORMA INSEGURA (IDOR) PERMITE ACESSO A DADOS DE PACIENTES	Crítica	Corrigido
PT_03	ESCALAÇÃO DE PRIVILÉGIOS VIA MANIPULAÇÃO DE PARÂMETROS NA ATUALIZAÇÃO DE PERFIL	Crítica	Não corrigido
PT_04	AUSÊNCIA DE CONTROLE ANTI AUTOMAÇÃO NO CAMPO LOGIN PERMITE ATAQUES DE FORÇA BRUTA	Média	Não corrigido
PT_05	FLOOD DE E-MAIL POR MEIO DE REDEFINIÇÃO DE SENHA	Média	Não corrigido
PT_06	POSSIBILIDADE DE INCLUSÃO DE PÁGINAS DA APLICAÇÃO EM FRAMES DE OUTRO DOMÍNIO	Média	Não corrigido
PT_07	AUSÊNCIA DO CABEÇALHO HTTP STRICT TRANSPORT SECURITY	Informativa	Corrigido

7.0 DETALHES DAS VULNERABILIDADES

Nas páginas a seguir encontram-se os detalhes de cada vulnerabilidade identificada durante o processo.

EXPOSIÇÃO DE CREDENCIAIS DA API EM TEXTO CLARO NO FRONT-END	
Severidade: Crítica	**Categoria**: Abuse of Functionality
CVSS Score: 9.3	**Reportado em**: 10/02/2026

Descrição

A exposição excessiva de informações acontece quando uma aplicação web, sem intenção, revela dados sensíveis em páginas, mensagens de erro ou no corpo de respostas enviadas ao usuário. Isso pode incluir informações como: endereços de e-mail ou dados pessoais de usuários, localização física ou caminhos de diretórios, detalhes de infraestrutura (por exemplo, configurações, versões de software), PII (Personally Identifiable Information) ou dados críticos de negócio.

Essas informações podem ser acessadas por usuários não autorizados, facilitando ataques como engenharia social ou ataques direcionados a configurações conhecidas.

A vulnerabilidade ocorre dentro do ativo https://transportes.acme.com/ em que foi identificado a presença da página main.js.

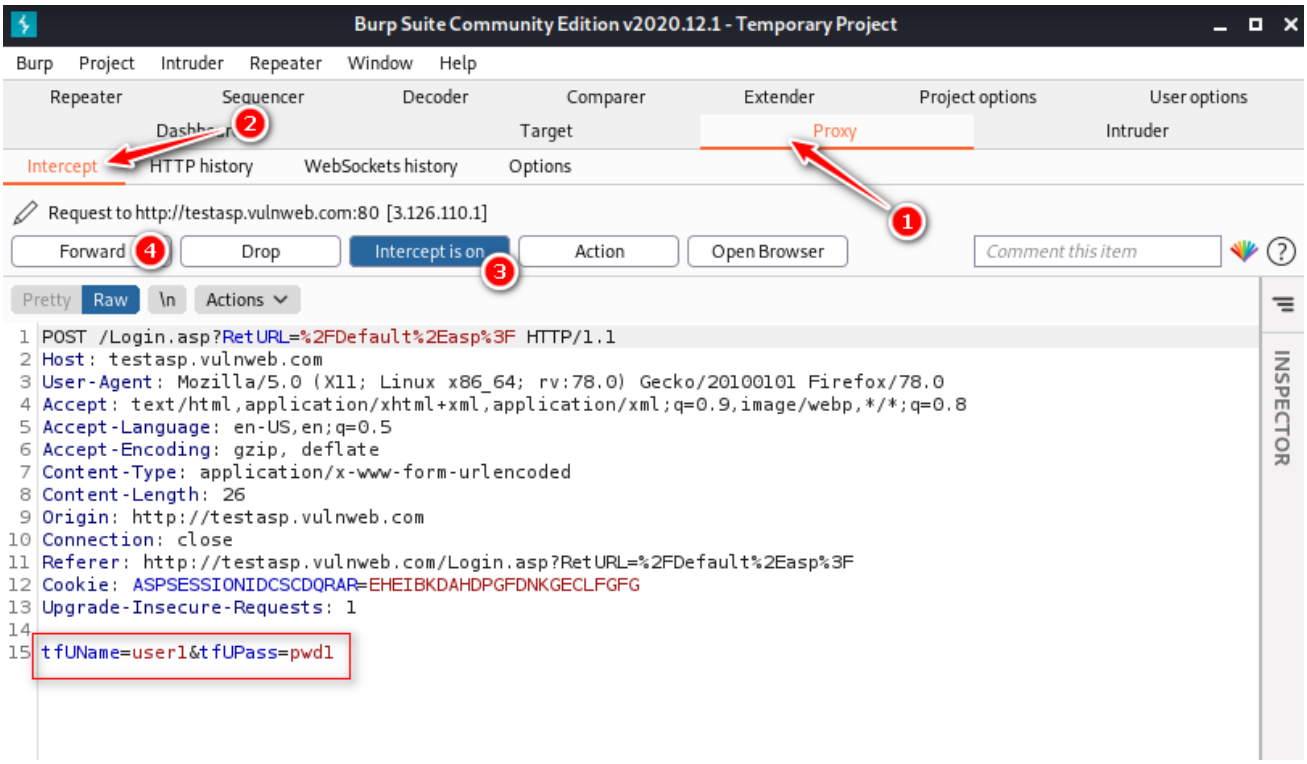


Figura: Exemplo1

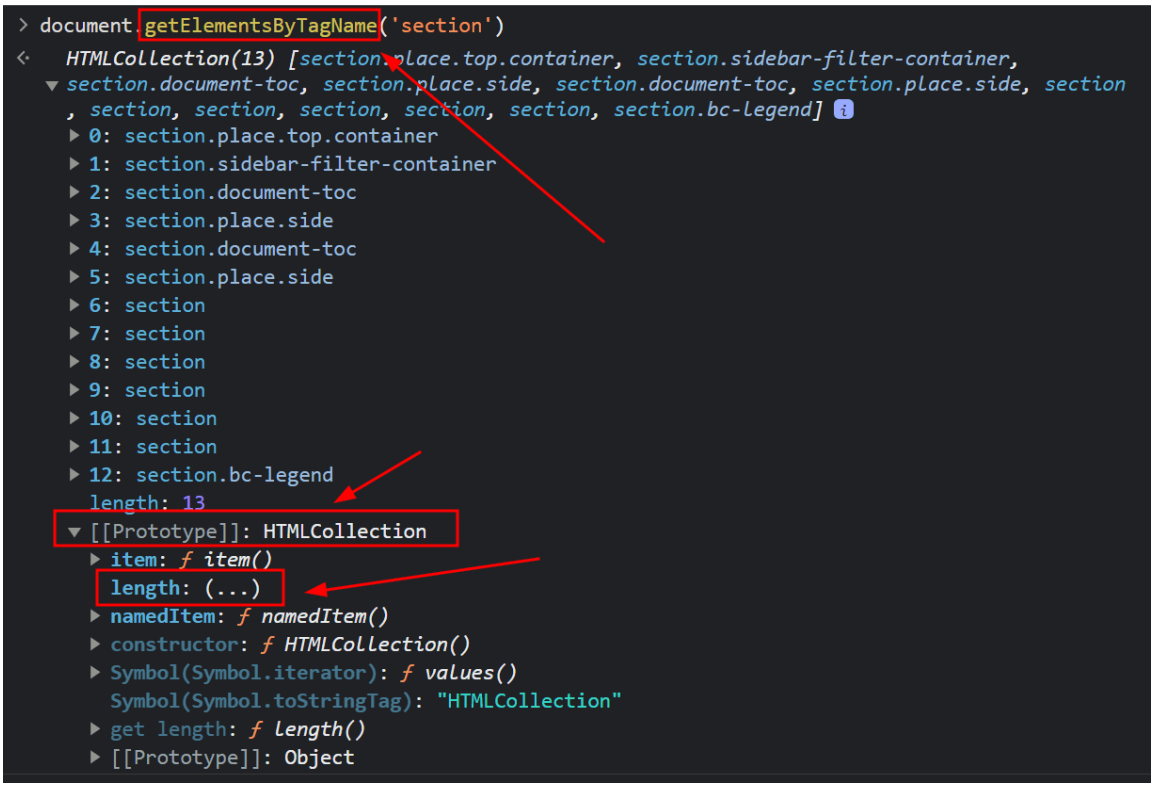


Figura: Identificação do arquivo main.js

Ao analisar o arquivo, foi identificado a exposição de credenciais válidas de um endpoint referente a API (https://api.acme.com), como é possível visualizar a seguir:

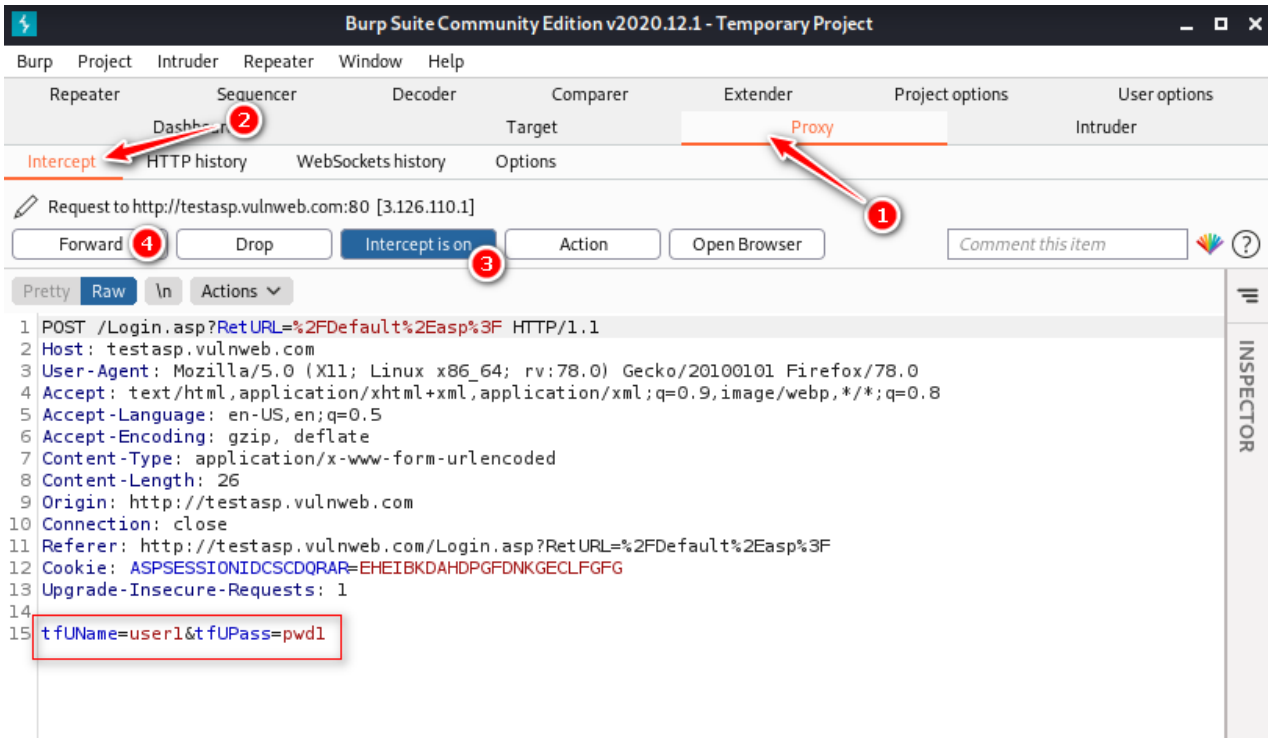


Figura: Credenciais expostas identificadas

Com estas informações, foi realizado uma requisição ao endpoint encontrado com as credenciais informadas, na resposta foi possível obter informações como CNPJs, e-mails, números de telefone, sites, números de inscrição estadual, endereços, entre outros.

Com as credenciais obtidas, foi possível realizar login dentro do endpoint (https://api.acme.com), possibilitando o acesso não autorizado e identificação de detalhes técnicos nas rotas da API.

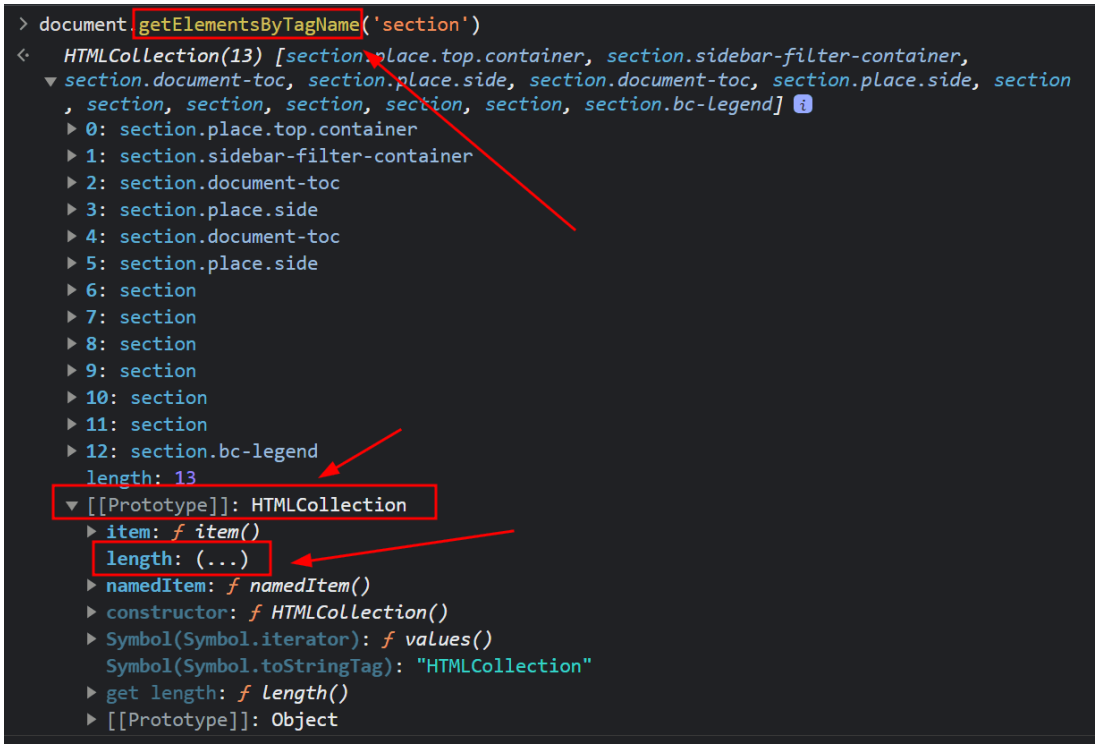


Figura: Acesso dentro do endpoint xxx.acme.com

Impacto de negócio:

Risco de Danos à Reputação: A percepção de que a organização expõe mais dados do que o necessário pode abalar a confiança de clientes e parceiros, afetando a imagem da empresa.

Responsabilidade Legal e Compliance: Dependendo dos dados expostos (por exemplo, PII), a organização pode incorrer em violações de leis de privacidade (como LGPD), resultando em sanções legais, multas e processos judiciais.

Impacto técnico:

Exposição Direta de Dados Sensíveis: Quando a API devolve informações não filtradas, como e-mails ou dados de identificação pessoal (PII), o risco de vazamento de informações confidenciais aumenta significativamente.

Facilitação de Ataques de Engenharia Social: Dados adicionais (como endereços de e-mail) podem ser usados para direcionar ataques de phishing ou spear phishing, elevando a probabilidade de comprometimento de contas.

Recomendações:

Sanitizar e filtrar dados antes de exibi-los aos usuários, garantindo que apenas o necessário para a funcionalidade seja mostrado.

Remover imediatamente todas as credenciais do código front-end público.

Rotacionar os tokens comprometidos e revogar quaisquer sessões associadas.

Mascarar dados (por exemplo, endereços de e-mail e números de telefone) quando forem exibidos para fins de usabilidade mínima.

Validar periodicamente as respostas enviadas pela aplicação para detectar possíveis vazamentos de informações.

Referências:

https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html

https://cwe.mitre.org/data/definitions/200.html

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Web_Page_Content_for_Information_Leakage

Ativos afetados:

https://transportes.acme.com

https://transportes.acme.com/main.7e4fxxxxxx.js

https://api.acme.com

https://api.acme.com/xxx/api/acme/consulta/v2/xxxx