vantico

vantico.com.br

RELATÓRIO TÉCNICO TESTE DE INTRUSÃO EM APLICAÇÃO WEB ACME

Data de emissão:

00/00/2025

1. AVISO LEGAL

1.1. ISENÇÃO DE RESPONSABILIDADE

Reconhece-se a impossibilidade de testar redes, sistemas, serviços e aplicações contra todas as potenciais vulnerabilidades de segurança. Este relatório, portanto, não pode garantir a proteção integral dos ativos contra todas as ameaças existentes.

Os testes realizados refletem apenas a perspectiva da **Vantico**, e os problemas identificados são específicos a esse contexto. Não se pode assegurar a segurança completa dos ativos contra todas as formas de ataque.

Considerando o ambiente dinâmico da tecnologia da informação, é possível que vulnerabilidades em software ou sistemas, desconhecidas no momento do teste de intrusão, não sejam identificadas.

1.2. DECLARAÇÃO DE CONFIDENCIALIDADE

Este documento é de propriedade exclusiva da **Acme** e da **Vantico**, contendo informações de caráter proprietário e confidencial.

Qualquer forma de duplicação, redistribuição ou utilização, seja total ou parcial, é estritamente proibida, salvo mediante consentimento expresso e conjunto de ambas as partes por escrito.

A **Vantico** autoriza o **Acme** 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. INTRODUCÃO

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

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.

Realizado no período de 22/04/2024 a 03/06/2024, o teste buscou identificar falhas de segurança e fornecer recomendações para suas correções.

O teste incluiu a coleta de evidências para cada vulnerabilidade detectada, validando assim sua existência.

O processo de análise seguiu etapas pré-estabelecidas, começando com o mapeamento do ambiente, seguido da priorização dos ativos com base em sua relevância e risco para o negócio, exploração das vulnerabilidades e, por fim, a documentação de cada falha encontrada.

Este procedimento representa um ataque simulado, controlado e adaptado ao contexto específico da **Acme**, imitando um adversário real com capacidade técnica e motivação.

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.

A classificação da severidade das falhas leva em conta seu potencial em facilitar fraudes, vazamentos de dados e outros incidentes que podem resultar em danos financeiros diretos.

3. SUMÁRIO EXECUTIVO

A análise de segurança realizada pela **Vantico** teve como objetivo principal a exploração aprofundada das vulnerabilidades. 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.

Esta abordagem difere do enfoque em largura, que se limita a reportar a presença de vulnerabilidades.

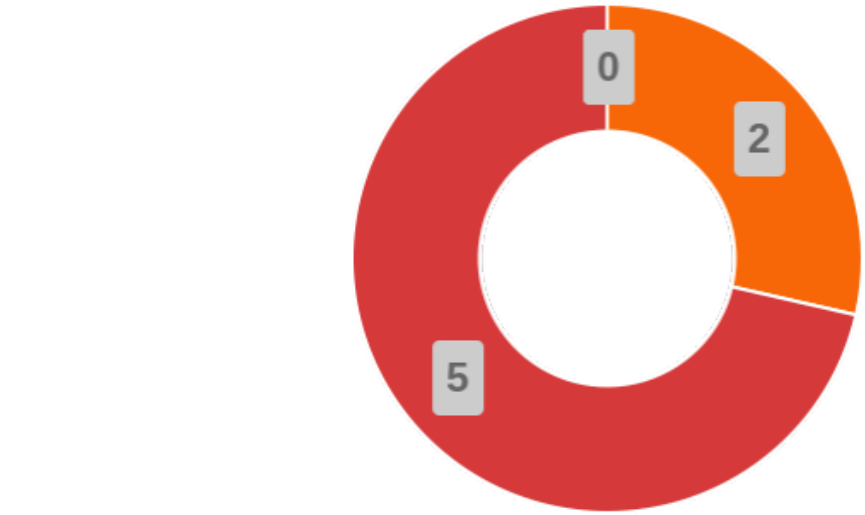
Os objetivos específicos determinados pela **Vantico** para este serviço incluíram:

1. Mapear vetores de ataque;
2. Identificar riscos reais;
3. Sugerir estratégias de mitigação para cada falha de segurança identificada.

O resultado desta análise proporciona uma visão abrangente e clara dos riscos aos quais a instituição está sujeita. Isso oferece uma base sólida, equipada com evidências concretas e estratégias de mitigação, para tomadas de decisão assertivas, contribuindo para a otimização da eficiência da postura de segurança do parque tecnológico sob análise.

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:



Total de vulnerabilidades: 7
- Crítica - 5 - 71%
- Alta - 2 - 29%
- Média - 0 - 0%
- Baixa - 0 - 0%
- Informativa - 0 - 0%

4. ESCOPO

Os testes conduzidos foram inteiramente realizados através da internet.

No decorrer do projeto, a utilização de ferramentas e técnicas personalizadas foi essencial para atender às necessidades específicas do ambiente em análise.

No âmbito deste projeto, foram adotadas todas as precauções necessárias para evitar qualquer prejuízo ao funcionamento dos sistemas do cliente. O objetivo foi assegurar que não houvesse impacto sobre os sistemas ou interrupção na disponibilidade dos serviços.

Escopo avaliado	
Ambiente	Produção
Alvo(s)	*.acme.com *.acme.com.br

Não Escopo

Destaca-se que atividades ou ataques de engenharia social e similares, que visam explorar a confiança dos usuários ou influenciar seu comportamento em relação ao uso dos serviços, não foram incluídos no escopo deste trabalho.

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.

No teste "Black-Box", os especialistas em segurança cibernética adotam a posição de um atacante que tem como único ponto de partida a interface externa do sistema, sem acesso a detalhes como arquitetura de rede, códigos-fonte ou qualquer outra documentação interna.

Essa abordagem permite que os testadores explorem as vulnerabilidades que são visíveis e acessíveis a partir de uma perspectiva externa, identificando falhas que poderiam ser exploradas por agentes mal-intencionados sem conhecimento interno.

White Box

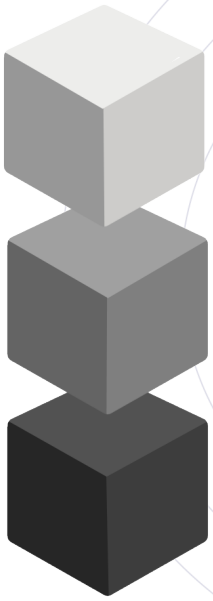
Teste executado com total acesso às informações do sistema e infraestrutura, incluindo bancos de dados, servidores e outros.

Gray Box

Teste executado em áreas específicas do ativo, com informações limitadas fornecidas pelo cliente sobre o sistema e infraestrutura.

Black Box

Teste externo, executado sem nenhuma informação fornecida pelo cliente sobre o sistema e infraestrutura.



5. METODOLOGIA

Durante os testes, iremos abranger centenas de possibilidades para encontrar e / ou provocar vulnerabilidades, além de coletar o máximo de informações possíveis sobre a aplicação e o ambiente que a hospeda, e então, analisar os riscos que essas informações poderão trazer ao negócio.

Será exercido maior esforço dos 10 grupos de vulnerabilidades mais comuns nos últimos anos, esse conjunto de 10 vulnerabilidades representam um número substancial de todas as vulnerabilidades em aplicações web reportadas, também conhecido como OWASP TOP 10.

OWASP é a sigla utilizada para se referir ao Open Web Application Security Project, ou Projeto Aberto de Segurança de Aplicações Web, em português. A OWASP é uma comunidade internacional sem fins lucrativos, cujo objetivo é ajudar organizações a conceber, desenvolver, adquirir, operar e manter aplicações confiáveis. Os 10 principais itens são selecionados e priorizados de acordo com esses dados de prevalência, em combinação com estimativas consensuais de explorabilidade, detectabilidade e impacto.

As top 10 vulnerabilidades referentes a aplicação Web que daremos foco nesse relatório são do último relatório da OWASP de 2021:

A01: Quebra de controle de acesso

A02: Falhas criptográficas

A03: Injeção

A04: Design inseguro

A05: Configuração incorreta de segurança

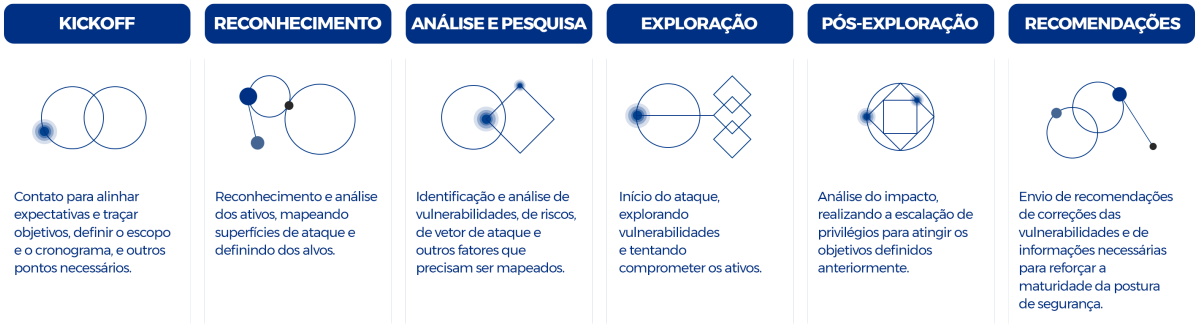
A06: Componentes vulneráveis e desatualizados

A07: Falhas de identificação e autenticação

A08: Falhas de software e integridade de dados

A09: Falhas de registro e monitoramento de segurança

A10: Falsificação de solicitação do lado do servidor (SSRF)



Os testes foram realizados de acordo com as melhores práticas de mercado, seguindo as metodologias a seguir: PTES: O Padrão de Execução de Testes de Penetração (PTES) é um framework abrangente que delineia uma abordagem estruturada para testes de penetração. Ele consiste em várias fases, incluindo:

1. Interações pré-engajamento
2. Coleta de Inteligência
3. Modelagem de Ameaças
4. Análise de Vulnerabilidades
5. Exploração
6. Pós-Exploração
7. Relatório

NIST 800-115: O Guia Técnico NIST 800-115 para Testes e Avaliação de Segurança da Informação é uma diretriz abrangente que fornece um framework para avaliar a segurança de sistemas de informação. Ele abrange vários aspectos, tais como:

1. Técnicas de teste e exame de segurança
2. Planejamento e execução de avaliação de segurança
3. Relatório e documentação
4. Remediação e verificação

Ao utilizar estas metodologias em conjunto, o processo de teste garante uma avaliação abrangente da postura de segurança do sistema alvo. O objetivo é identificar vulnerabilidades e fornecer recomendações práticas para mitigar riscos potenciais de forma eficaz.

6. CLASSIFICAÇÃO DE RISCOS

A Vantico utiliza uma categorização simples de risco para cada vulnerabilidade, a fim de concentrar o processo de triagem nos riscos que realmente importam.

O Common Vulnerability Scoring System (CVSS) é uma fórmula padrão da indústria que atribui pontuações de risco numa escala de 0.0 a 10.0.

A tabela abaixo explica as categorias de risco e demonstra uma equivalência de regra geral com as pontuações do CVSS.

Severidade	CVSS	Descrição
Crítica	9.0 – 10.0	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 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.

O CVSS não é aplicável a todos os tipos de riscos. Por exemplo, não é eficaz em detectar os riscos encontrados em um “design inseguro de funcionalidade”. Com base na experiência, identificamos que isso geralmente constitui um risco alto. Por essa razão, o leitor pode encontrar vulnerabilidades sem classificação CVSS em nossos relatórios.

Nos esforçamos para esclarecer o porquê da pontuação de riscos não ser empregada nesses casos, bem como para indicar, como regra geral, a pontuação CVSS em todas as situações aplicáveis.

7. TABELA DE VULNERABILIDADES

A tabela a seguir resume todas as vulnerabilidades encontradas assim como uma referência ao seu grau de severidade:

ID	Vulnerabilidade	Severidade	Status
PT_01	Acesso a qualquer conta através do código OTP	**Crítica**	**Não corrigido**
PT_02		**Crítica**	**Não corrigido**
PT_03		**Crítica**	**Corrigido**

8. DETALHES DAS VULNERABILIDADES

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

Acesso a qualquer conta através do código OTP	
Severidade: Crítica	**Reportado em**: 28/08/2024
CVSS Score: 9.3	**Categoria**: Abuse of Functionality

Descrição

Foi possível manipular o fluxo de autenticação da aplicação para iniciar sessão com qualquer e-mail que seja conhecido pelo atacante, possibilitando o acesso e vazamento de dados de qualquer conta, inclusive com possibilidade de realizar compras pelos meios de pagamento cadastrados pelo usuário.

Inicialmente, com qualquer token de autorização funcionando, realizar o request para liberar o challenge OTP inserindo o e-mail para o qual deseja iniciar o challenge, o que fará o envio do código para o e-mail:

Figura: Realização do Request

Após isso, basta começar a realizar requisições para validação do OTP, enviando no parâmetro “email” o e-mail que foi iniciado o challenge anteriormente, e no parâmetro “otp” realizar um ataque de força bruta enviando códigos de 6 digitos, entre 000000 e 999999.

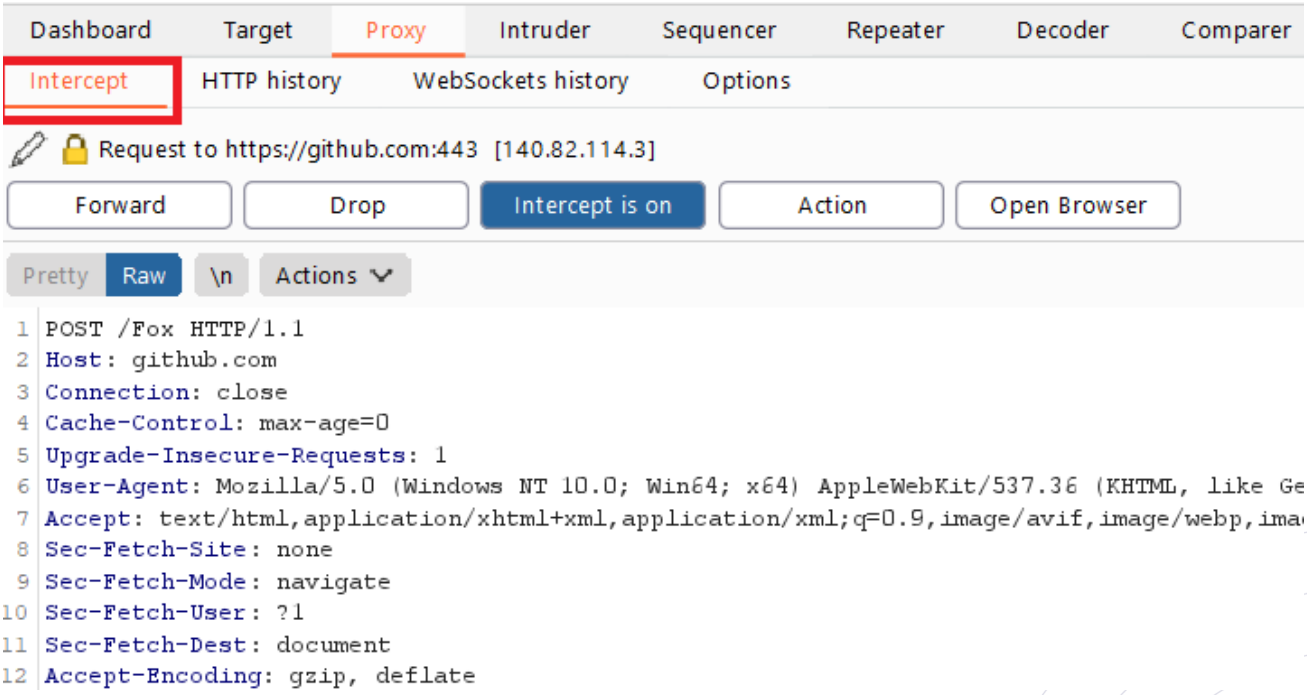


Figura: Força Bruta na validação

Como não há limite para tentativas de envio do OTP, é possível enviar tokens até que o código certo seja descoberto no ataque, com isso recebemos o token de acesso da conta em questão, dando controle dela:

Figura: Exposição de dados

Figura: Exposição Token de acesso

Recomendação

Impor um limite de requisições para a validação do código OTP, inclusive tirando a validade do código antigo caso o limite seja atingido, sendo necessário gerar um novo código, impedindo que o atacante faça inúmeras tentativas até ser capaz de acessar a conta em questão.

Referências

https://owasp.org/API-Security/editions/2019/en/0xa4-lack-of-resources-and-rate-limiting/

https://owasp.org/API-Security/editions/2019/en/0xa2-broken-user-authentication/

Ativos Afetados

api.acme.dev/v1/auth/login